IP 地址管理員

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: IP 地址管理員

Table of Contents

什麼是 IPAM？

Amazon VPC IP 地址管理員 (IPAM) 是一項 VPC 功能，可讓您更輕鬆地規劃、追蹤和監控您 AWS 工作負載的 IP 地址。使用 IPAM 自動化工作流程可以更有效率地管理 IP 地址。

使用 IPAM 可執行以下作業：

- 整理各路由和安全性網域的 IP 地址空間
- 監控使用中的 IP 地址空間並監控按照商業規則使用空間的資源
- 檢視您組織中 IP 地址指派的歷程記錄
- 使用特定商業規則自動將 CIDR 配置給 VPC
- 疑難排解網路連線問題
- 啟用跨區域和跨帳戶共用自攜 IP (BYOIP) 地址
- 將 Amazon 提供的連續 IPv6 CIDR 區塊佈建至用於建立 VPC 的集區

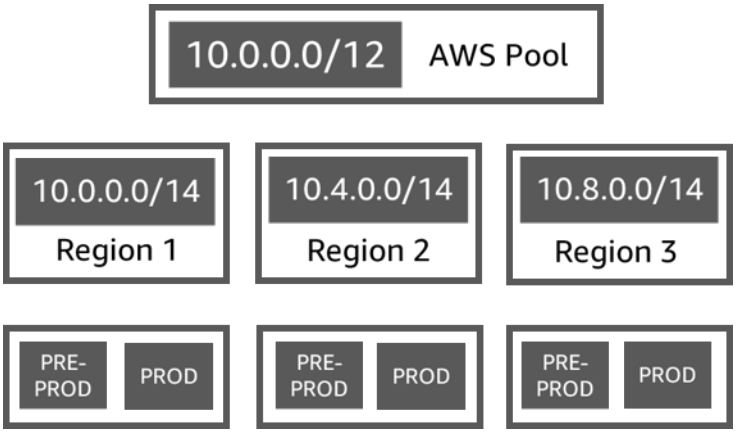
本指南涵蓋下列章節：

- IPAM 的運作方式：IPAM 概念和術語。
- IPAM 入門：啟用 AWS Organizations、建立 IPAM 以及規劃 IP 地址使用等全公司通用的 IP 地址管理步驟。
- 管理 IPAM 中的 IP 地址空間：管理 IPAM、範圍、集區和配置的步驟。
- 追蹤 IPAM 中的 IP 地址使用情況：IPAM 的監控和追蹤 IP 地址使用情況等步驟。
- Amazon VPC IP 地址管理員教學課程：有關建立 IPAM 和集區、分配 VPC CIDR 及自攜公有 IP 地址 CIDR 至 IPAM 的詳細逐步教學課程。

IPAM 的運作方式

為了協助您開始使用 IPAM，本主題解釋一些重要概念。

下圖顯示的 IPAM 集區階層跨頂層 IPAM 集區內的多個 AWS 區域。每個 AWS 區域集區內都有兩個 IPAM 開發集區，一個是用於上線前的集區，另一個是用於上線階段資源的集區。如需有關 IPAM 概念的詳細資訊，請參閱圖表下方的說明。



若要使用 Amazon VPC IP 地址管理員，您要先建立 IPAM。

建立 IPAM 時，請選擇要在其中建立的 AWS 區域。建立 IPAM 時，AWS VPC IPAM 會自動為 IPAM 建立兩個範圍。範圍以及集區和配置是 IPAM 的主要元件。

- 範圍是 IPAM 內最高層級的容器。當您建立 IPAM 時，系統會自動為您建立預設的公有範圍和預設的私有範圍。每個範圍代表單一網路的 IP 空間。私有範圍適用於所有無法公告到網際網路的 IP 位址。公有範圍通常適用於可以從 AWS 公告到網際網路的所有 IP 位址。請注意，將 BYOIPv6 地址佈建至 IPAM 集區時，您可以將這些位址設定為不可公開公告，即使這些位址在公有範圍內。範圍可讓您在多個未連線的網路上重複使用 IP 地址，而不會造成 IP 地址重疊或衝突。在範圍內，您可以建立 IPAM 集區。
- 集區是連續 IP 地址範圍 (或 CIDR) 的集合。IPAM 集區可讓您根據路由和安全需求來整頓 IP 地址。您可以在頂層集區內擁有多個集區。例如，如果您對開發和上線應用程式有不同的路由和安全需求，則可為這兩種應用程式建立各自的集區。在 IPAM 集區內，您可以將 CIDR 配置給 AWS 資源。
- 配置是指將某個 IPAM 集區中的 CIDR 指派到另一個資源或 IPAM 集區。建立 VPC 並為 VPC 的 CIDR 選擇 IPAM 集區時，會從佈建到 IPAM 集區的 CIDR 配置 CIDR。您可以使用 IPAM 來監控和管理配置。

IPAM 可以管理和監控公有和私有 IPv6 空間。如需公有和私有 IPv6 地址的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 IPv6 地址。

若要開始並建立 IPAM，請參閱 IPAM 入門。

IPAM 入門

請依照本節中的步驟，開始使用 IPAM。本節旨在協助您快速開始使用 IPAM，但您可能會發現，透過本部分中的步驟所能實現的目標無法滿足您的需求。如需有關不同 IPAM 使用方式的資訊，請參閱規劃 IP 地址佈建和 Amazon VPC IP 地址管理員教學課程。

在本節中，您將首先存取 IPAM 並決定是否要委派 IPAM 帳戶。在本節結束時，您將已建立 IPAM、建立多個 IP 地址集區，並將集區中 CIDR 配置給 VPC。

任務

- 存取 IPAM
- 設定 IPAM 的整合選項
- 建立 IPAM
- 規劃 IP 地址佈建
- 從 IPAM 集區配置 CIDR

存取 IPAM

與其他 AWS 服務一樣，您可以使用下列方法來建立、存取和管理您的 IPAM：

- AWS 管理主控台：提供 Web 介面，您可用來建立和管理 IPAM。請查看 https://console.aws.amazon.com/ipam/。
- AWS Command Line Interface (AWS CLI)：提供大量 AWS 服務 (包括 Amazon VPC) 的命令。Windows、macOS 和 Linux 都支援 AWS CLI。若要取得 AWS CLI，請參閱 AWS Command Line Interface。
- AWS 開發套件：提供語言特定的 API。AWS 開發套件會處理許多連線詳細資訊，例如計算簽章、處理請求重試和處理錯誤。如需詳細資訊，請參閱 AWS 開發套件。
- 查詢 API：提供您使用 HTTPS 請求呼叫的低階 API 動作。使用查詢 API 是存取 IPAM 最直接的方式。不過，查詢 API 需要您的應用程式處理低階詳細資訊，例如產生雜湊以簽署要求以及處理錯誤。如需詳細資訊，請參閱《Amazon EC2 API 參考》中的 Amazon IPAM 動作。

本指南主要著重於使用 AWS 管理主控台來建立、存取和管理您的 IPAM。在如何在主控台中完成程序的每項描述中，我們都會包含指向 AWS CLI Command Reference 的連結，這樣一來，您便可使用 AWS CLI 完成相同的任務。

如果您是第一次使用 IPAM，請先檢閱 IPAM 的運作方式 以了解 IPAM 在 Amazon VPC 中的角色，然後再繼續執行 設定 IPAM 的整合選項 中的指示。

設定 IPAM 的整合選項

本節介紹將 IPAM 與 AWS Organizations、其他 AWS 帳戶整合，或與單一 AWS 帳戶搭配使用的選項。

開始使用 IPAM 之前，您必須選擇本節中的其中一個選項，才能讓 IPAM 監控與 EC2 聯網資源和存放指標相關聯的 CIDR：

- 若要將 IPAM 與 AWS Organizations 整合，讓 Amazon VPC IPAM 服務管理和監控由所有 AWS Organizations 成員帳戶所建立的聯網資源，請參閱 將 IPAM 與 AWS Organizations 中的帳戶整合。
- 與 AWS Organizations 整合之後，若要整合 IPAM 與組織外部的帳戶，請參閱將 IPAM 與組織外的帳戶整合。
- 若要將單一 AWS 帳戶與 IPAM 一起使用，並啟用 Amazon VPC IPAM 服務來管理和監控您使用單一帳戶所建立的聯網資源，請參閱 與單一帳戶共用 IPAM。

如果您沒有選擇其中一個選項，您仍可建立 IPAM 資源 (例如集區)，但無法在儀表板中看見指標，也無法監控資源的狀態。

目錄

將 IPAM 與 AWS Organizations 中的帳戶整合

或者，您可以依照本節中的步驟，將 IPAM 與 AWS Organizations 整合，並將成員帳戶委派為 IPAM 帳戶。

IPAM 帳戶負責建立 IPAM，並使用 IPAM 來管理和監控 IP 地址使用情況。

將 IPAM 與 AWS Organizations 整合並委派 IPAM 管理員的優點如下：

- 與您的組織共用 IPAM 集區：當您委派 IPAM 帳戶時，IPAM 可讓組織中的其他 AWS Organizations 成員帳戶從使用 AWS Resource Access Manager (RAM) 共用的 IPAM 集區來配置 CIDR。

如需有關設定組織的詳細資訊，請參閱《AWS Organizations 使用者指南》中的什麼是 AWS Organizations？。

- 監控組織中的 IP 地址使用情況：當您委派 IPAM 帳戶時，您會授與 IPAM 許可，以監控所有帳戶的 IP 使用情況。因此，IPAM 會自動將由現有 VPC 跨其他 AWS Organizations 成員帳戶使用的 CIDR 匯入 IPAM。

如果您未將 AWS Organizations 成員帳戶委派為 IPAM 帳戶時，IPAM 將僅監控您用於建立 IPAM 的 AWS 帳戶中的資源。

> **Note**
>
> 與 AWS Organizations 整合：
>
> - 您必須使用 AWS 管理主控台中的 IPAM 或 enable-ipam-organization-admin-account AWS CLI 命令來啟用與 AWS Organizations 的整合。此可確保建立了 `AWSServiceRoleForIPAM` 服務連結角色。若使用 AWS Organizations 主控台或 register-delegated-administrator AWS CLI 命令來啟用 AWS Organizations 的受信任存取，則不會建立 `AWSServiceRoleForIPAM` 服務連結角色，而您也無法在組織內管理或監控資源。
> - IPAM 帳戶必須是 AWS Organizations 成員帳戶。您無法使用 AWS Organizations 管理帳戶作為 IPAM 帳戶。若要檢查您的 IPAM 是否已與 AWS Organizations 整合，請執行下列步驟，並在 Organization 設定中檢視與整合相關的詳細資訊。
> - IPAM 會針對在組織成員帳戶中監控的每個有效 IP 地址向您收費。如需定價的詳細資訊，請參閱 IPAM 定價。
> - 您必須在 AWS Organizations 中擁有帳戶，並擁有設定有一或多個成員帳戶的管理帳戶。如需帳戶類型的詳細資訊，請參閱《AWS Organizations 使用者指南》中的術語與概念。如需有關設定組織的詳細資訊，請參閱《AWS Organizations 入門》。
> - IPAM 帳戶使用的 IAM 角色所連接的 IAM 政策必須允許 `iam:CreateServiceLinkedRole` 動作。當您建立 IPAM 時，您將自動建立 AWSServiceRoleForIPAM 服務連結角色。
> - 與 AWS Organizations 管理帳戶關聯的使用者使用的 IAM 角色必須連接有下列 IAM 政策動作：
>
>   - `ec2:EnableIpamOrganizationAdminAccount`
>   - `organizations:EnableAwsServiceAccess`
>   - `organizations:RegisterDelegatedAdministrator`
>   - `iam:CreateServiceLinkedRole`

如需有關建立 IAM 角色的詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 IAM 使用者。

- 與 AWS Organizations 管理帳戶關聯的使用者可以使用連接有下列 IAM 政策動作的 IAM 角色，來列出您目前的 AWS Orgs 委派管理員：`organizations:ListDelegatedAdministrators`

AWS Management Console

選取 IPAM 帳戶

1. 使用 AWS Organizations 管理帳戶，造訪 https://console.aws.amazon.com/iam/ 開啟 IPAM 主控台。
2. 在 AWS 管理主控台中，選擇欲使用 IPAM 的 AWS 區域。
3. 在導覽窗格中，選擇 Organization settings (組織設定)。
4. 只有在您已經以 AWS 組織管理帳戶的身分登入主控台後，才能使用 Delegate (委派) 選項。選擇委派。
5. 針對 IPAM 帳戶，輸入 AWS 帳戶 ID。IPAM 管理員必須是 AWS Organizations 成員帳戶。
6. 選擇儲存變更。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

- 若要使用 AWS CLI 委派 IPAM 管理員帳戶，請使用下列的命令：enable-ipam-organization-admin-account

當您將 Organizations 成員帳戶委派為 IPAM 帳戶時，IPAM 會自動在組織的所有成員帳戶中建立服務連結的 IAM 角色。IPAM 會擔任每個成員帳戶中的服務連結 IAM 角色、探索資源及其 CIDR，並將其與 IPAM 整合，以監控這些帳戶中的 IP 地址使用情況。IPAM 可以探索所有成員帳戶內的資源，無論其 Organizational Unit 為何。例如，如果有已建立 VPC 的成員帳戶，您將會在 IPAM 主控台的 Resources 區段中看到 VPC 及其 CIDR。

> **Important**
>
> 委派 IPAM 管理員的 AWS Organizations 管理帳戶的角色現已完成。若要繼續使用 IPAM，IPAM 管理員帳戶必須登入 Amazon VPC IPAM 並建立 IPAM。

將 IPAM 與組織外的帳戶整合

本節描述如何將 IPAM 與組織外的 AWS 帳戶整合。若要完成本節中的步驟，您必須已完成 將 IPAM 與 AWS Organizations 中的帳戶整合 中的步驟，並已委託 IPAM 帳戶。

整合 IPAM 與組織外的 AWS 帳戶可讓您執行下列操作：

- 從單一 IPAM 帳戶管理組織外部的 IP 地址。
- 與其他 AWS Organizations 中其他 AWS 帳戶託管的第三方服務共用 IPAM 集區。

將 IPAM 與組織外部的 AWS 帳戶整合後，可以直接與所需之其他組織的帳戶共用 IPAM 集區。

目錄

考量與限制

本節包含整合 IPAM 與組織外部帳戶時的考量和限制：

- 當您與其他帳戶共用資源探索時，交換的唯一資料是 IP 地址和帳戶狀態監控資料。在共用之前，可使用 get-ipam-discovered-resource-cidrs 和 get-ipam-discovered-accounts CLI 命令或 GetIpamDiscoveredResourceCidrs 和 GetIpamDiscoveredAccounts API 來檢視此資料。對於監控組織資源的資源探索，不會共用任何組織資料 (例如組織中的組織單位名稱)。
- 當您建立資源探索時，資源探索會監控擁有者帳戶中的所有可見資源。如果擁有者帳戶是為其自己的多個客戶建立資源的第三方服務 AWS 帳戶，則將由資源探索來探索這些資源。如果第三方 AWS 服務帳戶與最終使用者 AWS 帳戶共用資源探索，則最終使用者可以了解第三方 AWS 服務的其他客戶的資源。因此，第三方 AWS 服務應謹慎建立和共用資源探索，或為每位客戶使用單獨的 AWS 帳戶。

程序概觀

本節介紹如何將 IPAM 與組織外的 AWS 帳戶整合。其指的是本指南其他章節中涵蓋的主題。保持此頁面可見，並在新視窗中開啟以下連結主題，以便您可以返回此頁面獲取指引。

當您將 IPAM 與組織外的 AWS 帳戶整合時，此過程中涉及 4 個 AWS 帳戶：

- 主要組織擁有者 - 組織 1 的 AWS Organizations 管理帳戶。
- 主要組織 IPAM 帳戶 - 組織 1 的 IPAM 委派管理員帳戶。
- 次要組織擁有者 - 組織 2 的 AWS Organizations 管理帳戶。
- 次要組織管理員帳戶 - 組織 2 的 IPAM 委派管理員帳戶。

步驟

1. 主要組織擁有者將其組織的成員委派為主要組織 IPAM 帳戶 (請參閱 將 IPAM 與 AWS Organizations 中的帳戶整合)。
2. 主要組織 IPAM 帳戶會建立 IPAM (請參閱 建立 IPAM)。
3. 次要組織擁有者將其組織的成員委派為次要組織管理員帳戶 (請參閱 將 IPAM 與 AWS Organizations 中的帳戶整合)。
4. 次要組織管理員帳戶會建立資源探索，並使用 AWS RAM 將其與主要組織 IPAM 帳戶共用 (請參閱 建立資源探索以與其他 IPAM 整合 和 與其他 AWS 帳戶共用資源探索)。必須在與主要組織 IPAM 相同的主要區域中建立資源探索。
5. 主要組織 IPAM 帳戶使用 AWS RAM 接受資源共用邀請 (請參閱《AWS RAM 使用者指南》中的接受和拒絕資源共用邀請)。
6. 主要組織 IPAM 帳戶將資源探索與其 IPAM 建立關聯 (請參閱 將資源探索與 IPAM 建立關聯)。
7. 主要組織 IPAM 帳戶現在可以監控和/或管理次要組織中帳戶所建立的 IPAM 資源。
8. (選用) 主要組織 IPAM 帳戶與次要組織中的成員帳戶共用 IPAM 集區 (請參閱 透過 AWS RAM 共用 IPAM 集區)。
9. (選用) 如果主要組織 IPAM 帳戶想要停止探索次要組織中的資源，則其可以取消資源探索與 IPAM 的關聯 (請參閱 取消關聯資源探索)。
10. (選用) 如果次要組織管理員帳戶想要停止參與主要組織的 IPAM，則他們可以取消共用已共用的資源探索 (請參閱《AWS RAM 使用者指南》中的更新 AWS RAM 中的資源共用) 或刪除資源探索 (請參閱 刪除資源探索)。

與單一帳戶共用 IPAM

如果選擇不 將 IPAM 與 AWS Organizations 中的帳戶整合，則能以單一 AWS 帳戶使用 IPAM。

在下一節中建立 IPAM 時，系統會自動在 AWS Identity and Access Management (IAM) 中為 Amazon VPC IPAM 服務建立服務連結角色。

服務連結角色是一種 IAM 角色，可讓 AWS 服務代表您存取其他 AWS服務。它們會自動建立和管理特定 AWS 服務的必要許可，以執行所需的動作，簡化這些服務的設定和管理，藉此簡化許可管理程序。

IPAM 使用服務連結角色來監控並存放與 EC2 聯網資源相關聯的 CIDR 的指標。如需服務連結角色和 IPAM 如何使用的詳細資訊，請參閱 IPAM 的服務連結角色。

> **Important**
>
> 如果您以單一 AWS 帳戶使用 IPAM，則必須確保您用來建立 IPAM 的 AWS 帳戶使用的 IAM 角色連接了允許 `iam:CreateServiceLinkedRole` 動作的政策。當您建立 IPAM 時，您將自動建立 AWSServiceRoleForIPAM 服務連結角色。如需管理 IAM 政策的詳細資訊，請參閱《IAM 使用者指南》中的編輯 IAM 政策。

當單一 AWS 帳戶具有建立 IPAM 服務連結角色的許可後，移至 建立 IPAM。

建立 IPAM

請依照本節中的步驟來建立 IPAM。如果您已委派 IPAM 管理員，則這些步驟應由 IPAM 帳戶完成。

> **Important**
>
> 建立 IPAM 時，系統會要求您允許 IPAM 將來源帳戶的資料複寫到 IPAM 委派帳戶。若要將 IPAM 與 AWS Organizations 整合，IPAM 需要您的許可，才能跨帳戶（從成員帳戶到委派 IPAM 成員帳戶）和跨 AWS 區域（從操作區域到 IPAM 的主區域）複寫資源和 IP 用量詳細資訊。對於單一帳戶 IPAM 使用者，IPAM 需要您的許可才能將跨作業區域的資源和 IP 使用詳細資訊複寫到 IPAM 的主區域。

建立 IPAM 時，您可以選擇允許 IPAM 管理 IP 地址 CIDRs AWS 的區域。這些 AWS 區域稱為操作區域。IPAM 只會在您選取做為操作 AWS 區域的區域中探索和監控資源。IPAM 不會在您選取的作業區域之外存放任何資料。

下列範例階層顯示您在建立 IPAM 時指派 AWS 的區域將如何影響您稍後建立的集區可用的區域。

- 在 AWS 區域 1 和 AWS 區域 2 中操作的 IPAM
  - 私有範圍
    - 頂層 IPAM 集區
      - AWS 區域 2 中的區域 IPAM 集區
        - 開發集區
          - AWS 區域 2 中的 VPC 配置

您只能建立一個 IPAM。如需增加 IPAM 相關配額的詳細資訊，請參閱 IPAM 的配額。

AWS Management Console

建立 IPAM

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在 AWS 管理主控台中，選擇您要在其中建立 IPAM AWS 的區域。在您的主要作業區域中建立 IPAM。
3. 在服務首頁選擇 Create IPAM (建立 IPAM)。
4. 選擇 Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (允許 Amazon VPC IP 地址管理員將來源帳戶的資料複寫到 IPAM 委託帳戶)。若未選取此選項，即無法建立 IPAM。
5. 選擇 IPAM tier (IPAM 方案)。如需每個方案中的可用功能以及方案關聯成本的詳細資訊，請參閱 Amazon VPC 定價頁面中的 IPAM 索引標籤。
6. 在操作區域下，選取此 IPAM 可以管理和探索資源 AWS 的區域。您建立 IPAM AWS 的區域預設會選取為其中一個操作區域。例如，如果您要在 AWS 區域 `us-east-1` 中建立此 IPAM，但您希望稍後再建立區域 IPAM 集區，以便將 CIDR 提供給位於 `us-west-2` 的 VPC，請在此處選取 `us-west-2`。如果您忘記作業區域，稍後可以返回並編輯 IPAM 設定。

> **Note**
>
> 如果要在免費方案中建立 IPAM，可以為 IPAM 選取多個作業區域，但唯一可在各個作業區域使用的 IPAM 功能是公共 IP 洞察功能。無法在 IPAM 的作業區域中使用免費方案中的其他功能，例如 BYOIP。只能在 IPAM 的主區域中使用。若要跨作業區域使用所有 IPAM 功能，請在進階方案中建立 IPAM。

7. 選擇是否要啟用私有 IPv6 GUA CIDR。如需有關此選項的詳細資訊，請參閱 啟用佈建私有 IPv6 GUA CIDR。
8. 選擇是否要啟用計量模式。如需有關此選項的詳細資訊，請參閱 啟用成本分配。
9. 選擇 Create IPAM (建立 IPAM)。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來建立、修改和檢視 IPAM 的相關詳細資訊：

1. 建立 IPAM：create-ipam
2. 檢視您已建立的 IPAM：describe-ipams
3. 檢視自動建立的範圍：describe-ipam-scopes
4. 修改現有 IPAM：modify-ipam

當您完成這些步驟後，IPAM 已完成下列動作：

- 建立您的 IPAM。您可以在主控台的左側導覽窗格中選擇 IPAM，來查看 IPAM 和目前選取的作業區域。
- 建立一個私有和一個公有範圍。您可以在導覽窗格中選擇 Scopes (範圍) 來查看範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。

規劃 IP 地址佈建

依照本節中的步驟，使用 IPAM 集區來規劃 IP 地址佈建。如果您已設定 IPAM 帳戶，則該帳戶需完成這些步驟。公有和私有範圍內的集區建立程序不同。本節包含在私有範圍內建立區域集區的步驟。如需 BYOIP 和 BYOASN 教學課程，請參閱教學課程。

> **Important**
>
> 若要使用跨多個 AWS 帳戶的 IPAM 集區，必須先整合 IPAM 與 AWS Organizations，否則某些功能可能無法正常運作。如需詳細資訊，請參閱 將 IPAM 與 AWS Organizations 中的帳戶整合。

在 IPAM 中，集區是連續 IP 地址範圍 (或 CIDR) 的集合。集區可讓您根據路由和安全需求來整頓 IP 地址。您可在 IPAM 區域以外的 AWS 區域中建立集區。例如，如果您對開發和上線應用程式有不同的路由和安全需求，則可為這兩種應用程式建立各自的集區。

在本節的第一個步驟中，您會建立最上層集區。然後，您會在最上層集區內建立一個區域集區。在區域集區內，您可視需要建立其他集區，例如上線和開發環境集區。依預設，建立的集區最多可深達 10 層。如需 IPAM 配額的相關資訊，請參閱 IPAM 的配額。

> **Note**
>
> 本使用者指南和 IPAM 主控台中不時會使用佈建和配置等專有名詞。佈建是指在 IPAM 集區中新增 CIDR。配置是指在 IPAM 集區中的 CIDR 與資源之間建立關聯。

只要完成本節中的步驟，即可建立如下的集區結構階層範例：

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
  - 私有範圍
    - 最上層集區
      - AWS 區域 1 中的區域集區
        - 開發集區
          - VPC 的配置

此結構可作為 IPAM 使用方式的參考範例，但您可調整 IPAM 以配合貴組織的需求。如需最佳實務的詳細資訊，請參閱 Amazon VPC IP 地址管理員最佳實務。

如果您要建立單一 IPAM 集區，請完成 建立頂層 IPv4 集區 中的步驟，然後跳到 從 IPAM 集區配置 CIDR。

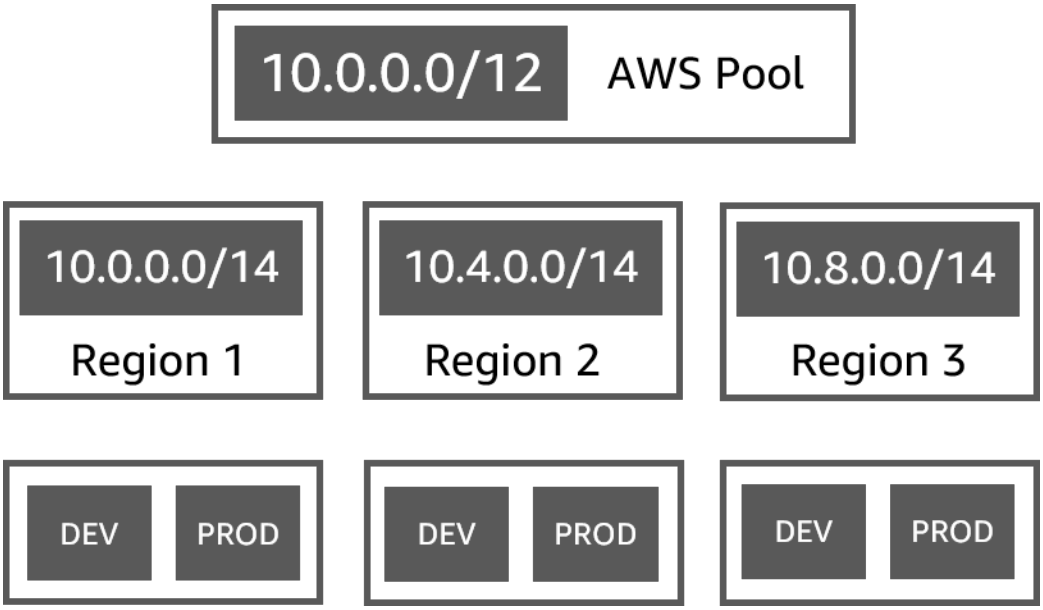
目錄

IPAM 集區計畫範例

您可使用 IPAM 滿足貴組織的需求。本節將示範如何整頓 IP 地址。

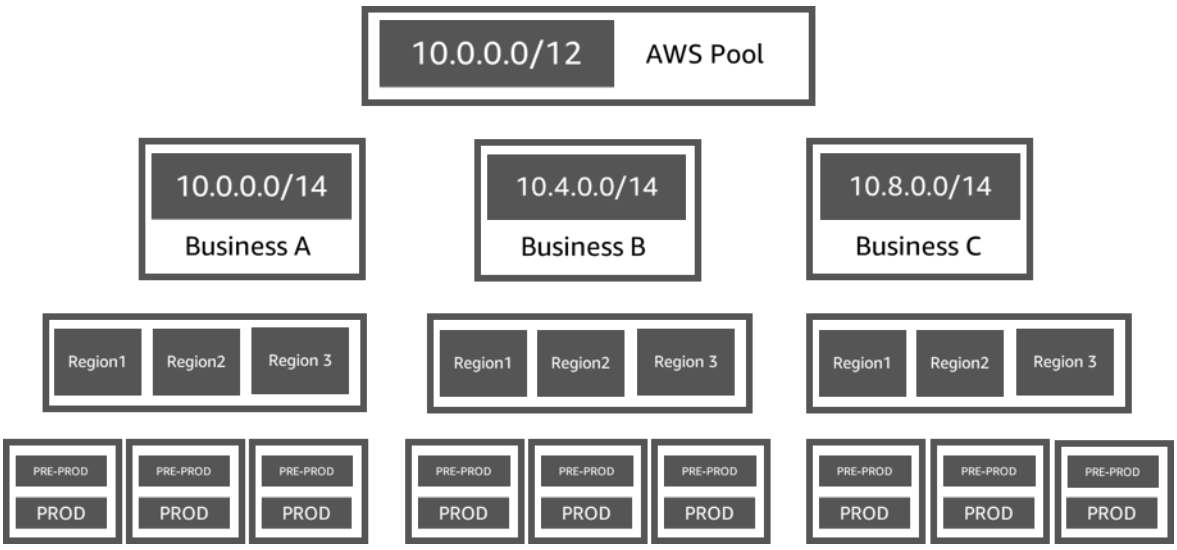
多個 AWS 區域中的 IPv4 集區

下列範例顯示頂層集區中多個 AWS 區域的 IPAM 集區階層。每個 AWS 區域集區都有兩個 IPAM 開發集區，一個集區用於開發資源，另一個集區用於生產資源。



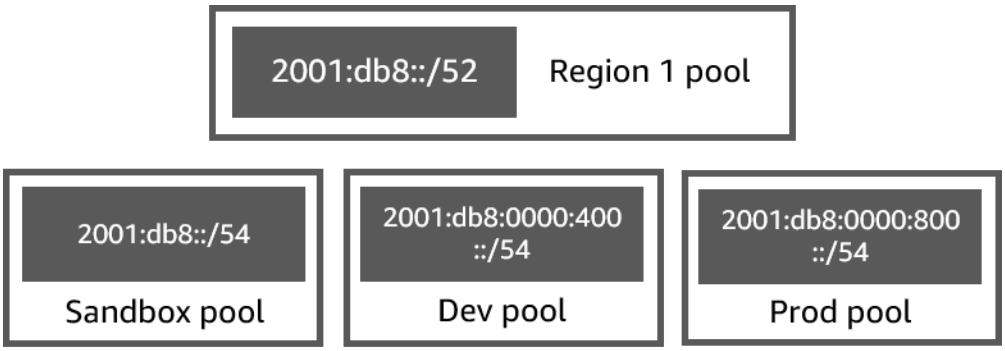
多個業務單位的 IPv4 集區

下例顯示的 IPAM 集區階層跨最上層集區內的多個業務單位。每個業務線的每個集區都包含三個 AWS 區域集區。每個區域集區內都有兩個 IPAM 開發集區，一個是用於上線前資源的集區，另一個是用於上線階段資源的集區。



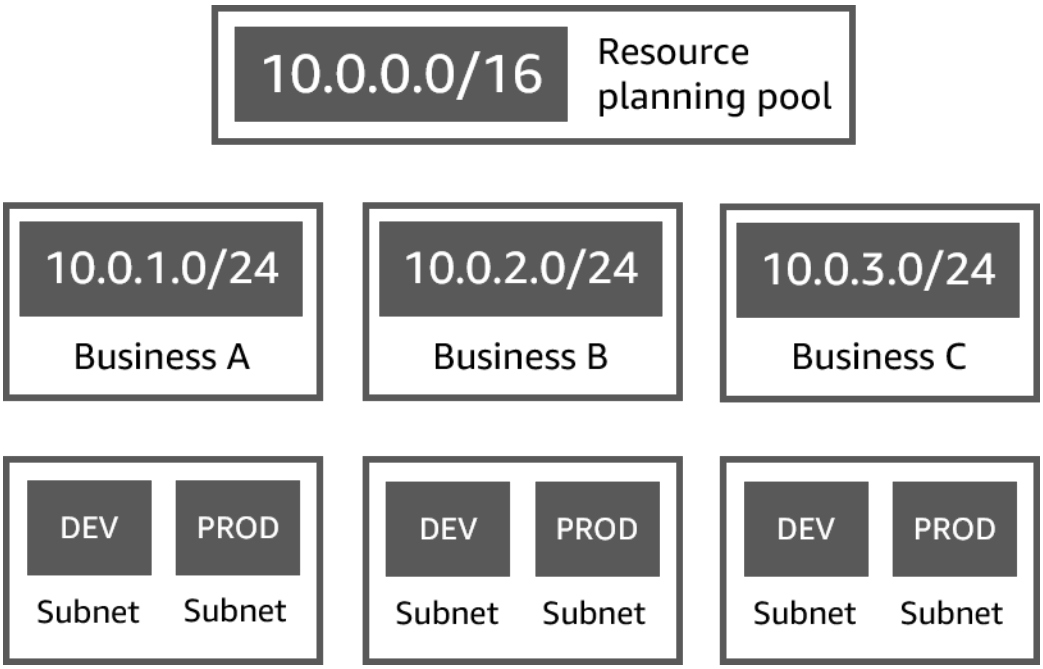
AWS 區域中的 IPv6 集區

下例顯示區域集區內多個業務單位的 IPAM IPv6 集區階層。每個區域集區內都有三個 IPAM 集區，一個集區用於沙盒資源，一個集區用於開發資源，一個集區用於生產資源。



多個業務單位的子網路集區

下例顯示多個業務單位和開發/生產子網路集區的資源規劃集區階層。如需使用 IPAM 規劃子網路 IP 地址空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。



建立 IPv4 集區

請依照本節中的步驟來建立 IPv4 IPAM 集區階層。

只要依照本指南中的指示，即可建立如下例所示的集區結構階層。在本節中，將建立 IPv4 IPAM 集區階層：

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
  - 私有範圍
    - 最上層集區 (10.0.0.0/8)
      - AWS 區域 2 中的區域集區 (10.0.0.0/16)
        - 開發集區 (10.0.0.0/24)
          - VPC 的分配 (10.0.0.0/25)

在上述範例中，所使用的 CIDR 只是範例。其說明頂層集區內的每個集區都使用頂層 CIDR 的一部分進行佈建。

目錄

建立頂層 IPv4 集區

請依照本節中的步驟來建立 IPv4 頂層 IPAM 集區。建立集區時，您可以佈建要使用的集區 CIDR。然後，可以將該空間指派給配置。配置是指將某個 IPAM 集區中的 CIDR 指派到另一個 IPAM 集區或資源。

只要依照本指南中的指示，即可建立如下例所示的集區結構階層。在此步驟中，您要建立頂層 IPAM 集區：

- 在 AWS 區域 1 和 AWS 區域 2 中操作的 IPAM
  - 私有範圍
    - 最上層集區 (10.0.0.0/8)
      - AWS 區域 1 中的區域集區 (10.0.0.0/16)
        - 非生產 VPC 的開發集區 (10.0.0.0/24)
          - VPC 的分配 (10.0.0.0/25)

在上述範例中，所使用的 CIDR 只是範例。其說明頂層集區內的每個集區都使用頂層 CIDR 的一部分進行佈建。

建立 IPAM 集區時，您可以設定 IPAM 集區內所進行的配置的規則。

配置規則可讓您設定下列項目：

- IPAM 是否應該自動將 CIDR 匯入 IPAM 集區 (如果 IPAM 在此集區的 CIDR 範圍內找到 CIDR)
- 集區內配置所需的網路遮罩長度
- 集區內資源所需的標籤
- 集區中資源所需的地區設定。地區設定是 IPAM 集區可用於配置 AWS 的區域。

配置規則會決定資源是否合規或不合規。如需合規的詳細資訊，請參閱 依資源監控 CIDR 使用情況。

> **Important**
>
> 配置規則中沒有顯示額外的隱含規則。如果資源位於 AWS 資源存取管理員 (RAM) 中為共用資源的 IPAM 集區中，則必須將資源擁有者設定為 RAM AWS 中的主體。如需使用 RAM 共用集區的詳細資訊，請參閱 透過 AWS RAM 共用 IPAM 集區。

以下範例顯示如何使用配置規則來控制 IPAM 集區的存取：

Example

根據路由和安全性需求建立集區時，可能只允許特定資源使用集區。在這種情況下，您可以設定配置規則，指出任何想要來自此集區的 CIDR 的資源都必須具有符合配置規則標籤需求的標籤。例如，您可以設定配置規則，指出只有具有 prod 標籤的 VPC 才可從 IPAM 集區取得 CIDR。您也可以設定規則，指出從此集區配置的 CIDR 不得大於 /24。在這種情況下，在此集區中使用大於 /24 的 CIDR 建立資源會違反集區的配置規則，導致建立失敗。CIDR 大於 /24 的現有資源會標記為不合規。

> **Important**
>
> 本主題說明如何使用 AWS提供的 IP 地址範圍建立頂層 IPv4 集區。如果您想要將自己的 IPv4 地址範圍帶到 AWS (BYOIP)，則有先決條件。如需詳細資訊，請參閱教學課程：將 IP 地址帶入 IPAM。

AWS Management Console

建立集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。

2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇建立集區。
4. 在 IPAM 範圍下，選擇您要使用的私有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。

   根據預設，建立集區時，系統會選取私有範圍。私有範圍中的集區必須是 IPv4 集區。公有範圍中的集區可以是 IPv4 或 IPv6 集區。公有範圍適用於所有公有空間。
5. (選用) 為集區新增 Name tag (名稱標籤) 以及集區的描述。
6. 在 Source (來源) 下，選擇 IPAM scope (IPAM 範圍)。
7. 在 Address family (地址系列) 下，選擇 IPv4。
8. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
9. 針對 Locale (地區設定)，選擇 None (無)。您將設定區域集區上的地區設定。

   地區設定是您希望此 IPAM 集區可用於配置 AWS 的區域。例如，您只能從與 VPC 區域共用地區設定的 IPAM 集區為 VPC 配置 CIDR。請注意，當您為集區選擇地區時，您無法對其進行修改。如果 IPAM 的主區域因中斷而無法使用，且集區的地區設定與 IPAM 的主區域不同，則仍然可以使用集區來配置 IP 位址。
10. (選用) 您可以在沒有 CIDR 的情況下建立集區，但是在為其佈建 CIDR 之前，您將無法使用集區進行配置。若要佈建 CIDR，請選擇新增新的 CIDR。輸入要為集區佈建的 IPv4 CIDR。如果您想要將自己的 IPv4 或 IPv6 IP 地址範圍帶到 AWS ，有先決條件。如需詳細資訊，請參閱教學課程：將 IP 地址帶入 IPAM。
11. 選擇此集區的選擇性配置規則：

    - Automatically import discovered resources (自動匯入探索的資源)：如果 Locale (地區設訂) 已設定為 None (無)，則此選項不可用。如果選取此選項，IPAM 會持續尋找此集區 CIDR 範圍內的資源，並自動將其作為配置匯入 IPAM。注意下列事項：
      - 為這些資源分配的 CIDR 必須尚未分配給其他資源，才能使匯入程序成功。
      - IPAM 會匯入 CIDR，不論其是否符合集區的配置規則，因此可能會匯入資源，隨後再將其標記為不合規。
      - 如果 IPAM 發現多個重疊的 CIDR，IPAM 只會匯入最大的 CIDR。
      - 如果 IPAM 發現多個 CIDR 具有相符的 CIDR，IPAM 將只會隨機匯入其中一個 CIDR。

> **Warning**
>
> - 建立 IPAM 後，當您建立 VPC 時，請選擇 IPAM 配置的 CIDR 區塊選項。如果不這樣做，您為 VPC 選擇的 CIDR 可能會與 IPAM CIDR 配置重疊。
> - 如果您已在 IPAM 集區中配置了 VPC，則無法自動匯入具有重疊 CIDR 的 VPC。例如，如果您的 VPC 在 IPAM 集區中配置了 10.0.0.0/26 CIDR，則無法匯入具有 10.0.0.0/23 CIDR 的 VPC (這不會涵蓋 10.0.0.0/26 CIDR)。
> - 將現有的 VPC CIDR 配置自動匯入 IPAM 需要花一些時間。

- Minimum netmask length (最小網路遮罩長度)：此 IPAM 集區中 CIDR 配置要符合所需的最小網路遮罩長度，以及可從集區配置的最大 CIDR 區塊。最小網路遮罩長度必須小於網路遮罩長度上限。IPv4 地址的可能網路遮罩長度為 0 - 32。IPv6 地址的可能網路遮罩長度為 0 - 128。
- Default netmask length (預設網路遮罩長度)：新增至此集區的配置的預設網路遮罩長度。例如，如果佈建至此集區的 CIDR 是 **`10.0.0.0/8`**，且您在此輸入 **`16`**，則此集區中任何新配置的網路遮罩長度都會預設為 /16。
- Maximum netmask length (最大網路遮罩長度)：此集區中的 CIDR 配置所需的最大網路遮罩長度。此數值指定可以從集區配置的最小 CIDR 區塊。
- Tagging requirements (標記需求)：資源從集區配置空間所需的標籤。如果資源在配置空間之後變更了其標籤，或在集區上變更了配置標記規則，則資源可能會標示為不合規。
- Locale (地區設定)：從此集區使用 CIDR 的資源所需的地區設定。沒有此地區設定的自動匯入資源會被標示為不合規。未自動匯入集區的資源將不允許從集區配置空間，除非其位於此地區設定。

> **Note**
>
> 配置規則僅適用於該集區中的受管資源。這些規則不適用於集區中集區的資源。

12. (選用) 為集區選擇 Tags (標籤)。
13. 選擇建立集區。
14. 請參閱 建立區域 IPv4 集區。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令在 IPAM 中建立或編輯頂層集區：

1. 建立集區：create-ipam-pool。
2. 在建立集區後編輯集區以修改配置規則：modify-ipam-pool。

建立區域 IPv4 集區

請依照本節中的步驟，在您的頂層集區中建立區域集區。如果您只需要頂層集區，且不需要其他區域和開發集區，請跳至 從 IPAM 集區配置 CIDR。

> **Note**
>
> 公有和私有範圍內的集區建立程序不同。本節包含在私有範圍內建立區域集區的步驟。如需 BYOIP 和 BYOASN 教學課程，請參閱教學課程。

只要依照本指南中的指示，即可建立如下例所示的集區結構階層。在此步驟中，您要建立區域 IPAM 集區：

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
  - 私有範圍
    - 最上層集區 (10.0.0.0/8)
      - AWS 區域 1 中的區域集區 (10.0.0.0/16)
        - 非生產 VPC 的開發集區 (10.0.0.0/24)
          - VPC 的分配 (10.0.0.0/25)

在上述範例中，所使用的 CIDR 只是範例。其說明頂層集區內的每個集區都使用頂層 CIDR 的一部分進行佈建。

AWS Management Console

在頂層集區內建立一個區域集區。

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。

2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇建立集區。
4. 在 IPAM 範圍下，選擇在建立頂層集區時所使用的相同範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
5. (選用) 為集區新增 Name tag (名稱標籤) 以及集區的描述。
6. 在 Source (來源) 下，選擇 IPAM pool (IPAM 集區)。然後，選擇您在上一節建立的頂層集區。
7. 如果您要在公有範圍內建立此集區，您會看到 地址系列 選項。選擇 IPv4。
8. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
9. 為集區選擇地區設定。選擇地區設定可確保您的集區和從中分配的資源之間沒有跨區域的依賴關係。可用選項來自您在建立 IPAM 時選擇的作業區域。

   地區設定為您希望此 IPAM 集區可供配置使用的 AWS 區域。例如，您只能從與 VPC 區域共用地區設定的 IPAM 集區為 VPC 配置 CIDR。請注意，當您為集區選擇地區時，您無法對其進行修改。如果 IPAM 的主區域因中斷而無法使用，且集區的地區設定與 IPAM 的主區域不同，則仍然可以使用集區來配置 IP 地址。

   > **Note**
   >
   > 如果要在免費方案中建立集區，則只能選擇符合 IPAM 主區域的地區設定。若要跨地區設定使用所有 IPAM 功能，請升級至進階方案。

10. 如果您要在公有範圍內建立此集區，您會看到 服務 選項。選擇 EC2 (EIP/VPC)。您選取的服務確定可公告 CIDR 的 AWS 服務。目前，唯一的選項是 EC2 (EIP/VPC)，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務 (適用於彈性 IP 地址) 和 Amazon VPC 服務 (適用於與 VPC 關聯的 CIDR) 進行公告。
11. (選用) 選擇要為集區佈建的 CIDR。您可以在沒有 CIDR 的情況下建立集區，但是在為其佈建 CIDR 之前，您將無法使用集區進行配置。您可以隨時編輯集區，將 CIDR 新增至集區。
12. 您在此處具有與建立頂層集區時相同的配置規則選項。請參閱 建立頂層 IPv4 集區，以取得建立集區時可用選項的說明。區域集區的配置規則不是繼承自頂層集區。如果您未在此處套用任何規則，則不會為集區設定配置規則。
13. (選用) 為集區選擇 Tags (標籤)。
14. 當您完成集區的設定後，請選擇 Create pool (建立集區)。
15. 請參閱 建立開發 IPv4 集區。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令在 IPAM 中建立區域集區：

1. 取得您要在其中建立集區的範圍 ID：describe-ipam-scopes
2. 取得您要在其中建立集區的集區 ID：describe-ipam-pools
3. 建立集區：create-ipam-pool
4. 檢視新集區：describe-ipam-pools

請重複這些步驟，視需要在頂層集區內建立其他集區。

建立開發 IPv4 集區

請依照本節中的步驟，在您的區域集區內建立開發集區。如果您只需要頂層和區域集區，且不需要開發集區，請跳至 從 IPAM 集區配置 CIDR。

只要依照本指南中的指示，即可建立如下例所示的集區結構階層。在此步驟中，您要建立開發 IPAM 集區：

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
  - 私有範圍
    - 最上層集區 (10.0.0.0/8)
      - AWS 區域 1 中的區域集區 (10.0.0.0/16)
        - 非生產 VPC 的開發集區 (10.0.0.0/24)
          - VPC 的分配 (10.0.1.0/25)

在上述範例中，所使用的 CIDR 只是範例。其說明頂層集區內的每個集區都使用頂層 CIDR 的一部分進行佈建。

AWS Management Console

在區域集區內建立開發集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。

2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇建立集區。
4. 在 IPAM 範圍下，選擇在建立頂層集區和區域集區時所使用的相同範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
5. (選用) 為集區新增 Name tag (名稱標籤) 以及集區的描述。
6. 在 Source (來源) 下，選擇 IPAM pool (IPAM 集區)。然後選擇區域集區。
7. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
8. (選用) 選擇要為集區佈建的 CIDR。您只能佈建已佈建至頂層集區的 CIDR。您可以在沒有 CIDR 的情況下建立集區，但是在為其佈建 CIDR 之前，您將無法使用集區進行配置。您可以隨時編輯集區，將 CIDR 新增至集區。
9. 您在此處具有與建立頂層和區域集區時相同的配置規則選項。請參閱 建立頂層 IPv4 集區，以取得建立集區時可用選項的說明。集區的配置規則不是繼承自階層中其上方的集區。如果您未在此處套用任何規則，則不會為集區設定配置規則。
10. (選用) 為集區選擇 Tags (標籤)。
11. 當您完成集區的設定後，請選擇 Create pool (建立集區)。
12. 請參閱 從 IPAM 集區配置 CIDR。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令在 IPAM 中建立區域集區：

1. 取得您要在其中建立集區的範圍 ID：describe-ipam-scopes
2. 取得您要在其中建立集區的集區 ID：describe-ipam-pools
3. 建立集區：create-ipam-pool
4. 檢視新集區：describe-ipam-pools

請重複這些步驟，視需要在區域集區內建立其他開發集區。

在 IPAM 中建立 IPv6 地址集區

AWS 在包括 EC2、VPC 和 S3 在內的許多服務中提供 IPv6 連線，讓您可以充分利用增加的位址空間和增強的 IPv6 安全功能。IPv6 旨在解決 IPv4 的基本限制。透過移至 128 位元位址空間，IPv6 提供大量的唯一 IP 位址。這種大規模的位址擴充，讓從智慧型手機和 IoT 裝置再到雲端基礎設施在內的連線技術得以持續擴充。

此外，您可以使用 IPAM 來確保自己使用連續的 IPv6 CIDR 來建立 VPC。連續配置的 CIDR 即為依序配置的 CIDR。這些 CIDR 讓您能夠簡化安全與網路規則；IPv6 CIDR 可以彙總在網路與安全建構模組 (例如存取控制清單、路由表、安全群組與防火牆) 之間的單一項目中。

請依照本節中的步驟來建立 IPAM IPv6 集區階層。建立集區時，可以佈建要使用的集區 CIDR。集區會將該 CIDR 內的空間指派給集區內的配置。配置是指將某個 IPAM 集區中的 CIDR 指派到另一個資源或 IPAM 集區。

> **Note**
>
> AWS 提供公有和私有 IPv6 地址。AWS 會考慮從 AWS 公告到網際網路的所有 IP 位址，而私有 IP 位址則不會也無法從 AWS 公告到網際網路。如果您希望私有網路支援 IPv6，且無意將流量從這些位址路由到網際網路，請在私有範圍內建立 IPv6 集區。如需公有和私有 IPv6 地址的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 IPv6 地址。

只要依照本指南中的指示，即可建立如下例所示的集區結構階層。在本節中，將建立 IPv6 IPAM 集區階層：

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
  - 範圍
    - AWS 區域 1 中的區域集區 (2001:db8::/52)
      - 開發集區 (2001:db8::/54)
        - VPC 的配置 (2001:db8::/56)

在上述範例中，所使用的 CIDR 只是範例。它們說明區域集區內的每開發集區如何使用區域集區 CIDR 的一部分進行佈建。

目錄

- 在 IPAM 中建立開發 IPv6 地址集區

在 IPAM 中建立區域 IPv6 地址集區

請依照本節中的步驟來建立 IPv6 區域 IPAM 集區。當您將 Amazon 提供的 IPv6 CIDR 區塊佈建至集區時，必須將它佈建至已選取地區設定 (AWS 區域） 的集區。建立集區時，可以佈建要使用的集區 CIDR，或稍後新增。然後，可以將該空間指派給配置。配置是指將某個 IPAM 集區中的 CIDR 指派到另一個 IPAM 集區或資源。

只要依照本指南中的指示，即可建立如下例所示的集區結構階層。在此步驟中，您要建立 IPv6 區域 IPAM 集區：

- 在 AWS 區域 1 和 AWS 區域 2 中操作的 IPAM
  - Scope (範圍)
    - AWS 區域 1 中的區域集區 (2001：db8：：/52)
      - 開發集區 (2001:db8::/54)
        - VPC 的配置 (2001:db8::/56)

在上述範例中，所使用的 CIDR 只是範例。它們說明 IPv6 區域集區內的每個集區都使用 IPv6 區域 CIDR 的一部分進行佈建。

建立 IPAM 集區時，您可以設定 IPAM 集區內所進行的配置的規則。

配置規則可讓您設定下列項目：

- 集區內配置所需的網路遮罩長度
- 集區內資源所需的標籤
- 集區中資源所需的地區設定。地區設定是 IPAM 集區可用於配置 AWS 的區域。

配置規則會決定資源是否合規或不合規。如需合規的詳細資訊，請參閱 依資源監控 CIDR 使用情況。

> **Note**
>
> 配置規則中沒有顯示額外的隱含規則。如果資源位於 AWS 資源存取管理員 (RAM) 中為共用資源的 IPAM 集區中，則必須將資源擁有者設定為 RAM AWS 中的主體。如需使用 RAM 共用集區的詳細資訊，請參閱 透過 AWS RAM 共用 IPAM 集區。

以下範例顯示如何使用配置規則來控制 IPAM 集區的存取：

Example

根據路由和安全性需求建立集區時，可能只允許特定資源使用集區。在這種情況下，您可以設定配置規則，指出任何想要來自此集區的 CIDR 的資源都必須具有符合配置規則標籤需求的標籤。例如，您可以設定配置規則，指出只有具有 prod 標籤的 VPC 才可從 IPAM 集區取得 CIDR。

> **Note**
>
> - 本主題說明如何使用 AWS 提供的 IPv6 地址範圍或私有 IPv6 範圍建立 IPv6 區域集區。如果您想要將自己的公有 IPv4 或 IPv6 IP 地址範圍帶到 AWS (BYOIP)，有先決條件。如需詳細資訊，請參閱教學課程：將 IP 地址帶入 IPAM。
> - 如果您要在私有範圍內建立 IPv6 集區，可以使用私有 IPv6 GUA 或 ULA 範圍。若要使用私有 GUA 範圍，您必須先在 IPAM 上啟用此選項 (請參閱啟用佈建私有 IPv6 GUA CIDR)。

AWS Management Console

建立集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇建立集區。
4. 在 IPAM 範圍 下，選擇私有範圍或公有範圍。如果您希望私有網路支援 IPv6，且無意將流量從這些地址路由到網際網路，請選擇私有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。

   根據預設，建立集區時，系統會選取私有範圍。
5. (選用) 為集區新增 Name tag (名稱標籤) 以及集區的描述。
6. 在 Source (來源) 下，選擇 IPAM scope (IPAM 範圍)。
7. 針對地址系列，選取 IPv6。如果您是在公有範圍內建立此集區，則此集區中的所有 CIDR 都可公開公告。
8. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。

9. 為集區選擇地區設定。如果您想要將 Amazon 提供的 IPv6 CIDR 區塊佈建至集區，則必須將其佈建至已選取地區設定 (AWS 區域） 的集區。選擇地區設定可確保您的集區和從中分配的資源之間沒有跨區域的依賴關係。可用選項來自您在建立 IPAM 時為其選擇的作業區域。您可隨時新增其他作業區域。

   地區設定是您希望此 IPAM 集區可用於配置 AWS 的區域。例如，您只能從與 VPC 區域共用地區設定的 IPAM 集區為 VPC 配置 CIDR。請注意，當您為集區選擇地區時，您無法對其進行修改。如果 IPAM 的主區域因中斷而無法使用，且集區的地區設定與 IPAM 的主區域不同，則仍然可以使用集區來配置 IP 位址。

   > **Note**
   >
   > 如果要在免費方案中建立集區，則只能選擇符合 IPAM 主區域的地區設定。若要跨地區設定使用所有 IPAM 功能，請升級至進階方案。

10. (可選) 如果您要在公有範圍內建立 IPv6 集區，請在 服務 下選擇 EC2 (EIP/VPC)。您選取的服務確定可公告 CIDR 的 AWS 服務。目前，唯一的選項是 EC2 (EIP/VPC)，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務 (適用於彈性 IP 地址) 和 Amazon VPC 服務 (適用於與 VPC 關聯的 CIDR) 進行公告。
11. （選用） 如果您要在公有範圍內建立 IPv6 集區，請在公有 IP 來源選項下，選擇 Amazon 擁有，讓 為此集區 AWS 提供 IPv6 地址範圍。如本頁頂端所述，本主題涵蓋如何使用 提供的 IP 地址範圍建立 IPv6 區域集區 AWS。如果您想要將自己的 IPv4 或 IPv6 地址範圍帶到 AWS (BYOIP)，則有先決條件。如需詳細資訊，請參閱教學課程：將 IP 地址帶入 IPAM。
12. (選用) 您可以在沒有 CIDR 的情況下建立集區，但是在為其佈建 CIDR 之前，您將無法使用集區進行配置。若要佈建 CIDR，請執行下列其中一項操作：

    - 如果您要在公有範圍內建立 IPv6 集區，並且使用 公有 IP 來源 Amazon 擁有佈建 CIDR，則請在 佈建的 CIDR 下，選擇 新增 Amazon 擁有的 CIDR，並為 CIDR 選擇介於 /40 和 /52 之間的網路遮罩大小。在下拉式選單中選擇網路遮罩長度時，會看到網路遮罩長度以及網路遮罩所代表的 /56 CIDR 數目。依預設，您可以將 Amazon 提供的一個 IPv6 CIDR 區塊新增至區域集區。如需有關提高預設限制的資訊，請參閱 IPAM 的配額。
    - 如果您要在私有範圍內建立 IPv6 集區，可以使用私有 IPv6 GUA 或 ULA 範圍：
      - 如需有關私有 IPv6 定址的重要詳細資訊，請參閱《Amazon VPC 使用者指南》中的私有 IPv6 地址。
      - 若要使用私有 IPv6 ULA 範圍，請在佈建的 CIDR 下，選擇透過網路遮罩新增 ULA CIDR，然後選擇網路遮罩大小，或選擇輸入私有 IPv6 CIDR 並輸入 ULA 範圍。有效的 IPv6 ULA 空間為 fd00::/8 下不與 Amazon 保留範圍 fd00::/16 重疊的任何空間。

- 若要使用私有 IPv6 GUA 範圍，您必須先在 IPAM 上啟用此選項 (請參閱啟用佈建私有 IPv6 GUA CIDR)。啟用私有 IPv6 GUA CIDRs 後，請在 輸入私有 IPv6 CIDR 中輸入 IPv6 GUA。

13. 選擇此集區的選擇性配置規則：

    - Minimum netmask length (最小網路遮罩長度)：此 IPAM 集區中 CIDR 配置要符合所需的最小網路遮罩長度，以及可從集區配置的最大 CIDR 區塊。最小網路遮罩長度必須小於網路遮罩長度上限。IPv6 地址的可能網路遮罩長度為 0 - 128。
    - Default netmask length (預設網路遮罩長度)：新增至此集區的配置的預設網路遮罩長度。例如，如果佈建至此集區的 CIDR 是 `2001:db8::/52`，且您在此輸入 56，則此集區中任何新配置的網路遮罩長度都會預設為 /56。
    - Maximum netmask length (最大網路遮罩長度)：此集區中的 CIDR 配置所需的最大網路遮罩長度。此數值指定可以從集區配置的最小 CIDR 區塊。例如，如果您在此輸入 /56，則可從此集區配置給 CIDR 的最小網路遮罩長度為 /56。
    - Tagging requirements (標記需求)：資源從集區配置空間所需的標籤。如果資源在配置空間之後變更了其標籤，或在集區上變更了配置標記規則，則資源可能會標示為不合規。
    - Locale (地區設定)：從此集區使用 CIDR 的資源所需的地區設定。沒有此地區設定的自動匯入資源會被標示為不合規。未自動匯入集區的資源將不允許從集區配置空間，除非其位於此地區設定。

14. (選用) 為集區選擇 Tags (標籤)。
15. 選擇建立集區。
16. 請參閱 在 IPAM 中建立開發 IPv6 地址集區。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令在您的 IPAM 中建立或編輯 IPv6 區域集區：

1. 如果您想要啟用佈建私有 IPv6 GUA CIDRs，請使用 modify-ipam 修改 IPAM，並將此選項加入 `enable-private-gua`。如需詳細資訊，請參閱啟用佈建私有 IPv6 GUA CIDR。
2. 使用 create-ipam-pool 建立集區。
3. 在集區中佈建新的 CIDR：provision-ipam-pool-cidr。
4. 在建立集區後編輯集區以修改配置規則：modify-ipam-pool。

在 IPAM 中建立開發 IPv6 地址集區

請依照本節中的步驟，在您的 IPv6 區域集區內建立開發集區。如果您只需要頂層集區，不需要區域集區，請跳至 從 IPAM 集區配置 CIDR。

只要依照本指南中的指示，即可建立如下例所示的集區結構階層。在此步驟中，您要建立開發 IPAM 集區：

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
  - 範圍
    - AWS 區域 1 中的區域集區 (2001:db8::/52)
      - 開發集區 (2001:db8::/54)
        - VPC 的配置 (2001:db8::/56)

在上述範例中，所使用的 CIDR 只是範例。其說明頂層集區內的每個集區都使用頂層 CIDR 的一部分進行佈建。

AWS Management Console

在 IPv6 區域集區內建立開發集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇建立集區。
4. 在 IPAM 範圍下，選擇一個範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
5. (選用) 為集區新增 Name tag (名稱標籤) 以及集區的描述。
6. 在 Source (來源) 下，選擇 IPAM pool (IPAM 集區)。然後，在來源集區下，選擇 IPv6 區域集區。
7. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
8. (選用) 選擇要為集區佈建的 CIDR。您只能佈建已佈建至頂層集區的 CIDR。您可以在沒有 CIDR 的情況下建立集區，但是在為其佈建 CIDR 之前，您將無法使用集區進行配置。您可以隨時編輯集區，將 CIDR 新增至集區。

9. 您在此處具有與建立 IPv6 區域集區時相同的配置規則選項。請參閱 在 IPAM 中建立區域 IPv6 地址集區，以取得建立集區時可用選項的說明。集區的配置規則不是繼承自階層中其上方的集區。如果您未在此處套用任何規則，則不會為集區設定配置規則。
10. (選用) 為集區選擇 Tags (標籤)。
11. 當您完成集區的設定後，請選擇 Create pool (建立集區)。
12. 請參閱 從 IPAM 集區配置 CIDR。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令在 IPAM 中建立 IPv6 區域集區：

1. 取得您要在其中建立集區的範圍 ID：describe-ipam-scopes
2. 取得您要在其中建立集區的集區 ID：describe-ipam-pools
3. 建立集區：create-ipam-pool
4. 檢視新集區：describe-ipam-pools

請重複這些步驟，視需要在 IPv6 區域集區內建立其他開發集區。

從 IPAM 集區配置 CIDR

IPAM 的一個重要功能是能夠配置和管理 IP 位址空間。建立 VPC 時，您必須指定 IP 位址 CIDR 區塊，以定義該 VPC 可用的 IP 位址範圍。IPAM 透過提供整個 IP 位址庫存的全域視圖來簡化此程序，協助您跨多個 VPC 策略性地分配和重複使用 IP 字首。

此地址空間配置對於確保沒有重疊 IP 範圍 (可能會導致路由衝突和連線問題) 至關重要。IPAM 也可讓您為未來的 VPC 擴充預留 IP 位址空間，避免日後需要複雜的重新編號。

請依照本節中的步驟，從 IPAM 集區將 CIDR 配置給資源。

> **Note**
>
> 本使用者指南和 IPAM 主控台中不時會使用佈建和配置等專有名詞。佈建是指在 IPAM 集區中新增 CIDR。配置是指在 IPAM 集區中的 CIDR 與資源之間建立關聯。

您可以使用下列方式從 IPAM 集區配置 CIDR：

- 使用與 IPAM 整合 AWS 的服務，例如 Amazon VPC，然後選取選項以使用 CIDR 的 IPAM 集區。IPAM 會自動在集區中為您建立配置。
- 在 IPAM 集區中手動配置 CIDR，以保留供日後與 IPAM 整合 AWS 的服務使用，例如 Amazon VPC。

本節會逐步解說這兩個選項：如何使用與 IPAM 整合 AWS 的服務來佈建 IPAM 集區 CIDR，以及如何手動預留 IP 地址空間。

目錄

建立使用 IPAM 集區 CIDR 的 VPC

使用 Amazon Virtual Private Cloud (Amazon VPC)，您可以在已定義的邏輯隔離虛擬網路中啟動 AWS 資源。這個虛擬網路與您在資料中心中操作的傳統網路非常相似，且具備使用 AWS可擴展基礎設施的優勢。

虛擬私有雲端 (VPC) 是您 AWS 帳戶的專用虛擬網路。其在邏輯上與 AWS 雲端的其他虛擬網路隔離。您可以為 VPC 指定 IP 地址範圍、新增子網、新增閘道，以及與安全群組建立關聯。

請遵循 Amazon VPC User Guide 的 Create a VPC 中的步驟。當您到達為 VPC 選擇 CIDR 的步驟時，您可以選擇從 IPAM 集區使用 CIDR。

如果您在建立 VPC 時選擇使用 IPAM 集區的選項， 會在 IPAM 集區中 AWS 配置 CIDR。您可以在 IPAM 主控台的內容窗格中選擇集區，然後檢視集區的 Resources (資源) 索引標籤，以檢視 IPAM 中的配置。

> **Note**
>
> 如需使用 的完整說明 AWS CLI，包括建立 VPC，請參閱 Amazon VPC IP 地址管理員教學課程一節。

手動將 CIDR 配置給集區，以保留 IP 地址空間

請依照本節中的步驟，手動將 CIDR 配置給集區。您可以執行此步驟，在 IPAM 集區內保留 CIDR 以供日後使用。您也可以在 IPAM 集區中保留空間，以代表內部部署網路。IPAM 會為您管理該保留區，並指出是否有任何 CIDR 與您的內部部署 IP 空間重疊。

AWS Management Console

手動配置 CIDR

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 按預設，會選取預設的私有範圍。如果不想使用預設的私有範圍，請從內容窗格最上方的下拉式選單中選擇您要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 在內容窗格中，選擇集區。
5. 選擇動作 > 建立自訂配置。
6. 選擇是否新增要配置的特定 CIDR (例如，適用於 IPv4 的 `10.0.0.0/24`，或者適用於 IPv6 的 `2001:db8::/52`)，或者只選擇網路遮罩長度，依大小新增 CIDR (例如，適用於 IPv4 的 `/24`，或者適用於 IPv6 的 `/52`)。
7. 選擇 Allocate (配置)。
8. 在 IPAM 中檢視配置的方法是選擇導覽窗格中的 Pools (集區)、選擇集區，然後檢視該集區的 Allocations (配置) 索引標籤。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令手動將 CIDR 配置到集區：

1. 取得您要在其中建立配置的 IPAM 集區 ID：describe-ipam-pools。
2. 建立配置：allocate-ipam-pool-cidr。
3. 檢視配置：get-ipam-pool-allocations。

若要釋放手動配置的 CIDR，請參閱 釋出配置。

管理 IPAM 中的 IP 地址空間

本節中的任務是選用的。請注意，本節提供與使用 IPAM 相關的一組程序。程序依字母順序排列。

如果您要完成本節中的任務，且已委派 IPAM 帳戶，則需由 IPAM 管理員完成這些任務。

請依照本節中的步驟來管理 IPAM 中的 IP 地址空間。

目錄

使用 IPAM 自動化字首清單更新

受管字首清單是一組 CIDR 區塊，您可以在安全群組規則與路由表中引用，而不是指定個別 IP 位址。例如，您可以建立一個包含所有三個 CIDR 的字首清單，並在單一規則中引用它，而不是為 10.1.0.0/16、10.2.0.0/16 和 10.3.0.0/16 分別建立安全群組規則。

受管字首清單有兩種類型：

- 客戶管理字首清單：您定義並管理的 IP 範圍
- AWS受管字首清單： AWS 服務的 IP 範圍 （ 例如 S3 或 CloudFront)

此 IPAM 功能可使 CIDR 項目與您的網路變更保持同步，從而自動化管理客戶管理字首清單。

此功能解決了以下問題

如果沒有自動化，網路團隊會在基礎結構變更與維護跨環境和跨區域的字首清單一致性時，花費大量時間手動更新字首清單。

IPAM 可讓您建立自動填入字首清單的規則，從而解決了此問題。您可以使用兩種方法：參考 IPAM 集區的 CIDRs，或根據您的實際 AWS 資源建立規則，例如 ' 包含標記 env=prod' 的所有 VPCs、' 包含 us-east-1' 中的所有子網路，或 ' 包含帳戶 123456789' 擁有的所有彈性 IP 地址。您新增或移除這些資源時，IPAM 會自動根據 CIDR 更新字首清單。

運作方式

您可以建立規則，告知 IPAM 要在字首清單中包含的 IP 位址。例如「包含帶有 env=prod 標記的所有 VPC CIDR」。您新增或移除生產 VPC 時，IPAM 會自動更新字首清單。

使用時機

- 安全群組：建立規則「包含標記帶有 env=prod 標記所有 VPC」，因此當您新增新的生產 VPC 時，安全群組規則會自動允許這些 VPC
- 多區域：在多個區域中部署相同的 IPAM 規則，以保持相同的字首清單，而無需手動複製 CIDR 項目
- 動態基礎結構：您建立/刪除 VPC 或子網路時，其 CIDR 會自動從字首清單中新增/移除，無需手動更新

先決條件

開始前，請確保您具備以下條件：

- 已啟用進階方案的 IPAM
- 客戶管理字首清單 (或在設定期間建立字首清單)
- IPAM 與 EC2 字首清單操作的 IAM 許可

設定步驟

步驟 1：建立 IPAM 字首清單解析程式

透過建立 IPAM 字首清單解析程式，定義要包含在字首清單中的 CIDR。

AWS Management Console

建立 IPAM 字首清單解析程式

1. 開啟 IAM 主控台。
2. 在導覽窗格中，選擇字首清單解析程式。
3. 選擇建立字首清單解析程式。
4. 在步驟 1：設定解析程式詳細資訊中，選擇下列項目：
   - IPAM：IPAM 執行個體
   - 位址系列：IPv4 或 IPv6
   - 名稱標籤 – 選用：描述性名稱
   - 描述 – 選用：描述
   - 標籤：資源標籤
5. 選擇下一步。
6. 在步驟 2：設定規則中，選擇新增規則。您最多可以新增 99 個規則。

   > **Important**
   >
   > 可以在沒有任何 CIDR 選取規則的情況下建立字首清單解析程式，但此操作會產生空白版本 (不包含任何 CIDR)，直至您新增規則為止。

7. 選擇其中一個規則類型：

- 靜態 CIDR：不會變更的 CIDR 固定清單 (例如，跨區域複寫的手動清單)
- IPAM 集區 CIDR：來自特定 IPAM 集區的 CIDR (例如來自 IPAM 生產集區的所有 CIDR)

  如果您選擇此選項，請選擇下列項目：
  - IPAM 範圍：選取用於搜尋資源的 IPAM 範圍
  - 條件：
    - 屬性
      - IPAM 集區 ID：選取包含資源的 IPAM 集區
      - CIDR (例如 10.24.34.0/23)
    - 操作：等於/不等於
    - 值：要比對條件的值
- 範圍資源 CIDR：來自 IPAM 範圍內 VPCs、子網路、EIPs 等 AWS 資源的 CIDRs

  如果您選擇此選項，請選擇下列項目：
  - IPAM 範圍：選取用於搜尋資源的 IPAM 範圍
  - 資源類型：選取資源，例如 VPC 或子網路。
  - 條件：
    - 屬性：
      - 資源 ID：資源的唯一 ID (例如 vpc-1234567890abcdef0)
      - 資源擁有者 (例如 111122223333)
      - 資源區域 (例如 us-east-1)
      - 資源標籤 (例如索引鍵：名稱、值：dev-vpc-1)
      - CIDR (例如 10.24.34.0/23)
    - 操作：等於/不等於
    - 值：要比對條件的值

8. 選擇下一步。
9. 選擇驗證並建立。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來建立 IPAM 字首清單解析程式：

- 使用 create-ipam-prefix-list-resolver 命令，並儲存傳回解析程式 ID，在步驟 2 中使用。

步驟 2：建立解析程式目標以連線至字首清單

建立解析程式目標，將解析程式連結至現有的字首清單。使用步驟 1 傳回的解析程式 ID。

AWS Management Console

建立 IPAM 字首清單解析程式目標

1. 在 IPAM 主控台中，選擇字首清單解析程式。
2. 選擇您在步驟 1 中建立的解析程式。
3. 在解析程式詳細資訊頁面上，選擇目標索引標籤。
4. 選擇建立目標。
5. 設定目標：
   - 區域：選取存在現有受管字首清單所在區域或您要在其中建立字首清單的區域。
   - 字首清單：選擇現有的受管字首清單或建立新的字首清單
6. 在所需版本下，選取下列其中一個項目：
   - 一律追蹤最新版本：如果您希望字首清單與基礎結構變更保持同步，完全不需要手動介入，請選擇此選項以進行自動更新。
   - 追蹤特定版本：如果您需要可預測、可控制的更新，並想要手動核准字首清單的變更，請選擇此選項，獲得針穩定性。
7. 選擇建立目標。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來建立 IPAM 字首清單解析程式目標：

- 使用步驟 1 的解析程式 ID 和現有的字首清單 ID 執行 create-ipam-prefix-list-resolver-target 命令。

IPAM 現在會根據規則自動更新您的字首清單。該字首清單會填入符合條件的 CIDR。

步驟 3：監控版本與同步情況

由於建立了字首清單解析程式與目標，字首清單解析程式會根據規則產生 CIDR 版本，然後目標會將這些 CIDR 從解析程式同步到特定的受管字首清單。每個版本都是在特定時刻與您的規則相符的 CIDR 的快照。每次 CIDR 清單因基礎設施變更而變更時，版本編號就會遞增。

版本範例：

初始狀態 (第 1 版)

生產環境：

- vpc-prod-web (10.1.0.0/16) – 帶有 env=prod 標記
- vpc-prod-db (10.2.0.0/16) – 帶有 env=prod 標記

解析程式規則：包含所有帶有 env=prod 標記的 VPC

第 1 版 CIDR：10.1.0.0/16、10.2.0.0/16

基礎結構變更 (第 2 版)

新增了新的 VPC：

- vpc-prod-api (10.3.0.0/16) – 帶有 env=prod 標記

IPAM 會自動偵測變更並建立新版本。

第 2 版 CIDR：10.1.0.0/16、10.2.0.0/16、10.3.0.0/16

本節說明如何使用 AWS 主控台或 CLI AWS 監控版本建立，以及使用 CLI AWS 同步成功。

此外，建議針對失敗指標設定 CloudWatch 警示，因為您可能需要重新評估與調整 CIDR 選取規則，以確保版本與字首清單大小在限制範圍內。如需與 IPAM 字首清單相關的 CloudWatch 指標清單，請參閱 IPAM 字首清單解析程式指標。

AWS Management Console

檢視建立的版本並監控目標同步情況

1. 在 IPAM 主控台中，選擇字首清單解析程式。

2. 選擇您在步驟 1 中建立的解析程式。
3. 在解析程式詳細資訊頁面上，選擇版本索引標籤。在這裡，您將看到解析程式已建立的所有版本，以及各版本中的所有 CIDR。
4. 在解析程式詳細資訊頁面上，選擇監控索引標籤。在此檢視中，IPAM 字首清單解析程式指標會以圖形形式顯示：
   - 字首清單解析程式版本建立成功
   - 字首清單解析程式版本建立失敗
5. 在監控索引標籤中，也可以選擇為字首清單解析程式版本建立建立警示來設定 CloudWatch 警示。系統會將您導向 CloudWatch 主控台，您會看到針對該指標的警示已完成部分設定。如需有關如何完成警示建立的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的建立基於靜態閾值的 CloudWatch 警示。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來監控版本和同步：

1. 使用 get-ipam-prefix-list-resolver-version-entries 命令來檢視解析程式建立的最新版本。
2. 使用 describe-ipam-prefix-list-resolver-targets 命令來監控解析程式目標同步狀態。

監控命令會顯示：

- state– 目前同步狀態 (建立完成、修改完成等)
- lastSyncedVersion – 上次成功同步的版本
- desiredVersion – 要同步的目標版本
- stateMessage – 同步失敗時的錯誤詳細資訊

> **Important**
>
> 為了支援轉返工作流程，IPAM 會為每個目標保留先前 10 個字首清單解析程式版本的副本；此外，如果超過此閾值的版本保留 7 天，IPAM 將會刪除這些版本。

步驟 4：(選用) 啟用和停用 IPAM 字首清單同步

如果受管字首清單已設定為 IPAM 字首清單目標，而且您想要變更字首清單，而不需要存取 IPAM 字首清單解析程式目標的許可，您可以修改受管字首清單，並停用與 IPAM 字首清單解析程式的同步。停用後，字首清單 CIDR 不會自動更新，您可以對其進行變更。啟用後，字首清單 CIDR 會根據相關聯的解析程式 CIDR 選取規則自動更新。

變更 VPC CIDR 的監控狀態

請依照本節中的步驟，變更 VPC CIDR 的監控狀態。如果您不希望 IPAM 管理或監控 VPC 並允許配置給 VPC 的 CIDR 可供使用，您可能希望將 VPC CIDR 從「已監控」變更為「已忽略」。如果您希望 IPAM 管理和監控 VPC CIDR，可能會想要將 VPC CIDR 從「已忽略」變更為「已監控」。

> **Note**
>
> - 您無法忽略公有範圍中的 VPC CIDR。
> - 如果忽略 CIDR，您仍需支付 CIDR 中作用中 IP 地址的費用。如需詳細資訊，請參閱IPAM 定價。
> - 如果忽略 CIDR，您仍然可以在 CIDR 中檢視 IP 地址的記錄。如需詳細資訊，請參閱檢視 IP 位址歷程記錄。

您可以將 VPC CIDR 的監控狀態變更為「已監控」或「已忽略」：

- Monitored (已監控)：IPAM 已偵測到 VPC CIDR，並正在監控是否與其他 CIDR 重疊和符合配置規則。
- Ignored (已忽略)：VPC CIDR 已被選擇為免於監控。不會評估已忽略的 VPC CIDR 是否與其他 CIDR 重疊或符合配置規則。若選擇忽略 VPC CIDR，從 IPAM 集區配置給該資源的任何空間都會傳回至集區，而且不會透過自動匯入再次將該 VPC CIDR 匯入 (如果已設定集區的自動匯入配置規則)。

AWS Management Console

變更配置給 VPC 之 CIDR 的監控狀態

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 Resources (資源)。

3. 請從內容窗格最上方的下拉式選單中選擇您要使用的私有範圍。
4. 在內容窗格中，選擇 VPC 並檢視該 VPC 的詳細資訊。
5. 在 VPC CIDR 下，選取配置給 VPC 的其中一個 CIDR，然後選擇動作 > 標記為已忽略或取消標記為已忽略。
6. 選擇 Mark as ignored (標記為已忽略) 或 Unmark as ignored (取消標記為已忽略)。

Command line

使用下列 AWS CLI 命令來變更 VPC CIDR 的監控狀態：

1. 取得範圍 ID：describe-ipam-scopes
2. 檢視 VPC CIDR 的目前監控狀態：get-ipam-resource-cidrs
3. 變更 VPC CIDR 的狀態：modify-ipam-resource-cidr
4. 檢視 VPC CIDR 新的監控狀態：get-ipam-resource-cidrs

建立其他範圍

請依照本節中的步驟來建立其他的範圍。

範圍是 IPAM 內最高層級的容器。建立 IPAM 時，IPAM 會為您建立兩個預設範圍。每個範圍代表單一網路的 IP 空間。私有範圍適用於所有私有空間。公有範圍適用於所有公有空間。範圍可讓您在多個未連線的網路上重複使用 IP 地址，而不會造成 IP 地址重疊或衝突。

建立 IPAM 時，會為您建立預設範圍 (一個私有和一個公有)。您可建立其他的私有範圍。您無法建立其他的公有範圍。

如果您需要支援多個中斷連線的私有網路，您可以建立其他的私有範圍。其他私有範圍可允許您建立集區，並管理使用相同 IP 空間的資源。

> **Important**
>
> 如果 IPAM 發現具有私有 IPv4 或私有 IPv6 CIDR 的資源，則資源 CIDR 會匯入預設的私有範圍，而且不會出現在您建立的任何其他私有範圍中。您可以將 CIDR 從預設的私有範圍移至另一個私有範圍。如需相關資訊，請參閱 在各範圍之間移動 VPC CIDR。

AWS Management Console

建立其他私有範圍

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 Scopes (範圍)。
3. 選擇 Create scope (建立範圍)。
4. 選擇您要新增範圍的 IPAM。
5. 新增範圍的描述。
6. 選擇 Create scope (建立範圍)。
7. 您可以在導覽窗格中選擇 Scopes (範圍) 來檢視 IPAM 中的範圍。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來建立額外的私有範圍：

1. 檢視目前的範圍：describe-ipam-scopes
2. 建立新的私有範圍：create-ipam-scope
3. 檢視您目前的範圍以檢視新的範圍：describe-ipam-scopes

刪除 IPAM

如果不再需要 IPAM、需要重組 IP 位址管理，或者想要開始使用新的 IPAM 組態，您可能想要刪除 IPAM。刪除 IPAM 有助於簡化 IP 位址管理，並滿足不斷變化的業務或營運需求。

請依照本節中的步驟來刪除 IPAM。如需有關增加可擁有的 IPAM 預設數量而非刪除現有 IPAM 的資訊，請參閱 IPAM 的配額。

> **Note**
>
> 若刪除 IPAM，會移除與 IPAM 相關聯的所有監控資料，包括 CIDR 的歷史資料。

AWS Management Console

刪除 IPAM

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 IPAMs。
3. 在內容窗格中，選取 IPAM。
4. 選擇 Actions (動作) > Delete IPAM (刪除 IPAM)。
5. 執行以下任意一項：

   - 選擇 Cascade delete (串聯刪除) 刪除 IPAM、私有範圍、私有範圍中的集區，以及私有範圍中集區的任何分配。如果您的公有範圍中存在集區，則無法使用此選項刪除 IPAM。如果使用此選項，則 IPAM 會執行以下操作：
     - 在私有範圍的集區中取消分配已分配給 VPC 資源 (如 VPC) 的所有 CIDR。

       > **Note**
       >
       > 啟用此選項後，不會刪除任何 VPC 資源。與資源關聯的 CIDR 將不再從 IPAM 集區中分配，但 CIDR 本身會保持不變。

     - 取消佈建已佈建至私有範圍中 IPAM 集區的所有 IPv4 CIDR。
     - 刪除私有範圍中的所有 IPAM 集區。
     - 刪除 IPAM 中的所有非預設私有範圍。
     - 刪除預設公有和私有範圍以及 IPAM。
   - 在刪除 IPAM 前，如果沒有選擇 Cascade delete (串聯刪除) 核取方塊，則您必須執行下列操作：
     - 釋出 IPAM 集區內的配置。如需詳細資訊，請參閱 釋出配置。
     - 取消佈建已佈建至 IPAM 內集區的 CIDR。如需詳細資訊，請參閱從集區解除佈建 CIDR。
     - 刪除任何其他非預設範圍。如需詳細資訊，請參閱刪除範圍。
     - 刪除 IPAM 集區。如需詳細資訊，請參閱刪除集區。
6. 輸入 **`delete`**，然後選擇 Delete (刪除)。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來刪除 IPAM：

1. 檢視目前的 IPAM：describe-ipams
2. 刪除 IPAM：delete-ipam
3. 檢視已更新的 IPAM：describe-ipam

若要建立新 IPAM，請參閱 建立 IPAM。

刪除集區

中的 IPAM 集區 AWS 代表可在特定 AWS 環境或組織中配置和管理的已定義 IP 地址範圍。集區用於組織 IP 位址空間、啟用自動化 IP 位址管理，以及在整個雲端基礎設施中強制執行 IP 位址控管政策。

您可能想要刪除某個 IPAM 集區，以移除未使用的或不必要的 IP 位址空間，並將其回收以用於其他目的。如果 IP 地址集區中有配置，則無法刪除 IP 地址集區。您必須先釋放配置和 從集區解除佈建 CIDR，然後才能刪除集區。

請依照本節中的步驟來刪除 IPAM 集區。

AWS Management Console

刪除集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 在內容窗格最上方的下拉式選單中，選擇想要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 在內容窗格中，選擇您要刪除其 CIDR 的集區。
5. 選擇 Actions (動作) > Delete pool (刪除集區集區)。
6. 輸入 **`delete`**，然後選擇 Delete (刪除)。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來刪除集區：

1. 檢視集區並取得 IPAM 集區 ID：describe-ipam-pools
2. 刪除集區：delete-ipam-pool
3. 檢視集區：describe-ipam-pools

若要建立新集區，請參閱 建立頂層 IPv4 集區。

刪除範圍

如果某個 IPAM 範圍不再符合其預期目的 (例如當您重組網路、合併區域或調整 IP 位址配置時)，您可能會想要刪除該範圍。刪除未使用的範圍有助於簡化 IPAM 組態，並最佳化 AWS中的 IP 位址管理。

> **Note**
>
> 如果以下任一情況為真，則無法刪除範圍：
>
> - 範圍是預設範圍。建立 IPAM 時，會自動建立兩個預設範圍 (一個公有、一個私有)，且無法刪除。若要查看範圍是否為預設範圍，請檢視範圍詳細資訊中的 Scope type (範圍類型)。
> - 範圍中有一或多個集區。您必須先 刪除集區，然後才能刪除範圍。

AWS Management Console

刪除範圍

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 Scopes (範圍)。
3. 在內容窗格中，選擇您要刪除的範圍。
4. 選擇 Actions (動作) > Delete scope (刪除範圍)。
5. 輸入 **`delete`**，然後選擇 Delete (刪除)。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來刪除範圍：

1. 檢視範圍：describe-ipam-scopes

2. 刪除範圍：delete-ipam-scope
3. 檢視更新的範圍：describe-ipam-scopes

若要建立新範圍，請參閱 建立其他範圍。若要刪除 IPAM，請參閱 刪除 IPAM。

從集區解除佈建 CIDR

您可能想要解除佈建集區 CIDR，以釋放 IP 位址空間、簡化 IP 位址管理、準備進行網路變更，或滿足合規要求。解除佈建集區 CIDR 可讓您在 IPAM 內更好地控制和最佳化 IP 位址配置，同時確保回收未使用的 IP 空間供日後使用。如果集區中有配置，則無法解除佈建 CIDR。若要移除配置，請參閱 the section called “釋出配置”。

請依照本節中的步驟，從 IPAM 集區解除佈建 CIDR。當您取消佈建所有集區 CIDR 時，集區將無法再用於配置。您必須先將新的 CIDR 佈建至集區，才能使用集區進行配置。

AWS Management Console

取消佈建集區 CIDR

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 在內容窗格最上方的下拉式選單中，選擇想要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 在內容窗格中，選擇您要取消佈建其 CIDR 的集區。
5. 選擇 CIDRs 索引標籤。
6. 選取一或多個 CIDR，然後選擇 Deprovision CIDRs (取消佈建 CIDR)。
7. 選擇 Deprovision CIDR (取消佈建 CIDR)。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來取消佈建集區 CIDR：

1. 取得 IPAM 集區 ID：describe-ipam-pools
2. 檢視集區目前的 CIDR：get-ipam-pool-cidrs

3. 取消佈建 CIDR：deprovision-ipam-pool-cidr
4. 檢視已更新的 CIDR：get-ipam-pool-cidrs

若要將新的 CIDR 佈建至集區，請參閱 從集區解除佈建 CIDR。若要刪除集區，請參閱 刪除集區。

編輯 IPAM 集區

您可能想要編輯集區以執行下列其中一項作業：

- 變更集區的配置規則。如需有關分配規則的詳細資訊，請參閱建立頂層 IPv4 集區。
- 修改集區的名稱、說明或其他中繼資料，以改善 IPAM 中的組織和可見性。
- 變更集區選項，例如自動匯入發現的資源，以最佳化 IPAM 的自動化 IP 位址管理。

請依照本節中的步驟來編輯 IPAM 集區。

AWS Management Console

編輯集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 按預設，會選取預設的私有範圍。如果不想使用預設的私有範圍，請從內容窗格最上方的下拉式選單中選擇您要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式
4. 在內容窗格中，選擇您要編輯其 CIDR 的集區。
5. 選擇 Actions (動作) > Edit (編輯)。
6. 對集區進行您需要的任何變更。如需集區組態選項的詳細資訊，請參閱 建立頂層 IPv4 集區。
7. 選擇 Update (更新)。

Command line

使用下列 AWS CLI 命令來編輯集區：

1. 取得 IPAM 集區 ID：describe-ipam-pools
2. 修改集區：modify-ipam-pool

啟用成本分配

啟用成本分配後，作用中 IP 位址的費用將分配給使用這些 IP 位址的帳戶，而不是 IPAM 擁有者。這對於委派 IPAM 管理員使用 IPAM 集中管理 IP 位址的大型組織很有用，每個帳戶都負責自己的使用量，因此不需要手動計算帳單費用。

在計量模式下建立 IPAM 或修改 IPAM 時，可以使用成本分配選項，其中：

- IPAM 擁有者 (預設)：擁有 IPAM 的 AWS 帳戶需為 IPAM 中管理的所有作用中 IP 位址付費。
- 資源擁有者：擁有 IP 位址的 AWS 帳戶需為作用中 IP 位址付費。

要求

- 您的 IPAM 必須與 AWS Organizations 整合。
- IPAM 必須由 AWS Organizations 中的委派 IPAM 管理員建立。
- IPAM 的主要區域必須是預設啟用的區域，不能是選擇加入區域。

費用分配的運作方式

- 雖然您可以在組織內分配 IP 位址費用，但透過 AWS Organizations 合併帳單功能，所有 IPAM 費用仍會合併到組織的付款人帳戶。
- 啟用成本分配後，組織成員帳戶仍然可以在其帳戶帳單中檢視個別 IPAM 用量與費用。
- 啟用成本分配後，IPAM ARN 會出現在個別帳戶帳單上，這讓資源擁有者可以追蹤其 IPAM 作用中 IP 用量。如果您使用 AWS 資料匯出，IPAM 費用會在合併帳戶帳單和個別帳戶帳單中與相關聯的 IPAM ARN 一起顯示。
- 只有委派管理員組織內的帳戶才會被收取所擁有資源的費用。組織外部的 IP 位址費用會向 IPAM 擁有者收取。

時間限制

- 啟用成本分配後，您有 24 小時可選擇退出。24 小時後將無法變更設定 7 天。7 天後可停用成本分配功能。

將 VPC IPAM 與 Infoblox 基礎設施整合

Amazon VPC IPAM 和 Infoblox 整合會將 AWS VPC IP Address Manager (IPAM) 與 Infoblox 連線，讓您能夠透過現有的 Infoblox 工作流程管理 AWS IP 地址，同時取得雲端原生 AWS 功能。

此整合解決了常見的企業挑戰：避免重複的 IP 管理系統。您可以指定 Infoblox 做為 VPC IPAM 範圍的管理授權單位，並繼續在所有 IP 地址操作中使用熟悉的 Infoblox 介面，而不是學習新工具 AWS 和維護個別的程序。

整合程序概觀

下列步驟提供完整整合程序的概觀：

1. 設定 IPAM 範圍（本文件所述）：Amazon VPC IPAM 委派管理員建立新的範圍，或修改現有範圍以使用 Infoblox 做為其外部授權。
2. 設定 Infoblox（本文件外部說明）：請參閱 後續步驟。
3. 建立最上層集區：Amazon VPC IPAM 委派管理員會在連結到 Infoblox 的範圍內建立集區。集區會從未指派 CIDR 開始。
4. 從外部授權機構佈建 CIDR：Amazon VPC IPAM 委派管理員為集區佈建 CIDR。您可以請求任何可用的 CIDR (Infoblox 從允許的範圍中選擇） 或請求特定的 CIDR (Infoblox 根據可用性接受或拒絕）。IPAM 會自動與 Infoblox 協調，以取得和佈建核准的 CIDR。
5. 繼續進行標準 IPAM 操作：使用標準 Amazon VPCs從配置的 CIDR 建立子集區和 VPC。

何時使用此整合

如果您已經使用或計劃使用 Infoblox 進行內部部署網路管理，並希望將現有的 IP 管理實務擴展到 ，AWS 而無需維護單獨的系統，請使用此整合。

先決條件

在設定此整合之前，請確定您有：

- VPC IPAM 進階方案：已在您的帳戶中啟用 AWS 。如需詳細資訊，請參閱 VPC IPAM 進階方案。
- 必要的 IAM 許可：如下所列
- Infoblox 資源識別符：來自 Infoblox 管理員

Infoblox 的 IAM 角色

為要擔任的 Infoblox 主體建立 IAM 角色，或使用現有角色。此角色需要這些許可：

- `ec2:DescribeIpamPools`
- `ec2:DescribeIpams`
- `ec2:DescribeIpamScopes`
- `ec2:GetIpamPoolAllocations`
- `ec2:GetIpamPoolCidrs`
- `ec2:GetIpamResourceCidrs`

如需如何將這些許可新增至 IAM 角色或政策的說明，請參閱《IAM 使用者指南》中的新增和移除 IAM 身分許可。

> **Note**
> 除了啟用此整合所需的這些許可之外，Infoblox 可能需要 VPC IPAM 探索的許可。

在 VPC IPAM 中設定 Infoblox 整合

您可以在 AWS VPC IPAM 主控台或 中建立或修改範圍時啟用 Infoblox 整合 AWS CLI。

> **Important**
> Infoblox 整合僅適用於私有範圍，不適用於公有範圍。

使用 Infoblox 整合建立新範圍

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 IPAM，然後選擇範圍。
3. 選擇 Create scope (建立範圍)。
4. 對於範圍設定，請執行下列動作：
   - IPAM ID 會自動填入。

- （選用）針對名稱標籤，輸入範圍的名稱。
- （選用）針對描述，輸入範圍的描述。

5. 針對範圍授權單位，選擇 Infoblox IPAM。
6. 針對 Infoblox 資源識別符，以 格式輸入 Infoblox 資源識別符`<version>.identity.account.<entity_realm>.<entity_id>`。
7. 確認您具有資訊方塊中顯示的所需 IAM 許可。
8. 選擇 Create scope (建立範圍)。

此的相關 AWS CLI 命令是 create-ipam-scope。

修改現有範圍

若要將現有範圍的範圍授權機構從 Amazon VPC IPAM 變更為 Infoblox IPAM，請編輯範圍設定，並遵循先前程序中相同的組態步驟。

此的相關 AWS CLI 命令是 modify-ipam-scope。

後續步驟

如此即完成整合所需的 Amazon VPC IPAM 組態。設定範圍授權機構後，您可以在範圍內建立頂層 IPAM 集區。如需詳細資訊，請參閱建立頂層 IPv4 集區。

整合還需要設定 Infoblox 來源集區、驗證探索任務狀態、設定由 Infoblox 管理的私有範圍、啟用 Amazon VPC IPAM 的 Infoblox 管理，以及從 Infoblox 整合或直接從 Infoblox 入口網站建立集區。

如需有關整合的 Infoblox 端的資訊，請參閱 Infoblox 文件中的 AWS IPAM 整合使用者指南。

啟用佈建私有 IPv6 GUA CIDR

如果您希望私有網路支援 IPv6，且無意將流量從這些位址路由到網際網路，可以將私有 IPv6 ULA 或 GUA 範圍佈建至私有範圍內的 IPAM 集區。

如需有關私有 IPv6 定址的重要詳細資訊，請參閱《Amazon VPC 使用者指南》中的私有 IPv6 地址。

私有 IPv6 地址有兩種類型：

- IPv6 ULA 範圍：RFC4193 中定義的 IPv6 地址。這些位址範圍一律以 “fc” 或 “fd” 開頭，以便它們易於識別。有效的 IPv6 ULA 空間為 fd00::/8 下不與 Amazon 保留範圍 fd00::/16 重疊的任何空間。

- IPv6 GUA 範圍：RFC3587 中定義的 IPv6 地址。使用 IPv6 GUA 範圍做為私有 IPv6 地址的選項預設為停用，必須先啟用才能使用。

若要使用 IPv6 ULA 位址範圍，請在將 CIDR 佈建至 IPAM 集區時選擇 IPv6 選項，然後輸入 IPv6 ULA 範圍。不過，若要使用您自己的 IPv6 GUA 範圍做為私有 IPv6 地址，您必須先完成本節中的步驟。依預設，此選項為停用。

> **Note**
>
> - 當您使用私有 IPv6 GUA 範圍時，您需要使用自己擁有的 IPv6 GUA 範圍。
> - IPAM 會發現使用 IPv6 ULA 和 GUA 地址的資源，並監控集區是否有重疊的 IPv6 ULA 和 GUA 地址空間。
> - 如果想要從使用私有 IPv6 地址的資源連線至網際網路，您雖然可以連線，但必須透過另一個子網路中的資源路由流量，並使用公有 IPv6 地址來完成。
> - 如果您的私有 IPv6 GUA 範圍已配置給 VPC，則無法使用與相同 VPC 中的私有 IPv6 GUA 空間重疊的公有 IPv6 GUA 空間。
> - 支援使用私有 IPv6 ULA 和 GUA 地址範圍的資源之間的通訊 (例如跨 Direct Connect、VPC 互連、轉換閘道或 VPN 連接)。
> - 私有 GUA IPv6 範圍無法轉換為公開公告的 IPv6 GUA 範圍。

AWS Management Console

啟用佈建私有 IPv6 GUA CIDR

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 IPAMs。
3. 選擇 IPAM，然後選擇 動作 > 編輯。
4. 在 私有 IPv6 GUA CIDR 下，選擇 啟用將 GUA CIDR 空間佈建至私有 IPv6 IPAM 集區。
5. 選擇儲存變更。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

使用以下 AWS CLI 命令來啟用佈建私有 IPv6 GUA CIDR：

1. 使用 describe-ipams 檢視目前的 IPAM
2. 使用 modify-ipam 修改 IPAM，並將選項納入 `enable-private-gua`。

啟用此選項以佈建私有 IPv6 GUA CIDR 後，您可以將私有 IPv6 GUA CIDR 佈建至集區。如需更多詳細資訊，請參閱 佈建集區的 CIDR。

使用 SCP 強制使用 IPAM 建立 VPC

> **Note**
>
> 本節僅適用於已啟用 IPAM 與 整合的情況 AWS Organizations。如需詳細資訊，請參閱將 IPAM 與 AWS Organizations 中的帳戶整合。

本節說明如何在 中建立服務控制政策 AWS Organizations ，要求組織中的成員在建立 VPC 時使用 IPAM。服務控制政策 (SCP) 是一種組織政策類型，可用來管理組織中的許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。

強制使用 IPAM 建立 VPC

請依照本節中的步驟來要求組織中的成員使用 IPAM 建立 VPC。

建立 SCP 並限制為使用 IPAM 建立 VPC

1. 請遵循 AWS Organizations User Guide 中的 Create a service control policy 的步驟進行操作，在 JSON 編輯器中輸入以下文字：

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
       "Effect": "Deny",
        "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
        "Resource": "arn:aws:ec2:*:*:vpc/*",
        "Condition": {
```

```
            "Null": {
                "ec2:Ipv4IpamPoolId": "true"
            }
        }
     }]
}
```

2. 將政策連接至組織中的一個或多個組織單位。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的連接政策與分離政策。

強制使用 IPAM 集區建立 VPC

請依照本節中的步驟來要求組織中的成員使用特定 IPAM 集區建立 VPC。

建立 SCP 並限制為使用 IPAM 集區建立 VPC

1. 請遵循 AWS Organizations User Guide 中的 Create a service control policy 的步驟進行操作，在 JSON 編輯器中輸入以下文字：

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Deny",
        "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
        "Resource": "arn:aws:ec2:*:*:vpc/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Ipv4IpamPoolId": "ipam-pool-0123456789abcdefg"
            }
          }
    }]
}
```

2. 將 `ipam-pool-0123456789abcdefg` 範例值變更為您想要限制使用者存取的 IPv4 集區 ID。
3. 將政策連接至組織中的一個或多個組織單位。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的連接政策與分離政策。

針對指定 OU 清單以外的所有 OU 強制執行 IPAM

請遵循本節中的步驟，針對指定組織單位 (OU) 清單以外的所有 OU 強制執行 IPAM。本節所述的政策需要組織中OUs，但您在 中指定的 OUs 除外，`aws:PrincipalOrgPaths`才能使用 IPAM 來建立和展開 VPCs。列出的 OU 可以在建立 VPC 時使用 IPAM，或手動指定 IP 地址範圍。

針對指定 OU 清單以外的所有 OU 建立 SCP 並強制執行 IPAM

1. 請遵循 AWS Organizations User Guide 中的 Create a service control policy 的步驟進行操作，在 JSON 編輯器中輸入以下文字：

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
 "Effect": "Deny",
     "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
     "Resource": "arn:aws:ec2:*:*:vpc/*",
     "Condition": {
         "Null": {
        "ec2:Ipv4IpamPoolId": "true"
                },
         "ForAnyValue:StringNotLike": {
             "aws:PrincipalOrgPaths": [
                 "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/",
                 "o-a1b2c3d4e5/r-ab12/ou-ab13-22222222/ou-ab13-33333333/"
             ]
                }
            }
     }]
}
```

2. 移除範例值（例如 `o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/`），並新增您想要有使用 IPAM 選項（但不需要）之 OUs 的 AWS Organizations 實體路徑。如需實體路徑的詳細資訊，請參閱《IAM 使用者指南》中的了解 AWS Organizations 實體路徑和 aws：PrincipalOrgPaths。
3. 將此政策連接至組織根目錄。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的連接政策與分離政策。

從 IPAM 排除組織單位

如果您的 IPAM 已與 AWS Organizations 整合，您可以排除由 IPAM 管理的組織單位 (OU)。排除組織單位後，IPAM 就不會管理該組織單位帳戶中的 IP 位址。此功能可讓您更靈活地使用 IPAM。

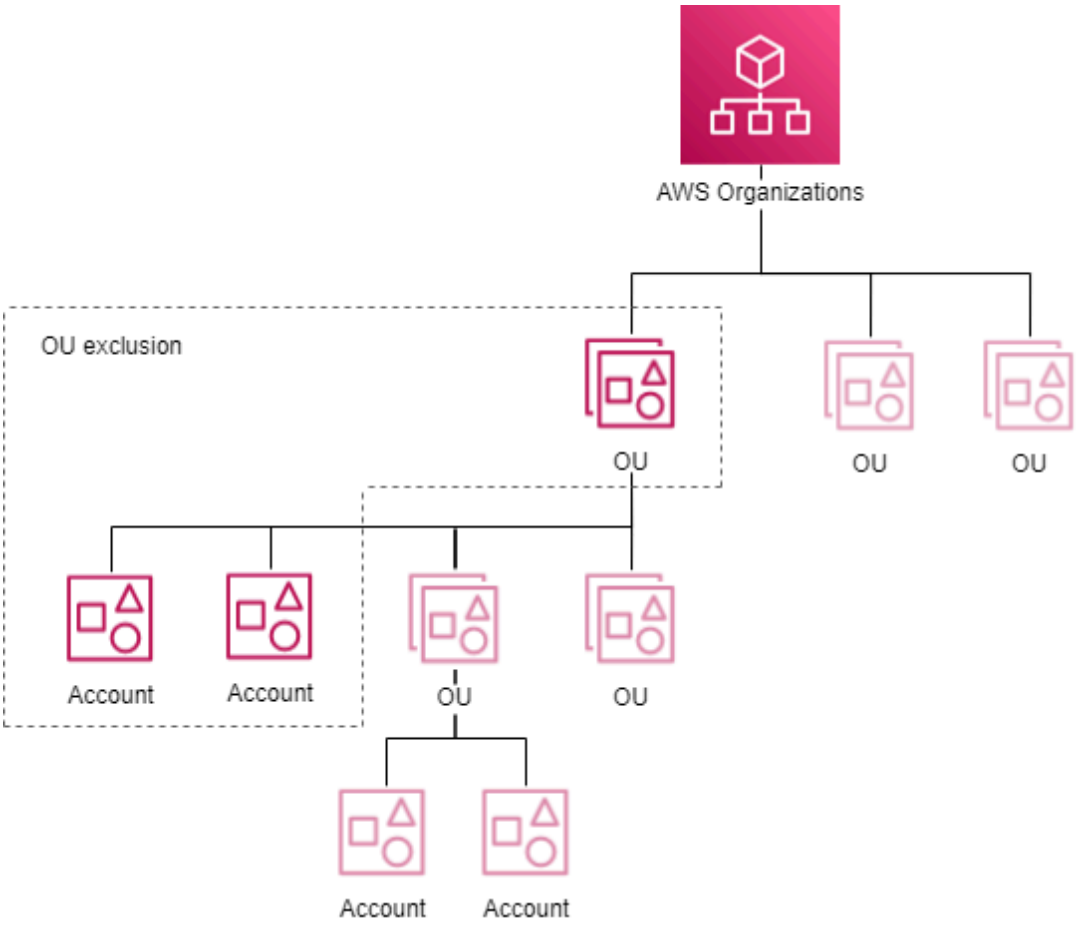
您可以透過以下方式使用 OU 排除：

- 為業務的特定部分啟用 IPAM：如果您在 AWS Organizations 中多個業務部門或子公司，您現在可以只為需要的部門使用 IPAM。
- 保持沙盒帳戶分離：您可以將沙盒帳戶排除在 IPAM 之外，只專注於對 IP 管理真正重要的帳戶。

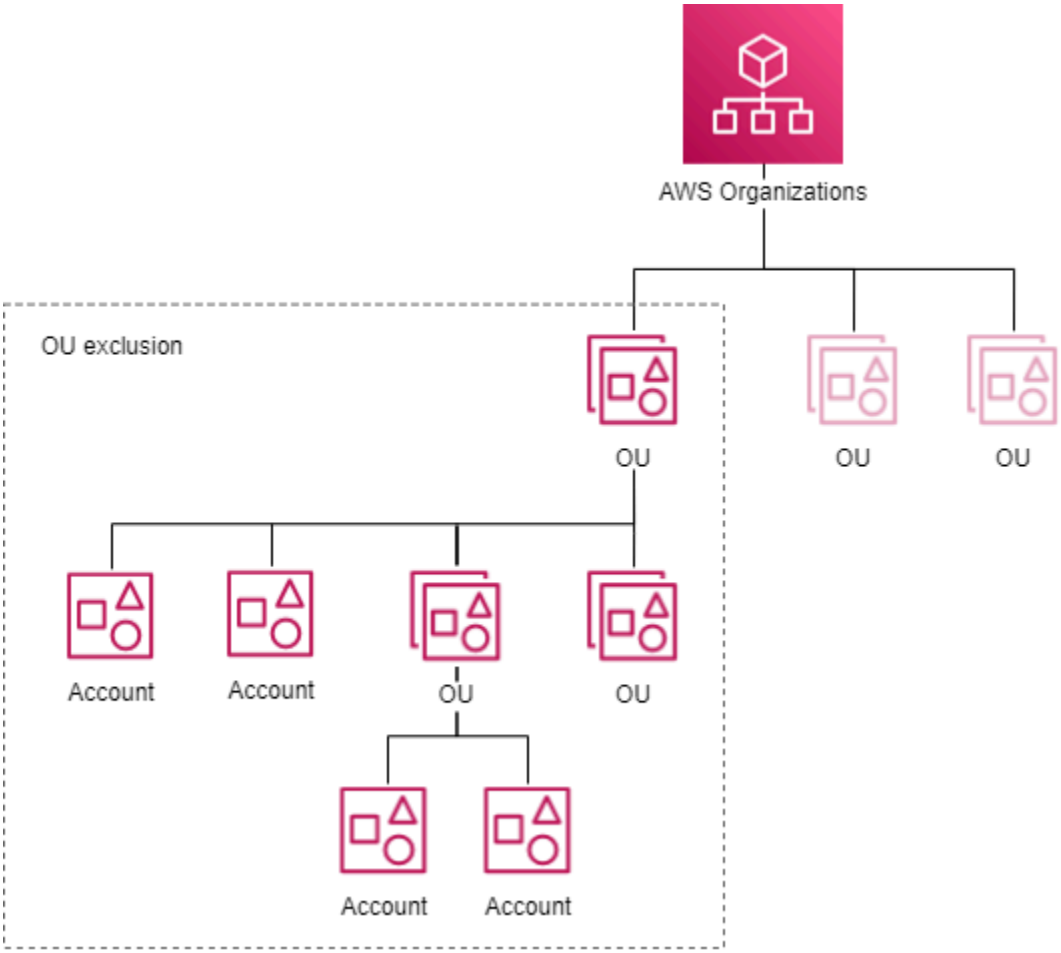
OU 排除的運作方式

本節中的圖表示範了在 IPAM 中新增組織單位排除的兩個使用案例。

第一個圖表顯示僅在父級 OU 上新增組織單位 (OU) 排除的影響。結果是，IPAM 不會管理父級 OU 中帳戶的 IP 位址。IPAM 會管理其他不在排除範圍內的 OU 中帳戶的 IP 位址。



第二個圖表顯示在父級 OU 和所有子級 OU 上新增組織單位 (OU) 排除的影響。結果是，IPAM 不會管理父級 OU 中帳戶的 IP 位址，也不會管理任何子級 OU 中帳戶的 IP 位址。IPAM 仍然會管理不在排除範圍內的其他 OU 中帳戶的 IP 位址。



新增或移除 OU 排除

完成本節中的步驟，以新增或移除 OU 排除。

> **Note**
>
> - 即使委派的 IPAM 管理帳戶位於已排除的 OU 中，也不會被排除。
> - 您的 IPAM 必須與 整合 AWS Organizations ，才能新增 OU 排除。組織中必須有 OU。
> - 您必須是委派 IPAM 管理員，才能檢視、新增或移除 OU 排除。
> - IPAM 需要一些時間來發現最近建立的組織單位。
> - 每次資源發現會有一個預設配額，限制您能夠新增的排除數量。如需詳細資訊，請參閱 IPAM 的配額中每個資源發現的組織單位排除。

- 如果您將資源探索共享給另一個帳戶，則該帳戶可以看到與資源發現相關的組織單位排除，並能查看其中包含的資源發現擁有者的組織 ID、根 ID 以及組織單位 ID 等資訊。

AWS Management Console

新增或移除 OU 排除

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇尋找探索。
3. 選擇預設資源發現。
4. 選擇編輯。
5. 在 組織單位排除 下，執行以下操作：
   - 新增 OU 排除：
     - 如果要排除 OU 及其所有子級 OU：
       - 在資料表中尋找 OU，然後選取核取方塊。系統會自動選取所有子級 OU。
     - 如果只想要排除父級 OU 帳戶：
       - 在資料表中尋找 OU，然後選取核取方塊。系統會自動選取所有子級 OU。取消選取所有子級 OU。
     - 或者，您可以使用動作欄來僅選取父級 OU，或父級和子級 OU：
       - 選取所有子級 OU：在排除範圍中包含所有子級 OU。選擇一個 OU 之後，該 OU 會被顯示在畫面上。每個 OU 都包含該 OU 排除的 ID 和實體路徑。
       - 僅選取此 OU：在排除範圍中僅包含此 OU。選擇一個 OU 之後，該 OU 會被顯示在畫面上。每個 OU 都包含該 OU 排除的 ID 和實體路徑。
       - 複製組織單位實體路徑：視需要複製要使用的組織實體路徑。
     - 如果您已經知道 AWS Organizations 實體路徑，或想要建置它：
       - 選擇 輸入組織單位排除，然後輸入 OU 排除的實體路徑。使用 AWS Organizations ID 建立 OU 路徑，並以 / 分隔。若要包含所有子級 OU，請將路徑結尾加上 /*。
         - 範例 1
           - 子級 OU 的路徑：`o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsdddddd/`

- 在此範例中，o-a1b2c3d4e5 是組織 ID，r-f6g7h8i9j0example 是根 ID，ou-ghi0-awsccccc 是組織單位 ID，ou-jkl0-awsdddddd 是子組織單位 ID。
- IPAM 不會管理子級 OU 中帳戶的 IP 位址。

- 範例 2
  - 所有子級 OU 都包含在排除範圍內的路徑：o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*
  - 在此範例中，IPAM 不會管理 OU (ou-ghi0-awsccccc) 中帳戶的 IP 位址，也不會管理任何其子級 OU 中帳戶的 IP 位址。

- 移除 OU 排除：
  - 選擇已新增的 OU 旁的 X。OU ID 後的 /* 表示它是父級 OU，並且其子級 OU 在排除範圍內。

6. 選擇儲存變更。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

1. 使用 describe-ipam-resource-discoveries 查看資源發現詳細資訊，以取得預設資源發現的 ID 供後續步驟使用。

   輸入:

```
aws ec2 describe-ipam-resource-discoveries
```

   輸出：

```
{

    "IpamResourceDiscoveries": [

        {

            "OwnerId": "111122223333",

            "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",
```

```
            "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-
resource-discovery/ipam-res-disco-1234567890abcdef0",
            "IpamResourceDiscoveryRegion": "us-east-1",

            "OperatingRegions": [

                {

                    "RegionName": "us-east-1"

                },

                {

                    "RegionName": "us-west-1"

                },

                {

                    "RegionName": "us-west-2"

                }

            ],

            "IsDefault": true,

            "State": "modify-complete",

            "Tags": []

        }

    ]

}
```

2. 使用 modify-ipam-resource-discovery 以及 `--add-organizational-unit-exclusions` 或 `--remove-organizational-unit-exclusions` 選項，在資源發現中新增或移除組織單位排除。您需要輸入 AWS Organizations 實體路徑。使用以 分隔 AWS 的組織 IDs 來建置

OU 的路徑 (OU)/。若要包含所有子級 OU，請將路徑結尾加上 /*。無法在新增或移除參數中多次包含相同的實體路徑。

- 範例 1
  - 子級 OU 的路徑：o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/
  - 在此範例中，o-a1b2c3d4e5 是組織 ID，r-f6g7h8i9j0example 是根 ID，ou-ghi0-awsccccc 是組織單位 ID，ou-jkl0-awsddddd 是子組織單位 ID。
  - IPAM 不會管理子級 OU 中帳戶的 IP 位址。
- 範例 2
  - 所有子級 OU 都包含在排除範圍內的路徑：o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*
  - 在此範例中，IPAM 不會管理 OU (ou-ghi0-awsccccc) 中帳戶的 IP 位址，也不會管理任何其子級 OU 中帳戶的 IP 位址。

> **Note**
>
> 產生的排除項目集不得「重疊」，這表示兩個或多個組織單位排除項目不得排除相同的組織單位。
> 非重疊實體路徑的範例：
>
> - 路徑 1 ="o-1/r-1/ou-1/"
> - 路徑 2 ="o-1/r-1/ou-1/ou-2/"
>
> 這些路徑不重疊，因為路徑 1 僅排除 ou-1 下的帳戶，而路徑 2 僅排除 ou-2 下的帳戶。
> 重疊實體路徑的範例：
>
> - 路徑 1 ="o-1/r-1/ou-1/*"
> - 路徑 2 ="o-1/r-1/ou-1/ou-2/"
>
> 這些路徑重疊，因為路徑 1 同時代表 "o-1/r-1/ou-1/" 和 "o-1/r-1/ou-1/ou-2/"，而 "o-1/r-1/ou-1/ou-2/" 與路徑 2 重疊。

輸入:

```
aws ec2 modify-ipam-resource-discovery \
    --ipam-resource-discovery-id ipam-res-disco-1234567890abcdef0 \
    --add-organizational-unit-exclusions OrganizationsEntityPath='o-a1b2c3d4e5/
r-f6g7h8i9j0example/ou-ghi0-awsccccc/*' \
    --remove-organizational-unit-exclusions OrganizationsEntityPath='o-
a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/' \
    --region us-east-1
```

輸出：

```
{
    "IpamResourceDiscovery": {
        "OwnerId": "111122223333",
        "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-resource-
discovery/ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryRegion": "us-east-1",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "IsDefault": false,
        "State": "modify-in-progress",
        "OrganizationalUnitExclusions": [
            {
                "OrganizationsEntityPath": "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-
ghi0-awsccccc/*"
            }
        ]
    }
}
```

修改 IPAM 方案

IPAM 提供兩種方案：免費方案和進階方案。切換到 Amazon VPC IP 位址管理員的進階方案可讓您更精細地控制 IP 位址管理。隨著網路複雜性的增加，這會有所助益，讓您更好地最佳化和管理 IP 位址空

間。如需免費方案中的可用功能以及進階方案關聯成本的詳細資訊，請參閱 Amazon VPC 定價頁面中的 IPAM 索引標籤。

> **Note**
>
> 在可以從進階方案切換至免費方案之前，必須：
>
> - 刪除私有範圍集區。
> - 刪除非預設的私有範圍。
> - 刪除地區設定不同於 IPAM 主區域的集區。
> - 刪除非預設資源探索關聯。
> - 刪除非 IPAM 擁有者帳戶的集區配置。

AWS Management Console

修改 IPAM 方案

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 IPAMs。
3. 在內容窗格中，選取 IPAM。
4. 選擇 Actions (動作) > Edit (編輯)。

> **Note**
>
> 如果您使用的是免費方案，您會看到預估 IPAM 作用中 IP 總數為...。
> 如果從免費方案切換到進階方案，則作用中 IP 總計數即為 IPAM 中需要支付費用的作用中 IP 位址的數量。作用中的 IP 位址是指與附加到 EC2 執行個體等資源的彈性網絡介面 (ENI) 關聯的 IP 位址或字首。
>
> - 此指標僅適用於免費方案客戶。
> - 如果您的 IPAM 已與 AWS Organizations 整合，則作用中 IP 計數會涵蓋所有 Organization 帳戶。
> - 您無法依 IP 類型 (公有/私有) 或類別 (IPv4/IPv6) 檢視作用中 IP 計數的明細。
> - IPAM 只計算由受監控帳戶擁有的 ENI 中的 IP 位址數量。共用子網路的計數可能不準確。如果 IPAM 未涵蓋子網路擁有者或 ENI 擁有者，則 IP 位址會被排除在外。

5. 選擇要用於 IPAM 的 IPAM tier (IPAM 方案)。
6. 選擇儲存變更。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來檢視和修改 IPAM 層：

1. 檢視目前的 IPAM：describe-ipams
2. 修改 IPAM 方案：modify-ipam
3. 檢視已更新的 IPAM：describe-ipam

修改 IPAM 作業區域

操作區域是允許 IPAM 管理 IP 地址 CIDRs AWS 的區域。IPAM 只會探索和監控您選取做為操作 AWS 區域的區域中的資源。

將操作區域新增至 IPAM 可讓您管理跨多個 AWS 區域的 IP 地址空間。這可以改善 IP 位址利用率、實現區域分割，並支援地理分散式基礎設施。擴充 IPAM 的區域範圍可為您的整體 IP 位址管理提供更高的靈活性和更大的控制力。

AWS Management Console

修改 IPAM 作業區域

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 IPAMs。
3. 在內容窗格中，選取 IPAM。
4. 選擇 Actions (動作) > Edit (編輯)。
5. 在 IPAM settings (IPAM 設定) 下，選擇要用於 IPAM 的 Operating Regions (作業區域)。
6. 選擇儲存變更。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來檢視和修改 IPAM 作業系統區域：

1. 檢視目前的 IPAM：describe-ipams
2. 新增或移除 IPAM 作業區域：modify-ipam
3. 檢視已更新的 IPAM：describe-ipam

佈建集區的 CIDR

請依照本節中的步驟來佈建集區 的 CIDR。如果在建立集區時已佈建 CIDR，則可能需要在集區已將近全數配置完畢時佈建其他 CIDR。若要監控集區使用情況，請參閱 使用 IPAM 儀表板監控 CIDR 使用情況。

> **Note**
>
> 本使用者指南和 IPAM 主控台中不時會使用佈建和配置等專有名詞。佈建是指在 IPAM 集區中新增 CIDR。將 IPAM 集區中的 CIDR 與 VPC 或彈性 IP 地址建立關聯時，會使用配置。

AWS Management Console

佈建集區的 CIDR

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 按預設，會選取預設的私有範圍。如果不想使用預設的私有範圍，請從內容窗格最上方的下拉式選單中選擇您要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 在內容窗格中，選擇您要在哪個集區中新增 CIDR。
5. 選擇 Actions (動作) > Provision CIDRs (佈建 CIDR)。
6. 執行以下任意一項：
   - 如果您要將 CIDR 佈建至公有範圍內的集區，請輸入 網路遮罩。
   - 如果您要將 CIDR 佈建至私有範圍內的 IPv4 集區，請輸入 CIDR。
   - 如果您要將 CIDR 佈建至私有範圍內的 IPv6 集區，請注意下列事項：
     - 如需有關私有 IPv6 定址的重要詳細資訊，請參閱《Amazon VPC 使用者指南》中的私有 IPv6 地址。

- 若要使用私有 IPv6 ULA 範圍，請在佈建的 CIDR 下，選擇透過網路遮罩新增 ULA CIDR，然後選擇網路遮罩大小，或選擇輸入私有 IPv6 CIDR 並輸入 ULA 範圍。私有 IPv6 ULA 的有效範圍為 /9 到 /60，開頭為 fd80::/9。
- 若要使用私有 IPv6 GUA 範圍，您必須先在 IPAM 上啟用此選項 (請參閱啟用佈建私有 IPv6 GUA CIDR)。啟用私有 IPv6 GUA CIDRs 後，請在 輸入私有 IPv6 CIDR 中輸入 IPv6 GUA。

> **Note**
>
> - 依預設，您可以將 Amazon 提供的一個 IPv6 CIDR 區塊新增至區域集區。如需有關提高預設限制的資訊，請參閱 IPAM 的配額。
> - 您要佈建的 CIDR 必須在該範圍內可用。
> - 如果您要在集區內佈建該集區的 CIDR，則您要佈建的 CIDR 空間必須在該集區中可用。

7. 選擇 Provision (佈建)。
8. 在 IPAM 中檢視 CIDR 的方法是選擇導覽窗格中的 Pools (集區)、選擇一個集區，然後檢視該集區的 CIDR 索引標籤。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令將 CIDRs佈建至集區：

1. 取得 IPAM 集區 ID：describe-ipam-pools
2. 取得佈建至集區的 CIDR：get-ipam-pool-cidrs
3. 在集區中佈建新的 CIDR：provision-ipam-pool-cidr
4. 取得佈建至集區的 CIDR 並檢視新的 CIDR：get-ipam-pool-cidrs

在各範圍之間移動 VPC CIDR

透過將 CIDR 在不同範圍之間移動，您可以最佳化 IP 位址配置、依區域進行組織、區隔顧慮、強制執行合規性，並適應基礎設施變更。隨著工作負載的演進，這種靈活性有助於高效管理 IP 位址空間。

請依照本節中的步驟，將某個範圍內的 VPC CIDR 移至另一個範圍內。

> **Important**
>
> - 您僅能移動 VPC CIDR。當您移動 VPC CIDR 時，VPC 的子網路 CIDR 也會自動移動。
> - 僅能將 VPC CIDR 從某個私有範圍移至另一個。無法將 VPC CIDR 從公有範圍移至私有範圍或從私有範圍移至公有範圍。
> - 相同的 AWS 帳戶必須擁有這兩個範圍。
> - 如果 VPC CIDR 目前從私有範圍中的集區配置，則移動請求成功，但在您從目前集區釋出 VPC CIDR 配置之前，不會移動 VPC CIDR。如需有關釋出配置的資訊，請參閱釋出配置。

AWS Management Console

如何移動配置給某個 VPC 的 CIDR

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 Resources (資源)。
3. 在內容窗格最上方的下拉式選單中，選擇想要使用的範圍。
4. 在內容窗格中，選擇某個 VPC 並檢視該 VPC 的詳細資訊。
5. 在 VPC CIDR 底下，選取配置給該資源的其中一個 CIDR，然後選擇 Actions (動作) > Move CIDR to different scope (將 CIDR 移至其他範圍)。
6. 選取要將 VPC CIDR 移至哪個範圍。
7. 選擇將 CIDR 移至不同範圍。

Command line

使用下列 AWS CLI 命令來移動 VPC CIDR：

1. 取得目前範圍內的 VPC CIDR：get-ipam-resource-cidrs
2. 移動 VPC CIDR：modify-ipam-resource-cidr
3. 取得其他範圍內的 VPC CIDR：get-ipam-resource-cidrs

使用 IPAM 政策定義公有 IPv4 配置策略

IPAM 政策是一組規則，定義如何將 IPAM 集區的公有 IPv4 地址分配給 AWS 資源。每個規則會將 AWS 服務映射至服務將用於取得 IP 地址的 IPAM 集區。單一政策可以有多個規則，並套用到多個 AWS 區域。如果 IPAM 集區的位址用盡，則服務會回復為使用 Amazon 提供的 IP 位址。政策可以套用到 AWS Organizations 內的個別 AWS 帳戶或實體。如果您使用自己的 IP (BYOIP)，這有助於降低 AWS 公有 IPv4 成本。

何時使用 IPAM 政策

使用 IPAM 政策來：

- 使用 BYOIP 地址降低公有 IPv4 成本
- 集中控制 AWS 資源使用的 IP 集區
- 確保整個組織的 IP 配置一致

運作方式

當您在強制執行 IPAM 政策的帳戶中建立需要公有 IP 地址 AWS 的資源時：

- IPAM 會依序檢查您的政策規則。
- 如果規則符合資源類型，IPAM 會從指定的集區配置 IP。
- 如果集區為空且啟用溢位，Amazon 會提供 IP 地址。
- 如果沒有相符的規則，則會套用預設行為。

支援的 服務和資源

您可以建立 IPAM 政策，以定義如何將 IPAM 集區的公有 IPv4 地址配置給下列 AWS 服務和資源：

- 彈性 IP 地址 EIPs)
- Application Load Balancer ALBs)
- Amazon Relational Database Service (RDS)
- 區域 NAT 閘道

> **Important**
>
> 如果您在建立 AWS 資源時選擇特定的 IPAM 集區或 EIP 配置 ID，會覆寫 IPAM 政策。

先決條件

- 委派管理員帳戶中已啟用進階方案的 IPAM
- 具有 IPv4 地址的公有 IPAM 集區
- IPAM 和 EC2 操作的 IAM 許可

術語

IPAM 政策

IPAM 政策是一組規則，定義如何將 IPAM 集區的公有 IPv4 地址分配給 AWS 資源。每個規則會將 AWS 服務映射至服務將用於取得 IP 地址的 IPAM 集區。單一政策可以有多個規則，並套用到多個 AWS 區域。如果 IPAM 集區的位址用盡，則服務會回復為使用 Amazon 提供的 IP 位址。政策可以套用到 AWS Organizations 內的個別 AWS 帳戶或實體。政策可以套用到 AWS Organizations 內的個別 AWS 帳戶或實體。

配置規則

IPAM 政策中的選用組態，可將 AWS 資源類型映射至特定 IPAM 集區。若未定義任何規則，資源類型會預設為使用 Amazon 提供的 IP 位址。

Target

組織中可套用 IPAM 政策 AWS 的個別 AWS 帳戶或實體。

步驟 1：建立 IPAM 政策

使用 AWS 主控台：

請依照下列步驟，使用 AWS 主控台建立 IPAM 政策：

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在左側導覽窗格中選擇 Policies (政策)。
3. 選擇建立政策。
4. 輸入政策的名稱（選用）。

5. 選取要與此政策建立關聯的 IPAM。
6. (選用) 新增標籤。
7. 選擇建立政策。

使用 AWS CLI：

使用 create-ipam-policy 命令。

步驟 2：新增配置規則

建立政策後，您需要新增配置規則，以定義 IP 地址的配置方式：

使用 AWS 主控台：

請依照下列步驟，使用 AWS 主控台新增配置規則：

1. 在左側導覽窗格中選擇 Policies (政策)。
2. 選擇您在上一個步驟中建立的政策。
3. 在您的政策詳細資訊頁面中，選擇配置規則索引標籤。
4. 選擇建立配置規則。
5. 設定 服務組態：
   - 地區設定：選擇您希望套用此政策 AWS 的區域 (us-east-1) 或本地區域。
   - 資源類型：選取此政策 AWS 的服務或資源類型（彈性 IP 地址、RDS 資料庫執行個體、Application Load Balancer 或區域可用性模式中的 NAT 閘道）。
6. 設定規則組態：
   - IPAM 集區：選取將提供 IP 地址的 IPAM 集區。
   - 檢閱集區詳細資訊（地區、公有 IP 來源、可用空間和可用 CIDR 範圍）。
7. （選用）選擇新增規則以建立其他規則。
8. 選擇建立配置規則。

使用 AWS CLI：

使用 modify-ipam-policy-allocation-rules 命令。

步驟 3：啟用政策

指定哪些帳戶應該使用此政策。

使用 AWS 主控台：

請依照下列步驟，使用 AWS 主控台啟用政策：

1. 在您的政策詳細資訊頁面中，選擇目標索引標籤。
2. 選擇管理政策目標。
3. 執行以下任意一項：

   - 對於單一帳戶用量 (IPAM 未與 AWS Organizations 整合），請為您的帳戶選擇啟用。
   - 對於與 AWS Organizations 整合的 IPAM（當您是委派管理員時）：
     - 在組織結構區段中，選取您要套用此政策的帳戶或組織單位。
     - 勾選每個目標的已啟用核取方塊。
     - 選擇 Save Changes (儲存變更)。
     - 重要：啟用此政策將取代所選帳戶或組織單位上的任何作用中 IPAM 政策。

使用 AWS CLI：

根據您的設定使用 enable-ipam-policy 命令：

對於單一帳戶使用 (IPAM 未與 AWS Organizations 整合）：

```
aws ec2 enable-ipam-policy \
    --ipam-policy-id ipam-policy-12345678
```

對於與 AWS Organizations 整合的 IPAM（當您是委派管理員時），請將政策設定為以 AWS Organization 中的帳戶為目標：

```
aws ec2 enable-ipam-policy \
    --ipam-policy-id ipam-policy-12345678 \
    --organization-target-id 123456789012
```

對於與 AWS Organizations 整合的 IPAM（當您是委派管理員時），請將政策設定為以組織單位為目標：

```
aws ec2 enable-ipam-policy \
```

```
    --ipam-policy-id ipam-policy-12345678 \
    --organization-target-id ou-123
```

> **Important**
>
> 啟用此政策將取代所選取帳戶或組織單位上的任何現行 IPAM 政策。

步驟 4：測試您的政策

為您在其中一個目標帳戶中設定的類型（例如 EIP) 建立新的資源。資源會自動使用來自 IPAM 集區的 IP 地址。

> **Important**
>
> 如果您在建立 AWS 資源時選擇特定的 IPAM 集區或 EIP 配置 ID，會覆寫 IPAM 政策。

步驟 5：監控用量

在主控台中檢查您的 IPAM 集區，以查看要配置給資源的 IP 地址。

釋出配置

如果您打算刪除某個集區，則可能需要釋出集區配置。配置是指將某個 IPAM 集區中的 CIDR 指派到另一個資源或 IPAM 集區。

如果集區已佈建 CIDR，則無法刪除集區，如果 CIDR 已分配給資源，則無法將 CIDR 取消佈建。

> **Note**
>
> - 若要解除手動分配，應使用本節中的步驟，或呼叫 ReleaseIpamPoolAllocation API。
> - 若要解除私有範圍中的分配，則必須忽略或刪除資源 CIDR。如需詳細資訊，請參閱變更 VPC CIDR 的監控狀態。一段時間後，Amazon VPC IPAM 將自動代表您解除分配。
>
>   Example
>
>   範例

如果您在私有範圍中具有 VPC CIDR，若要解除分配，則必須忽略或刪除 VPC CIDR。一段時間後，Amazon VPC IPAM 會自動解除 IPAM 集區的 VPC CIDR 分配。

- 若要解除公有範圍中的分配，則必須刪除資源 CIDR。您無法忽略公有資源 CIDR。如需詳細資訊，請參閱 僅使用 CLI 將您自己的公有 IPv4 CIDR AWS 帶到 IPAM 中的清除或 僅使用 CLI 將您自己的 IPv6 CIDR AWS 帶到 IPAM 中的清除。一段時間後，Amazon VPC IPAM 將自動代表您解除分配。

若要使 Amazon VPC IPAM 代表您解除分配，必須正確地將所有帳戶許可設定為 single-account use (單一帳戶使用) 或 multi-account use (多帳戶使用)。

當您釋出由 IPAM 管理的 CIDR 時，Amazon VPC IPAM 會將 CIDR 重新回收至 IPAM 集區。如果您在進階方案中使用 IPAM，則需要幾分鐘的時間才能將 CIDR 用於未來的配置。如果您在免費方案中使用 IPAM，則最多需要 48 小時才能將 CIDR 用於未來的配置。如需有關集區和配置的詳細資訊，請參閱 IPAM 的運作方式。

AWS Management Console

釋出集區配置

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 在內容窗格最上方的下拉式選單中，選擇想要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 在內容窗格中，選擇配置所在的集區。
5. 選擇 Allocations (配置) 索引標籤。
6. 選取一或多個配置。您可以依據配置的資源類型來識別配置：
   - 自訂：自訂配置。
   - vpc：某種 VPC 配置。
   - ipam-pool：某種 IPAM 集區配置。
   - ec2-public-ipv4-pool：某種公有 IPv4 集區配置。
   - 子網路：子網路配置。
7. 選擇動作 > 發佈自訂配置。

8. 選擇 Deallocate CIDR (解除分配 CIDR)。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令來釋出集區配置：

1. 取得 IPAM 集區 ID：describe-ipam-pools
2. 檢視集區中目前的配置：get-ipam-pool-allocations
3. 釋出配置：release-ipam-pool-allocation
4. 檢視更新後的配置：get-ipam-pool-allocations

若要新增配置，請參閱 從 IPAM 集區配置 CIDR。若要在釋出配置之後刪除集區，必須先 從集區解除佈建 CIDR。

透過 AWS RAM 共用 IPAM 集區

請依照本節中的步驟，透過 AWS Resource Access Manager (RAM) 來共用 IPAM 集區。當您透過 RAM 共用 IPAM 集區時，「委託人」可將集區中的 CIDR 配置給 AWS 資源 (例如委託人各自帳戶的 VPC)。主體是 RAM 中的概念，意指任何 AWS 帳戶、IAM 角色或 AWS Organizations 中的組織單位。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的共用 AWS 資源。

Note

- 必須先將 IPAM 與 AWS Organizations 整合，才能透過 AWS RAM 共用 IPAM 集區。如需更多詳細資訊，請參閱 將 IPAM 與 AWS Organizations 中的帳戶整合。如果您是單一 IPAM 帳戶的使用者，則您無法與 AWS RAM 共用 IPAM 集區。
- 您必須啟用與 AWS RAM 中的 AWS Organizations 共享資源。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的啟用 AWS Organizations 中的共享資源。
- RAM 共用功能僅適用於 IPAM 的本地 AWS 區域。必須在 IPAM 所在的 AWS 區域 (而不是 IPAM 集區的區域) 建立共用。
- 用來建立和刪除 IPAM 集區資源共用的帳戶，其 IAM 角色連接的 IAM 政策必須具有下列許可：
  - `ec2:PutResourcePolicy`

    - `ec2:DeleteResourcePolicy`
- 一次 RAM 共用可新增多個 IPAM 集區。
- 雖然您可以與 AWS 組織外部的任何 AWS 帳戶共用 IPAM 集區，但 IPAM 只會在帳戶擁有者已經歷與委派 IPAM 管理員共用其資源探索的程序時，才會監控組織外部帳戶中的 IP 位址，如 將 IPAM 與組織外的帳戶整合 中所述。

AWS Management Console

共用使用 RAM 的 IPAM 集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 按預設，會選取預設的私有範圍。如果不想使用預設的私有範圍，請從內容窗格最上方的下拉式選單中選擇您要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 在內容窗格中，選擇您要共用的集區，然後選擇 Actions (動作) > View details (檢視詳細資訊)。
5. 在 Resource sharing (資源共用) 底下，選擇 Create resource share (建立資源共用)。AWS RAM 主控台隨即開啟。您會在 AWS RAM 中建立共用集區。
6. 選擇 Create a resource share (建立資源共用)。
7. 新增要為共用資源指定的 Name (名稱)。
8. 在 Select resource type (選取資源類型) 底下，選取 IPAM 集區並選擇一或多個 IPAM 集區。
9. 選擇 Next (下一步)。
10. 選擇其中一個資源共用的許可：
    - AWSRAMDefaultPermissionsIpamPool：選擇此許可可允許委託人檢視共用 IPAM 集區中的 CIDR 和配置以及集區中的 CIDR 配置/釋出。
    - AWSRAMPermissionIpamPoolByoipCidrImport：選擇此許可可允許委託人將 BYOIP CIDR 匯入共用的 IPAM 集區。只有在您已有 BYOIP CIDR 且想要將它們匯入 IPAM 並與委託人共用時，才需要此許可。如需有關將 BYOIP CIDR 匯入 IPAM 的其他資訊，請參閱 教學課程：將 BYOIP IPv4 CIDR 傳輸至 IPAM。
11. 選擇可存取此資源的委託人。如果委託人要將現有的 BYOIP CIDR 匯入此共用的 IPAM 集區，請以委託人身分來新增 BYOIP CIDR 擁有者帳戶。
12. 檢閱資源共用選項以及您要與其共用的委託人，然後選擇 Create (建立)。

Command line

本節中的命令與 AWS CLI Command Reference 連結。該處載有執行命令時可用選項的相關詳細說明。

使用下列 AWS CLI 命令可透過 RAM 與他人共用 IPAM 集區：

1. 取得 IPAM 的 ARN：describe-ipam-pools
2. 建立資源共用：create-resource-share
3. 檢視資源共用：get-resource-shares

使用 RAM 建立資源共用之後，其他委託人就可以使用 IPAM 集區將 CIDR 配置給資源。如需監控委託人所建立之資源的相關資訊，請參閱 依資源監控 CIDR 使用情況。如需有關如何從共用 IPAM 集區建立 VPC 及配置 CIDR 的詳細資訊，請參閱 Amazon VPC User Guide 中的 Create a VPC。

使用資源探索

資源探索是一個 IPAM 元件，可讓 IPAM 管理和監控屬於擁有資源發現的帳戶的資源。這可讓 IPAM 維持工作負載中 IP 位址使用情況的最新清查，協助管理及規劃 IP 位址。

依預設，在建立 IPAM 時，會建立資源探索。您也可以獨立於 IPAM 建立資源探索，並將其與其他帳戶或組織擁有的 IPAM 整合。如果資源探索擁有者是組織的委派管理員，IPAM 將監控組織所有成員的資源。

> **Note**
>
> 建立、共用和關聯資源探索是整合 IPAM 與組織外部帳戶之處理程序的一部分 (請參閱 將 IPAM 與組織外的帳戶整合)。如果您不建立 IPAM 且不會將其與組織外部帳戶整合，則無需建立、共用或關聯資源探索。

請注意，本節提供與使用資源探索相關的一組程序。

目錄

- 將資源探索與 IPAM 建立關聯
- 取消關聯資源探索
- 刪除資源探索

建立資源探索以與其他 IPAM 整合

本節描述如何建立資源探索。依預設，在建立 IPAM 時，會建立資源探索。每個區域的資源探索預設配額為 1。如需有關配額的詳細資訊，請參閱 IPAM 的配額。

> **Note**
>
> 建立、共用和關聯資源探索是整合 IPAM 與組織外部帳戶之處理程序的一部分 (請參閱 將 IPAM 與組織外的帳戶整合)。如果您不建立 IPAM 且不會將其與組織外部帳戶整合，則無需建立、共用或關聯資源探索。

如果要將 IPAM 與組織外部帳戶整合，則這是次要組織管理員帳戶必須完成的必要步驟。如需有關本處理程序中所涉及角色的詳細資訊，請參閱 程序概觀。

AWS Management Console

建立資源探索

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇尋找探索。
3. 選擇建立資源探索。
4. 選擇 Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (允許 Amazon VPC IP 地址管理員將來源帳戶的資料複寫到 IPAM 委託帳戶)。若未選取此選項，則無法建立資源探索。
5. (選用) 將名稱標籤新增至資源探索。標籤是您指派給 AWS 資源的標籤。每個標籤皆包含索引鍵與選用值。您可以使用標籤來搜尋和篩選資源，或追蹤 AWS 成本。
6. (選用) 新增描述。
7. 在作業區域下，選取將在其中探索資源的 AWS 區域。目前的區域會自動設定為其中一個作業區域。如果正在建立資源探索，以便可以在作業區域 `us-east-1` 中與 IPAM 共用，則請務必在此處選取 `us-east-1`。如果忘記作業區域，稍後可以返回並編輯資源探索設定。

> **Note**
>
> 大多數情況下，資源探索應具有與 IPAM 相同的作業區域，否則您只能在該區域取得資源探索。

8. (選用) 為集區選擇其他標籤。
9. 選擇建立。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

- 建立資源探索：create-ipam-resource-discovery

檢視資源探索詳細資訊

檢視 AWS IPAM 中資源探索的詳細資訊可提供寶貴的洞見，例如：

- 識別已匯入的特定 AWS 資源及其相關聯的 IP 位址配置。
- 監控資源探索程序的狀態和進度。
- 對 IPAM 與探索的資源之間的任何問題或差異進行故障診斷。
- 分析 IP 位址使用率和趨勢。

此資訊可協助您最佳化 IP 位址管理，並確保 IPAM 與實際資源部署之間的一致性。

AWS Management Console

檢視資源探索詳細資訊

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇尋找探索。
3. 選擇資源探索。
4. 在資源探索詳細資訊下，檢視與資源探索相關的詳細資訊，例如「預設值」，指出資源探索是否為預設值。預設資源探索是建立 IPAM 時自動建立的資源探索。
5. 在索引標籤中，檢視資源探索的詳細資訊：

- 探索到的資源 - 在資源探索下監控的資源。IPAM 會監控下列資源類型的 CIDR：VPC、公有 IPv4 集區、VPC 子網路和彈性 IP 地址。
  - 名稱 (資源 ID) – 資源探索 ID。
  - 已分配 IP – 使用中 IP 位址空間的百分比。若要將小數轉換為百分比，請將小數乘以 100。注意下列事項：
    - 如果是 VPC 資源，則為 VPC 中由子網路 CIDR 佔用的 IP 地址空間百分比。
    - 如果是子網資源，若子網已佈建 IPv4 CIDR，則此為使用中的子網內 IPv4 地址空間的百分比。若子網已佈建 IPv6 CIDR，則不會顯示使用中的 IPv6 地址空間百分比。目前無法計算使用中的 IPv6 地址空間百分比。
    - 如果是公有 IPv4 集區資源，則為集區中已配置給彈性 IP 地址 (EIP) 的 IP 地址空間百分比。
  - CIDR – 資源 CIDR。
  - 區域 – 資源區域。
  - 擁有者 ID – 資源擁有者 ID。
  - 取樣時間 - 上次成功的資源探索時間。
- 探索到的帳戶：在資源探索下監控的 AWS 帳戶。如果已將 IPAM 與 AWS Organizations 整合，則組織中的所有帳戶都是探索到的帳戶。
  - 帳戶 ID – 帳戶 ID。
  - 區域 – 從中傳回帳戶資訊的 AWS 區域。
  - 上次嘗試探索時間 - 上次嘗試探索資源的時間。
  - 上次成功探索時間 – 上次成功資源探索時間。
  - 狀態 - 資源探索失敗原因。
- 作業區域 – 資源探索的作業區域。
- 資源共用 - 如果已共用資源探索，則會列出資源共用 ARN。
  - 資源共用 ARN – 資源共用 ARN。
  - 狀態 - 資源共用的目前狀態。可能值為：
    - 作用中 - 資源共用為作用中且可供使用。
    - 刪除 - 已刪除資源共用且無法再使用。
    - 待定 - 接受資源共用的邀請正在等待回應。
  - 建立時間 - 建立資源共用的時間。

- 標籤 - 標籤是您指派給 AWS 資源的標籤。每個標籤皆包含一個鍵和一個選用值。您可以使用標籤來搜尋和篩選資源，或追蹤 AWS 成本。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

- 檢視資源探索詳細資訊：describe-ipam-resource-discoveries

與其他 AWS 帳戶共用資源探索

請依照本節中的步驟，使用 AWS Resource Access Manager 來共用資源探索。如需有關 AWS RAM 的詳細資訊，請參閱《AWS RAM 使用者指南》中的共用 AWS 資源。

> **Note**
>
> 建立、共用和關聯資源探索是整合 IPAM 與組織外部帳戶之處理程序的一部分 (請參閱 將 IPAM 與組織外的帳戶整合)。如果您不建立 IPAM 並不會將其與組織外部帳戶整合，則無需建立、共用或關聯資源探索。

當您建立可監控組織外帳戶的 IPAM 時，次要組織管理員帳戶會使用 AWS RAM 與主要組織 IPAM 帳戶共用其資源探索。您必須先與主要組織 IPAM 帳戶共用資源探索，主要組織 IPAM 帳戶才能將資源探索與其 IPAM 建立關聯。如需有關本處理程序中所涉及角色的詳細資訊，請參閱 程序概觀。

> **Note**
>
> - 當您使用 AWS RAM 建立資源共用以共用資源探索時，必須在主要組織 IPAM 的主要區域中建立資源共用。
> - 用來建立和刪除資源探索之資源共享的帳戶在其 IAM 政策中必須具有下列許可：
>   - ec2:PutResourcePolicy
>   - ec2:DeleteResourcePolicy
> - 如果您將資源探索共享給另一個帳戶，則該帳戶可以看到與資源探索相關的組織單位排除項目，並能查看其中包含的資源探索擁有者的組織 ID、根 ID 以及組織單位 ID 等資訊。

如果要將 IPAM 與組織外部帳戶整合，則這是次要組織管理員帳戶必須完成的必要步驟。

AWS Management Console

共用資源探索

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇尋找探索。
3. 選擇資源共用索引標籤。
4. 選擇 Create resource share (建立資源共用)。AWS RAM 主控台隨即開啟，您可以在其中建立資源共用。
5. 在 AWS RAM 主控台中，選擇 Settings (設定)。
6. 選擇啟用與 AWS Organizations 共用，然後選擇儲存設定。
7. 選擇 Create a resource share (建立資源共用)。
8. 新增要為共用資源指定的 Name (名稱)。
9. 在選取資源類型下，選取 IPAM 資源探索，然後選擇資源探索。
10. 選擇下一步。
11. 在關聯許可下，可以檢視將針對已授權可存取此資源共用的主體而啟用的預設許可：
    - AWSRAMPermissionIpamResourceDiscovery
    - 此許可允許的動作：
      - ec2:AssociateIpamResourceDiscovery
      - ec2:GetIpamDiscoveredAccounts
      - ec2:GetIpamDiscoveredPublicAddresses
      - ec2:GetIpamDiscoveredResourceCidrs
12. 指定可存取此共用資源的主體。針對主體，選擇主要組織 IPAM 帳戶，然後選擇新增。
13. 選擇下一步。
14. 檢閱資源共用選項以及您要與其共用的主體。然後，選擇建立資源共用。
15. 共用資源探索之後，主要組織 IPAM 帳戶必須接受它，然後由主要組織 IPAM 帳戶將其與 IPAM 建立關聯。如需更多詳細資訊，請參閱 將資源探索與 IPAM 建立關聯。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

1. 建立資源共用：create-resource-share
2. 檢視資源共用：get-resource-shares

將資源探索與 IPAM 建立關聯

本節描述如何將資源探索與 IPAM 建立關聯。當您將資源探索與 IPAM 建立關聯時，IPAM 會監控資源探索下探索到的所有資源 CIDR 和帳戶。當您建立 IPAM 時，系統會為 IPAM 建立預設資源探索，並自動將其與 IPAM 建立關聯。

資源探索關聯的預設配額為 5。如需詳細資訊 (包括如何調整此配額)，請參閱 IPAM 的配額。

> **Note**
>
> 建立、共用和關聯資源探索是整合 IPAM 與組織外部帳戶之處理程序的一部分 (請參閱 將 IPAM 與組織外的帳戶整合)。如果您不建立 IPAM 並不會將其與組織外部帳戶整合，則無需建立、共用或關聯資源探索。

如果要將 IPAM 與組織外部帳戶整合，這是主要組織 IPAM 帳戶必須完成的必要步驟。如需有關本處理程序中所涉及角色的詳細資訊，請參閱 程序概觀。

AWS Management Console

關聯資源探索

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 IPAMs。
3. 選取已關聯的探索，然後選擇關聯資源探索。
4. 在 IPAM 資源探索下，選擇次要組織管理員帳戶已與您共用的資源探索。
5. 選擇關聯。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

- 關聯資源探索：associate-ipam-resource-discovery

取消關聯資源探索

本節描述如何將資源探索與 IPAM 取消關聯。當您將資源探索與 IPAM 取消關聯時，IPAM 便不再監控資源探索下探索到的所有資源 CIDR 和帳戶。

> **Note**
>
> 您無法取消預設資源探索關聯。預設資源探索關聯是在您建立 IPAM 時自動建立的關聯。但是，如果您刪除 IPAM，則會刪除預設的資源探索關聯。

此步驟必須由主要組織 IPAM 帳戶完成。如需有關本處理程序中所涉及角色的詳細資訊，請參閱 程序概觀。

AWS Management Console

取消關聯資源探索

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 IPAMs。
3. 選取已關聯的探索，然後選擇取消關聯資源探索。
4. 在 IPAM 資源探索下，選擇次要組織管理員帳戶已與您共用的資源探索。
5. 選擇取消關聯。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

- 取消關聯資源探索：disassociate-ipam-resource-discovery

刪除資源探索

本節描述如何刪除資源探索。

> **Note**
>
> 您無法刪除預設資源探索。預設資源探索是在您建立 IPAM 時自動建立的資源探索。但是，如果您刪除 IPAM，則會刪除預設的資源探索。

此步驟必須由次要組織管理員帳戶完成。如需有關本處理程序中所涉及角色的詳細資訊，請參閱 程序概觀。

AWS Management Console

刪除資源探索

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇尋找探索。
3. 選取資源探索，然後選擇動作 > 刪除資源探索。

Command line

本節中的命令與 AWS CLI Command Reference 連結。本文件旨在詳細說明執行命令時可使用的選項。

- 刪除資源探索：delete-ipam-resource-discovery

追蹤 IPAM 中的 IP 地址使用情況

Amazon VPC IP 位址管理員提供 IP 位址使用情況追蹤功能，可讓任何管理複雜網路環境的人員受益。IPAM 可讓您深入了解跨 AWS 的 IP 位址配置、使用率和使用量趨勢。這可協助您識別未使用或使用效率不佳的 IP 位址、最佳化地址空間，並防止潛在的 IP 位址耗盡。

IPAM 能在 CIDR、範圍和 IPAM 層級追蹤 IP 位址使用情況，並提供詳細的報告和分析。這對於大規模部署、多帳戶設定以及不斷變化的網路需求具有重要價值。

利用 IPAM 的使用情況追蹤，您可以做出明智決策、改善 IP 位址管理，並確保 IP 資源的高效利用。

> **Note**
>
> 本節中的任務是選用任務，不一定要完成。如果您要完成本節中的任務，且已委派 IPAM 帳戶，則需由 IPAM 帳戶完成這些任務。

目錄

使用 IPAM 儀表板監控 CIDR 使用情況

您可以利用 Amazon VPC IP 位址管理員中的 IPAM 儀表板監控數個重要案例的 CIDR 使用情況：

- 識別未使用或未充分利用的 IP 位址空間：儀表板可讓您深入了解 CIDR 使用情況，從而識別具有可用容量且可回收或重新配置的 CIDR。
- 最佳化 IP 位址管理：透過密切追蹤 CIDR 使用情況，您可以做出有關擴充、收縮或重新指派 IP 位址區塊的明智決策，以滿足不斷變化的業務和基礎設施需求。
- 防止 IP 位址耗盡：透過監控 CIDR 使用情況，您可以預測何時可能需要取得額外的 IP 位址空間，從而主動規劃並避免因 IP 位址耗盡而導致服務中斷。

- 確保合規和管理：IPAM 儀表板可協助您展示 IP 位址使用模式，以符合法規要求或 IP 位址管理的內部政策。
- 網路問題故障診斷：詳細的 CIDR 使用情況資料可協助找出網路連線問題或資源衝突的根本原因。

透過利用 IPAM 儀表板密切監控 CIDR 使用情況，您可以提升 AWS 內 IP 位址管理的效率、彈性及合規性。

AWS Management Console

使用 IPAM 儀表板監控 CIDR 使用情況

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 Dashboard (儀表板)。
3. 按預設，當您檢視儀表板時，系統會選取私有範圍。如果不想使用預設的私有範圍，請從內容窗格最上方的下拉式選單中選擇您要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 儀表板會顯示某個範圍內 IPAM 集區和 CIDR 的概觀。您可以新增、移除、調整和移動小工具以自訂儀表板。

    - Scope (範圍)：此範圍的詳細資訊。範圍是 IPAM 內最高層級的容器。IPAM 包含兩個預設範圍，分別是一個私有範圍和一個公有範圍。每個範圍代表單一網路的 IP 空間。您可能有多個私有範圍，但只能擁有一個公有範圍。
        - Scope ID (範圍 ID)：此範圍的 ID。
        - Scope type (範圍類型)：範圍的類型。
        - IPAM ID：範圍所在之 IPAM 的 ID。
        - 此範圍中的 IAPM 集區：範圍所在之 IPAM 的 ID。
        - 檢視此範圍中的聯網資源：帶您前往 IPAM 主控台資源區段。
        - 搜尋此範圍內 IP 地址的歷史記錄：帶您前往 IPAM 主控台的搜尋 IP 歷史記錄區段。
    - 資源 CIDR 類型：範圍中的資源 CIDR 類型。
        - 子網路：子網路的 CIDR 數目。
        - VPC：VPC 的 CIDR 數目。
        - EIP：彈性 IP 地址的 CIDR 數目。
        - 公有 IPv4 集區：公有 IPv4 集區的 CIDR 數目。
    - 管理狀態：CIDR 的管理狀態。

  - Unmanaged CIDRs (未受管 CIDR)：此範圍中未受管資源的資源 CIDR 數目。
  - Ignored CIDRs (被忽略的 CIDR)：您在範圍內 IPAM 中選擇不監控的資源 CIDR 數目。針對範圍內被忽略的資源，IPAM 不會評估其是否重疊或合規。選擇忽略資源時，從 IPAM 集區配置給該資源的任何空間都會傳回至集區，而且不會透過自動匯入再次將該資源匯入 (如果已設定集區的自動匯入配置規則)。
  - Managed CIDRs (受管 CIDR)：從範圍內 IPAM 集區配置之可管理資源 (VPC 或公有 IPv4 集區) 的資源 CIDR 數目。
- 重疊的資源 CIDR：重疊與非重疊 CIDR 的數目。重疊的 CIDR 可能會導致 VPC 中的路由不正確。
  - Overlapping CIDRs (重疊 CIDR)：範圍內 IPAM 集區中目前重疊的 CIDR 數目。重疊的 CIDR 可能會導致 VPC 中的路由不正確。
  - 非重疊 CIDR：範圍內集區中非重疊的資源 CIDR 數目。
- 合規資源 CIDR：合規資源 CIDR 的數目。
  - Compliant CIDRs (合規 CIDR)：符合範圍內 IPAM 集區配置規則的資源 CIDR 數目。
  - Noncompliant CIDRs (不合規 CIDR)：不符合範圍內 IPAM 集區配置規則的資源 CIDR 數目。
- 重疊狀態：隨時間重疊的 CIDR 數目。
  - OverlappingResourceCidrs：範圍內 IPAM 集區中重疊的 CIDR 數目。重疊的 CIDR 可能會導致 VPC 中的路由不正確。
- 合規狀態：隨時間符合 (與不符合) 範圍內 IPAM 集區分配規則的 CIDR 數目。
  - CompliantResourceCidrs ：符合配置規則的資源 CIDR 數目。
  - NoncompliantResourceCidrs：不符合配置規則的資源 CIDR 數目。
- VPC utilization (VPC 使用率)：IP 使用率最高或最低的 VPC (IPv4 和 IPv6)。您可以使用此資訊設定 Amazon CloudWatch 警示，以便在超出 IP 使用率閾值時收到警示。如需更多詳細資訊，請參閱 IPAM 資源使用率指標。
- Subnet utilization (子網路使用率)：IP 使用率最高或最低的子網路 (僅限 IPv4)。您可以使用此資訊來決定要保留還是刪除未充分利用的資源。如需更多詳細資訊，請參閱 IPAM 資源使用率指標。
- 配置最高 IP 的 VPC：配置給子網路之 IP 地址空間百分比最高的 VPC。這對於顯示是否需要為 VPC 佈建額外的 IP 地址空間非常有用。
- 配置最高 IP 的子網路：配置給資源之 IP 地址空間百分比最高的子網路。這對於顯示您是否需要為子網路佈建額外的 IP 地址空間非常有用。
- 集區指派：隨時間已指派給範圍內資源和手動配置使用的 IP 空間百分比。

- 集區配置：隨時間已配置給範圍內其他集區使用的集區 IP 空間百分比。

Command line

儀表板中顯示的資訊來自於存放在 Amazon CloudWatch 中的指標。如需有關儲存在 Amazon CloudWatch 中的測量結果的詳細資訊，請參閱 使用 Amazon CloudWatch 監控 IPAM。使用 AWS CLI 參考中的 Amazon CloudWatch 選項可檢視 IPAM 集區和範圍內配置的指標。

如果您發現針對集區佈建的 CIDR 幾乎已全數分配完，則可能需要佈建更多 CIDR。如需詳細資訊，請參閱 佈建集區的 CIDR。

依資源監控 CIDR 使用情況

Amazon VPC IP Address Manager 中的資源檢視提供跨 AWS 資源的 IP 地址使用率的集中式概觀。這讓您能夠快速識別哪些資源正在消耗 IP 位址、追蹤位址分配趨勢，以及最佳化 IP 位址管理，以滿足不斷變化的基礎設施和業務需求。

在 IPAM 中，資源是指派 IP 地址或 CIDR 區塊 AWS 的服務實體。IPAM 會管理一些資源，同時只會監控其他一些資源，因此了解兩者之間的差異非常重要：

- Managed resource (受管資源)：受管的資源具有從 IPAM 集區配置的 CIDR。IPAM 會監控 CIDR 是否與集區中其他 CIDR 的潛在 IP 地址重疊，並監控 CIDR 是否符合集區配置規則。IPAM 支援管理下列類型的資源：
  - 彈性 IP 位址
  - 公有 IPv4 集區

    > **Note**
    >
    > 公有 IPv4 集區和 IPAM 集區由 中的不同資源管理 AWS。公有 IPv4 集區是單一帳戶資源，可讓您將公有的 CIDR 轉換為彈性 IP 地址。使用 IPAM 集區可將公有空間配置給公有 IPv4 集區。

  - VPC
- 監控的資源：如果資源由 IPAM 監控，則 IPAM 已偵測到資源，您可以在`get-ipam-resource-cidrs`搭配 CLI 使用時，或在導覽窗格中檢視資源時，檢視資源 CIDR AWS 的詳細資訊。IPAM 支援監控下列資源：
  - 彈性 IP 位址

- 公有 IPv4 集區
- VPC
- VPC 子網路

AWS Management Console

依資源監控 CIDR 使用情況

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 Resources (資源)。
3. 在內容窗格最上方的 IP 下拉式選單中，選擇想要使用的 IP 位址通訊協定：IPv4 或 IPv6。
4. 在內容窗格最上方的範圍下拉式選單中，選擇想要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
5. 使用資源 CIDR 對應來檢視範圍中可用、已配置和重疊的 IP 地址空間：

   - 可用：IP 地址範圍可用於配置。
   - 相容與非重疊：IP 位址範圍會配置給 IPAM 管理的資源。
   - 已佔用：IP 位址範圍已配置給資源。
   - 重疊：IP 位址範圍已配置給多個資源且重疊。
   - 不相容：IP 位址範圍不相容。有一個資源使用的 IP 位址範圍不符合為集區設定的配置規則。

   在 CIDR 對應中，選擇對應底部的 IP 位址區塊，以檢視較小 CIDR 區塊中的資源。選擇對應頂部的 IP 位址區塊，以檢視較大 CIDR 區塊中的資源。
6. 您可以在資料表中檢視有關範圍內資源的下列詳細資訊：

   - 名稱 (資源 ID)：資源的名稱和資源 ID。
   - CIDR：與資源相關聯的 CIDR。
   - 管理狀態：資源的狀態。
     - Managed (受管)：資源具有從 IPAM 集區配置的 CIDR，而且正由 IPAM 監控潛在的 CIDR 是否重疊並符合集區配置規則。
     - Unmanaged (未受管)：資源沒有從 IPAM 集區配置的 CIDR，而且不會由 IPAM 監控潛在的 CIDR 是否符合集區配置規則。監控 CIDR 是否有重疊。

- 已忽略：已選擇不監控該資源。不會評估已忽略的資源是否有重疊或符合配置規則。選擇忽略資源時，從 IPAM 集區配置給該資源的任何空間都會傳回至集區，而且不會透過自動匯入再次將該資源匯入 (如果已設定集區的自動匯入配置規則)。
- -：此資源不是 IPAM 可以管理的資源類型之一。

- 合規狀態：CIDR 的合規狀態。
  - Compliant (合規)：受管的資源符合 IPAM 集區的配置規則。
  - 不合規：資源 CIDR 不符合 IPAM 集區的一或多項配置規則。

    Example

    如果 VPC 的 CIDR 不符合 IPAM 集區的網路遮罩長度參數，或者資源不在與 IPAM 集區相同的 AWS 區域中，則會將其標記為不合規。
  - 未受管：資源沒有從 IPAM 集區配置的 CIDR，而且 IPAM 不會監控其是否有符合集區配置規則的潛在 CIDR。監控 CIDR 是否有重疊。
  - 已忽略：已選擇不監控該資源。不會評估已忽略的資源是否有重疊或符合配置規則。選擇忽略資源時，從 IPAM 集區配置給該資源的任何空間都會傳回至集區，而且不會透過自動匯入再次將該資源匯入 (如果已設定集區的自動匯入配置規則)。
  - -：此資源不是 IPAM 可以管理的資源類型之一。
- 重疊狀態：CIDR 的重疊狀態。
  - Nonoverlapping (不重疊)：資源 CIDR 不會重疊在相同範圍內的另一個 CIDR。
  - Overlapping (重疊)：資源 CIDR 與相同範圍內的另一個 CIDR 相互重疊。請注意，如果資源 CIDR 重疊，則可能會與手動配置重疊。
  - 已忽略：已選擇不監控該資源。IPAM 不會評估已忽略的資源是否有重疊或符合配置規則。選擇忽略資源時，從 IPAM 集區配置給該資源的任何空間都會傳回至集區，而且不會透過自動匯入再次將該資源匯入 (如果已設定集區的自動匯入配置規則)。
  - -：此資源不是 IPAM 可以管理的資源類型之一。
- 配置的 IP：如果是 VPC 資源，此為 VPC 中由子網路 CIDR 佔用的 IP 位址空間百分比。如果是子網路資源，若子網路已佈建 IPv4 CIDR，則此為使用中的子網內 IPv4 位址空間的百分比。若子網路已佈建 IPv6 CIDR，則不會顯示使用中的 IPv6 位址空間百分比。目前無法計算使用中的 IPv6 位址空間百分比。如果是公有 IPv4 集區資源，則為集區中已配置給彈性 IP 位址 (EIP) 的 IP 位址空間百分比。
- 區域：資源 AWS 的區域。
- 擁有者 ID：建立此資源的人員 AWS 的帳戶 ID。
- 資源類型：資源是 VPC、子網路、彈性 IP 地址或公有 IPv4 集區。

- 集區 ID：資源所在 IPAM 集區的 ID。

7. 使用篩選資源，依欄屬性 (例如 VPC ID 或合規性狀態) 篩選資源表格。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列 AWS CLI 命令，依資源監控 CIDR 用量：

1. 取得範圍 ID：describe-ipam-scopes
2. 要求資源資訊：get-ipam-resource-cidrs

使用 Amazon CloudWatch 監控 IPAM

IPAM 會自動將與 IP 地址使用情況 (例如，您 IPAM 集區中可用的 IP 地址空間和符合分配規則的資源 CIDR 數量) 和資源使用率相關的指標，存放在您 IPAM 主區域的 AWS/IPAM Amazon CloudWatch 命名空間中。

將 IPAM 與 CloudWatch 整合可增強您在 AWS 中監控、分析和最佳化 IP 位址管理的能力。

使用案例包括：

- 追蹤 IP 位址使用率趨勢：CloudWatch 可以監控 CIDR 集區使用情況、範圍配置和其他 IPAM 指標，協助您主動識別潛在的 IP 位址耗盡風險。
- 設置基於利用率的提醒：您可以設定 CloudWatch 警示，以便在 CIDR 使用率達到預先定義的閾值時通知您，從而及時介入和進行最佳化。
- 監控 IPAM 事件：CloudWatch 可以擷取和分析 IPAM 相關事件，例如 CIDR 配置、解除配置和範圍修改，從而提供 IP 位址管理活動的可見性。
- 產生自訂儀表板：透過將 IPAM 資料與其他 AWS 指標結合，您可以建立全面的儀表板，從而以視覺化方式分析 IP 位址環境，以及相關的基礎設施和效能指標。

目錄

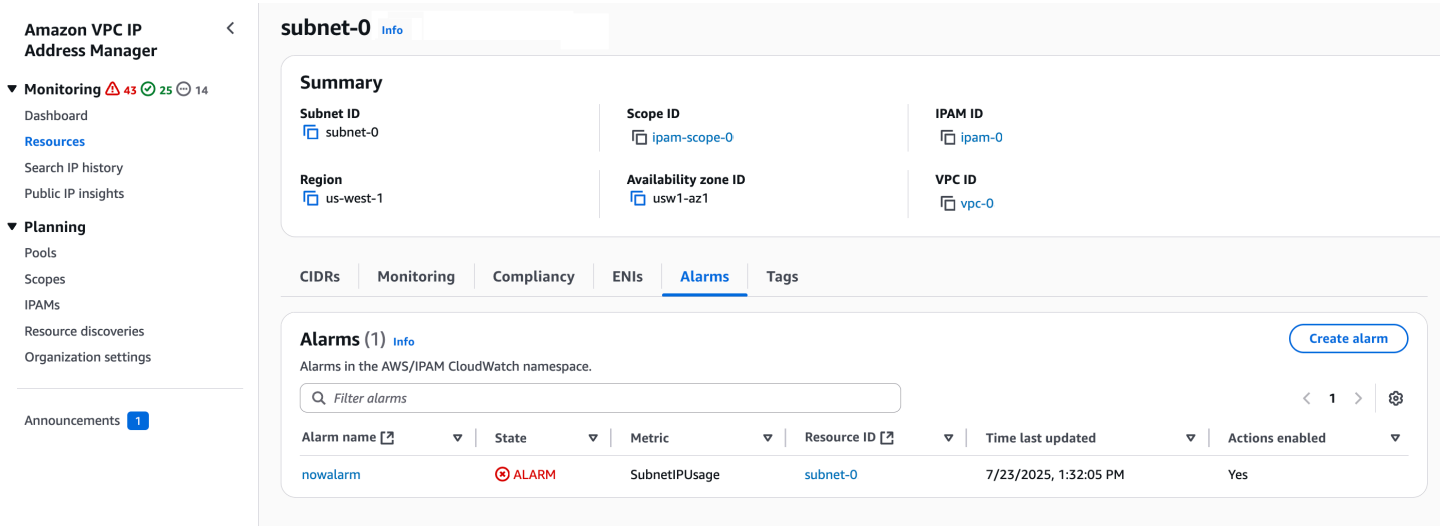
在 IPAM 主控台中管理警示

您可以直接在 IPAM 主控台中建立和管理 Amazon CloudWatch 警示。處於 INSUFFICIENT_DATA 或 ALARM 狀態的 IPAM 指標 或 IPAM 資源使用率指標 警示會在主控台頂端顯示為警告列，並在監控旁的左側導覽中顯示為視覺化指示器。

若要管理特定資源的警示，請選擇資源，然後依次選擇 VPC、子網路或集區。資源詳細資訊頁面開啟後，選擇警示索引標籤。

警示索引標籤會顯示與所選資源相關聯的所有 CloudWatch 警示。您可以在此索引標籤中檢視警示詳細資訊、監控目前狀態，以及存取警示組態選項。此索引標籤會顯示與您正在檢視之資源相關的 AWS/IPAM 命名空間中的警示。

下列螢幕擷取畫面顯示 IPAM 主控台中的警示管理介面：



警示索引標籤提供 IPAM 主要區域 AWS/IPAM Amazon CloudWatch 命名空間中的 CloudWatch 警示的詳細摘要：

- 警示名稱：CloudWatch 警示的使用者自訂名稱。
- 狀態：CloudWatch 警示的目前狀態：
  - 警示：指標超出定義的閾值。
  - 確定：指標在定義的閾值範圍內。
  - INSUFFICIENT_DATA：資料不足以確定警示狀態。
- 指標：警示功能會監控的特定 CloudWatch 指標。
- 資源 ID：警示正在監控 AWS 的資源的唯一識別符。
- 上次更新時間：上次變更或評估的警示狀態的日期和時間。

- 動作已啟用：指出是否已啟用警示的 CloudWatch 動作：
  - 是：當符合條件時，警示可觸發設定的動作。
  - 否：警示功能正在監控，但不執行動作。

此外，如果您在 VPC、子網路或集區的監控索引標籤上檢視使用率圖表，可以選擇為資源使用率建立警示的選項。然後，系統會將您重新導向至 CloudWatch 主控台，並預先填入資源與指標詳細資訊。例如，您可以設定警示閾值，以在使用率達到特定百分比時收到通知。

IPAM 指標

IPAM 會將 IPAM、集區和範圍的相關資料發佈到 Amazon CloudWatch。您可使用這些指標為 IPAM 集區建立警示，在地址集區即將耗盡或資源不符合集區上設定的分配規則時通知您。使用 Amazon CloudWatch 建立警示和設定通知不在本節的範圍內。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示。

以下列出 IPAM 傳送給 Amazon CloudWatch 的指標和維度。

IPAM 指標

`AWS/IPAM` 命名空間包含下列 IPAM 指標。

指標名稱	說明
TotalActiveIpCount	如果從免費方案切換到進階方案，則作用中 IP 總計數即為 IPAM 中需要支付費用的作用中 IP 位址的數量。作用中的 IP 位址是指與附加到 EC2 執行個體等資源的彈性網絡介面 (ENI) 關聯的 IP 位址或字首。 • 此指標僅適用於免費方案客戶。 • 如果您的 IPAM 已與 AWS Organizations 整合，則作用中 IP 計數會涵蓋所有組織帳戶。 • 您無法依 IP 類型 (公有/私有) 或類別 (IPv4/IPv6) 檢視作用中 IP 計數的明細。 • IPAM 只計算由受監控帳戶擁有的 ENI 中的 IP 位址數量。共用子網路的計數可能不準確。如果 IPAM 未涵蓋子網路擁有者或 ENI 擁有者，則 IP 位址會被排除在外。

IPAM 集區指標

AWS/IPAM 命名空間包含下列 IPAM 集區指標。

指標名稱	描述
CompliantResourceCidrs	符合 IPAM 集區分配規則的受管資源 CIDR 數目。如需有關分配規則的詳細資訊，請參閱建立頂層 IPv4 集區。
NoncompliantResourceCidrs	不符合 IPAM 集區分配規則的受管資源 CIDR 數目。如需有關分配規則的詳細資訊，請參閱建立頂層 IPv4 集區。
PercentAllocated	已分配給其他集區使用的集區 IP 空間百分比。
PercentAssigned	已分配給資源 (包括手動分配) 使用的集區 IP 空間百分比。
PercentAvailable	未分配給其他集區或資源使用的集區 IP 空間百分比。

IPAM 範圍指標

AWS/IPAM 命名空間包含下列 IPAM 範圍指標。

指標名稱	描述
CompliantResourceCidrs	符合範圍內 IPAM 集區分配規則的資源 CIDR 數目。
ManagedResourceCidrs	從範圍內 IPAM 集區分配之可管理資源 (VPC 或公有 IPv4 集區) 的資源 CIDR 數目。
NoncompliantResourceCidrs	不符合範圍內 IPAM 集區分配規則的資源 CIDR 數目。
OverlappingResourceCidrs	範圍內重疊的資源 CIDR 數目。
UnmanagedResourceCidrs	範圍內當前與可管理資源相關聯但不由 IPAM 管理的資源 CIDR 數目。

IPAM 公有 IP 指標

AWS/IPAM 命名空間包含下列 IPAM 公有 IP 指標。

指標名稱	說明
AmazonOwnedContigIPs	CIDR 中佈建至 IPAM 擁有、Amazon 提供之連續公有 IPv4 集區的 IP 位址數量。
AllocatedAmazonOwnedContigIPs	從 Amazon 提供的連續公有 IPv4 集區 CIDR 區塊配置的 IP 位址數量。
UnallocatedAmazonOwnedContigIPs	IPAM 擁有、Amazon 提供之連續公有 IPv4 集區 CIDR 區塊內的 IP 位址數量。
AssociatedAmazonOwnedContigIPs	從與彈性網路介面相關聯、Amazon 提供之連續公有 IPv4 集區 CIDR 區塊配置的彈性 IP 位址數量。
UnassociatedAmazonOwnedContigIPs	從未與彈性網路介面相關聯、Amazon 提供之連續公有 IPv4 集區 CIDR 區塊配置的彈性 IP 位址數量。

IPAM 字首清單解析程式指標

建議針對失敗指標設定 CloudWatch 警示，因為您可能需要重新評估與調整 IPAM 字首清單解析程式規則，以確保版本與字首清單大小在限制範圍內。

指標名稱	說明
IpamPrefixListResolverSyncFailure	字首清單解析程式與目標同步失敗。如果超過「每個字首清單解析程式版本的 CIDR 項目數量」等配額、找不到目標字首清單，或目標受管字首清單上的同步已停用，則可能會發生這種情況。
IpamPrefixListResolverSyncSuccess	字首清單解析程式已成功與目標同步。
IpamPrefixListResolverVersionCreationSuccess	版本建立成功。
IpamPrefixListResolverVersionCreationFailure	版本建立失敗。如果您已達到「每個字首清單解析程式版本的 CIDR 項目數量」配額，則可能會發生這種情況。

指標維度

若要篩選這些指標，請使用下列維度。

維度	說明
AddressFamily	資源 CIDR (IPv4 或 IPv6) 的 IP 地址系列。
Locale	IPAM 集區可供分配使用的 AWS 區域。
PoolID	集區的 ID。
ScopeID	範圍的 ID。

如需使用 Amazon CloudWatch 監控 VPC 的相關資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的 VPC 的 CloudWatch 指標。

IPAM 資源使用率指標

IPAM 會將 IPAM 監控之資源的 IP 使用率指標發佈至 Amazon CloudWatch。這些資源包括：

- VPC (IPv4 和 IPv6)
- 子網路 (IPv4)
- 公有 IPv4 集區

IPAM 會按 IP 地址系列 (IPv4 或 IPv6) 個別計算，並發佈 IP 使用率指標。資源的 IP 使用率是針對相同地址系列的所有 CIDR 進行計算。

針對每個資源類型和地址系列組合，IPAM 會使用三個規則來決定要發佈的指標：

- 最多 50 個 IP 使用率最高的資源。您可以使用此資訊設定警示，以便在超出 IP 使用率閾值時收到警示。
- 最多 50 個 IP 使用率最低的資源。您可以使用此資訊來決定要保留還是刪除未充分利用的資源。
- 最多 50 個其他資源。您可以使用此資訊來持續追蹤未在高使用率或低使用率群組中擷取之資源的 IP 使用率。
  - 最多 50 個 VPC，其中包含從 IPAM 集區配置的 CIDR (依 CIDR 區塊的大小總計排列優先順序)。

- 最多 50 個子網路，其 VPC 包含從 IPAM 集區配置的 CIDR (依 CIDR 區塊的大小總計排列優先順序)。
- 最多 50 個公有 IPv4 集區 ，其中包含從 IPAM 集區配置的 CIDR (依 CIDR 區塊的大小總計排列優先順序)。

套用每個規則之後，系統會針對每個資源類型，以相同的指標名稱彙總並發佈指標。如需有關指標名稱及其維度的詳細資訊，請參閱下方。

> **Important**
>
> 每個資源類型、地址系列和規則組合都有唯一的限制。每個限制的預設值為 50。您可以聯絡 AWS 支援中心 (如 AWS 一般參考 中的 AWS Service Quotas [服務配額] 所述) 來調整這些限制。

Example範例

假設您的 IPAM 可監控 2,500 個 VPC 和 10,000 個子網路，而且全都使用 IPv4 和 IPv6 CIDR。IPAM 會發佈下列 IP 使用率指標：

- 最多 150 個 VPC IPv4 IP 使用率的指標，包括：
  - IPv4 IP 使用率最高的 50 個 VPC
  - IPv4 使用率最低的 50 個 VPC
  - 最多 50 個 VPC，其中包含從 IPAM 集區配置的 IPv4 CIDR
- 最多 150 個 VPC IPv6 使用率的指標，包括：
  - IPv6 IP 使用率最高的 50 個 VPC
  - IPv6 使用率最低的 50 個 VPC
  - 最多 50 個 VPC，其中包含從 IPAM 集區配置的 IPv6 CIDR
- 最多 150 個子網路 IPv4 使用率的指標，包括：
  - IPv4 IP 使用率最高的 50 個子網路
  - IPv4 IP 使用率最低的 50 個子網路
  - 最多 50 個子網路，其 VPC 包含從 IPAM 集區配置的 IPv4 CIDR

VPC 指標

VPC 指標名稱和描述如下所列。

指標名稱	說明
VpcIPUsage	VPC 子網路中 CIDR 涵蓋的 IP 總數除以 VPC 中 CIDR 涵蓋的 IP 總數。這是針對相同 IPAM 範圍內的所有 VPC CIDR 進行計算，並針對 IPv4 和 IPv6 CIDR 分別計算。

您可以用來篩選 VPC 指標的維度列於下方。

維度	說明
AddressFamily	資源 CIDR (IPv4 或 IPv6) 的 IP 地址系列。
OwnerID	VPC 擁有者的 ID。
區域	VPC 所在的 AWS 區域。
ScopeID	VPC 所屬 IPAM 範圍的 ID。
VpcID	VPC 的 ID。

子網路指標

子網路指標名稱和描述如下所列。

指標名稱	說明
SubnetIPUsage	作用中 IP 的數目除以子網路的 IPv4 CIDR 中的 IP 總數。

您可以用來篩選子網路指標的維度列於下方。

維度	說明
AddressFamily	資源 CIDR 的 IP 地址系列 (僅限 IPv4)。

維度	說明
OwnerID	子網路擁有者的 ID。
區域	子網路所在的 AWS 區域。
ScopeID	子網路所屬 IPAM 範圍的 ID。
SubnetID	子網路的 ID。
VpcID	子網路所屬 VPC 的 ID。

公有 IPv4 集區指標

公有 IPv4 集區指標名稱和描述如下所列。

指標名稱	說明
PublicIPv4PoolIPUsage	公有 IPv4 集區中的 EIP 數目除以集區中的 IP 總數。

您可以用來篩選公有 IPv4 集區指標的維度列於下方。

維度	Description
OwnerID	公有 IPv4 集區擁有者的 ID。
PublicIPv4PoolID	公有 IPv4 集區的 ID。
區域	公有 IPv4 集區所在的 AWS 區域。
ScopeID	公有 IPv4 集區所屬 IPAM 範圍的 ID。

公共 IP 洞察功能指標

下方列出公共 IP 洞察功能指標名稱和說明。

指標名稱	說明
AmazonOwnedElasticIPs	已佈建或指派給 AWS 帳戶中資源之 Amazon 擁有的彈性 IP 地址數目。
AssociatedAmazonOwnedElasticIPs	已與 AWS 帳戶中資源關聯之 Amazon 擁有的彈性 IP 地址數目。
AssociatedBringYourOwnIPs	已使用自備 IP 地址 (BYOIP) 帶入 AWS 且已與 AWS 帳戶中之資源關聯的公有 IPv4 地址數目。
BringYourOwnIPs	已使用自備 IP 地址 (BYOIP) 帶入 AWS 之公有 IPv4 地址的數目。
EC2PublicIPs	執行個體啟動到預設子網路，或者執行個體啟動到已設定為自動指派公有 IPv4 地址的子網路時，指派給 EC2 執行個體之公有 IPv4 地址的數目。
ServiceManagedBringYourOwnIPs	已使用自備 IP 地址 (BYOIP) 帶入 AWS 且由 AWS 服務佈建和管理之公有 IPv4 地址的數目。
ServiceManagedIPs	由 AWS 服務佈建和管理之公有 IPv4 地址的數目。
UnassociatedAmazonOwnedElasticIPs	未與 AWS 帳戶中資源關聯之 Amazon 擁有的彈性 IP 地址數目。
UnassociatedBringYourOwnIPs	已使用自備 IP 地址 (BYOIP) 帶入 AWS 且未與 AWS 帳戶中之任何資源關聯的公有 IPv4 地址數目。

用於篩選公共 IP 洞察功能指標的維度如下所列。

維度	說明
IpamId	IP 地址所屬 IPAM 的 ID。
區域	公有 IP 地址所在的 AWS 區域。

建立警示的快速提示

若要為 IP 地址使用率高的資源快速建立 Amazon CloudWatch 警示，請開啟 CloudWatch 主控台，依序選擇 Metrics (指標)、All metrics (所有指標)、Query (查詢) 索引標籤、Namespace (命名空間) `AWS/IPAM > VPC IP Usage Metrics`、`AWS/IPAM > Subnet IP Usage Metrics`，或 `AWS/IPAM > Public IPv4 Pool IP Usage Metrics`，選擇 Metric name (指標名稱) `MAX(VpcIPUsage)`、`MAX(SubnetIPUsage)` 或 `MAX(PublicIPv4PoolIPUsage)`，然後選擇 Create alarm (建立警示)。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的在 Metrics Insights 查詢上建立警示。

檢視 IP 位址歷程記錄

請依照本節中的步驟檢視 IPAM 範圍中的 IP 地址或 CIDR 歷程記錄。您可使用歷程資料來分析和稽核網路安全和路由政策。IPAM 最長可自動保留您的 IP 地址監控資料三年。

您可使用 IP 歷程記錄資料來搜尋下列資源類型的 IP 地址或 CIDR 狀態變更：

- VPC
- VPC 子網路
- 彈性 IP 位址
- EC2 執行個體
- 連接至執行個體的 EC2 網路介面

> **Important**
>
> 雖然 IPAM 不會監控 Amazon EC2 執行個體或連接至介面的 EC2 網路介面，但您可使用搜尋 IP 歷史記錄功能來搜尋 EC2 執行個體和網路介面 CIDR 的相關歷程資料。

> **Note**
>
> - 若您將資源從一個 IPAM 範圍移至另一個範圍，則先前的歷程記錄會結束，且會在新的範圍下建立新的歷程記錄。如需詳細資訊，請參閱在各範圍之間移動 VPC CIDR。
> - 如果您刪除資源或將資源轉移到不受 IPAM 監控 AWS 的帳戶，則與資源相關的任何新歷史記錄都不會顯示，而且您的 IPAM 不會監控資源。不過，資源的 IP 位址仍然可以搜尋。

- 如果您將 IPAM 與組織外的帳戶整合，IPAM 擁有者可以檢視這些帳戶擁有的所有資源 CIDR 的 IP 位址歷史記錄。

AWS Management Console

檢視 CIDR 的歷程記錄

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇搜尋 IP 歷史記錄。
3. 輸入 IPv4 或 IPv6 IP 地址或 CIDR。這必須是資源使用的明確 CIDR。
4. 選擇 IPAM 範圍 ID。
5. 選擇日期/時間範圍。
6. 若您要依 VPC 篩選結果，請輸入 VPC ID。若 CIDR 出現在多個 VPC 中，請使用此選項。
7. 選擇 Search (搜尋)。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

- 檢視 CIDR 的歷程記錄：get-ipam-address-history

若要查看如何使用 AWS CLI 分析和稽核 IP 地址用量的範例，請參閱教學課程：使用 檢視 IP 地址歷史記錄 AWS CLI。

搜尋結果會整理成下列欄位：

- Sampled end time (抽樣結束時間)：IPAM 範圍內資源與 CIDR 關聯的抽樣結束時間。會從定期快照中取用變更，因此結束時間可能在此特定時間之前。
- Sampled start time (抽樣開始時間)：IPAM 範圍內資源與 CIDR 關聯的抽樣開始時間。會從定期快照中取用變更，因此開始時間可能在此特定時間之前。

Example

為了協助解說您在 Sampled start time (抽樣開始時間) 和 Sampled end time (抽樣結束時間) 下看到的時間，讓我們探討一下使用案例的範例：

在下午 2 點使用 CIDR 10.0.0.0/16 建立了 VPC。在下午 3 點使用 CIDR 10.0.0.0/8 建立 IPAM 和 IPAM 集區，然後選取自動匯入選項以允許 IPAM 探索及匯入位於 10.0.0.0/8 IP 地址範圍內的任何 CIDR。由於 IPAM 會取用定期快照中的 CIDR 變更，因此它到了下午 3:05 才探索到現有的 VPC CIDR。當您使用搜尋 IP 歷史記錄功能搜尋此 VPC 的 ID 時，VPC 的抽樣開始時間為下午 3:05 (IPAM 探索到它的時間)，而不是下午 2:00 (您建立 VPC 時的時間)。現在，假設您決定在下午 5 點刪除 VPC。刪除 VPC 時，配置給 VPC 的 CIDR 10.0.0.0/16 會由 IPAM 集區回收使用。IPAM 會在下午 5:05 拍攝定期快照並取用變更。當您在搜尋 IP 歷史記錄中搜尋此 VPC 的 ID 時，VPC CIDR 的抽樣結束時間是下午 5:05，而不是刪除 VPC 的時間下午 5:00。

- Resource ID (資源 ID)：建立資源與 CIDR 之間的關聯時產生的 ID。
- Name (名稱)：資源的名稱 (如果適用)。
- Compliance status (合規狀態)：CIDR 的合規狀態。
  - Compliant (合規)：受管的資源符合 IPAM 集區的配置規則。
  - 不合規：資源 CIDR 不符合 IPAM 集區的一或多項配置規則。

    Example

    如果 VPC 的 CIDR 不符合 IPAM 集區的網路遮罩長度參數，或者資源不在與 IPAM 集區相同的 AWS 區域中，則會將其標記為不合規。
  - 未受管：資源沒有從 IPAM 集區配置的 CIDR，而且 IPAM 不會監控其是否有符合集區配置規則的潛在 CIDR。監控 CIDR 是否有重疊。
  - Ignored (已忽略)：受管的資源已被選擇為免於監控。不會評估已忽略的資源是否有重疊或符合配置規則。選擇忽略資源時，從 IPAM 集區配置給該資源的任何空間都會傳回至集區，而且不會透過自動匯入再次將該資源匯入 (如果已設定集區的自動匯入配置規則)。
  - -：此資源不是 IPAM 可以監控或管理的資源類型之一。
- Overlap status (重疊狀態)：CIDR 的重疊狀態。
  - Nonoverlapping (不重疊)：資源 CIDR 不會重疊在相同範圍內的另一個 CIDR。
  - Overlapping (重疊)：資源 CIDR 與相同範圍內的另一個 CIDR 相互重疊。請注意，如果資源 CIDR 重疊，則可能會與手動配置重疊。
  - Ignored (已忽略)：受管的資源已被選擇為免於監控。IPAM 不會評估已忽略的資源是否有重疊或符合配置規則。選擇忽略資源時，從 IPAM 集區配置給該資源的任何空間都會傳回至集區，而且不會透過自動匯入再次將該資源匯入 (如果已設定集區的自動匯入配置規則)。
  - -：此資源不是 IPAM 可以監控或管理的資源類型之一。
- Resource Type (資源類型)

  - VPC：CIDR 與 VPC 相關聯。
  - subnet (子網路)：CIDR 與 VPC 子網路相關聯。
  - EIP：CIDR 與彈性 IP 地址相關聯。
  - instance (執行個體)：CIDR 與 EC2 執行個體相關聯。
  - network-interface (網路介面)：CIDR 與網路介面相關聯。
- VPC ID：此資源所屬 VPC 的 ID (如果適用)。
- 區域：此資源 AWS 的區域。
- 擁有者 ID：建立此資源之使用者 AWS 的帳戶 ID （如適用）。

檢視公有 IP 深入解析

您可以使用 公共 IP 洞察功能 來查看下列資訊：

- 如果您的 IPAM 已與 AWS Organization 中的帳戶整合，您可以檢視整個 AWS Organization 所有 AWS 區域中服務使用的所有公有 IPv4 地址。
- 如果您的 IPAM 已與單一帳戶整合，您可以檢視 服務在帳戶中所有 AWS 區域中使用的所有公有 IPv4 地址。

公有 IPv4 地址是可從網際網路路由的 IPv4 地址。若要透過 IPv4 從網際網路直接存取資源，必須使用公有 IPv4 地址。

> **Note**
>
> AWS 收取所有公有 IPv4 地址的費用，包括與執行中執行個體相關聯的公有 IPv4 地址和彈性 IP 地址。如需詳細資訊，請參閱 Amazon VPC 定價頁面中的公有 IPv4 地址。

您可以檢視下列公有 IPv4 地址類型的深入解析：

- 彈性 IP 地址 EIPs)：Amazon 提供的靜態公有 IPv4 地址，您可以與 EC2 執行個體、彈性網路介面或 AWS 資源建立關聯。
- EC2 公有 IPv4 地址：Amazon 指派給 EC2 執行個體的公有 IPv4 地址 (如果 EC2 執行個體啟動到預設子網路，或者如果執行個體啟動到已設定為自動指派公有 IPv4 地址的子網路)。
- BYOIPv4 地址：在您 AWS 使用自有 IPv4 地址 (BYOIP) 帶至 的 IPv4 地址範圍內的公有 IPv4 地址。 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html

- 服務受管 IPv4 地址：公有 IPv4 地址會自動佈建在 AWS 資源上，並由 AWS 服務管理。例如，Amazon ECS、Amazon RDS 或 Amazon WorkSpaces 上的公有 IPv4 地址。

公共 IP 洞察功能會顯示區域內的服務使用的所有公有 IPv4 地址。您可以使用這些深入解析來識別公有 IPv4 地址使用情況，並檢視釋出未使用之彈性 IP 地址的建議。

- 公有 IP 類型：依類型組織的公有 IPv4 地址數目。
  - Amazon 擁有EIPs：您已佈建或指派給 AWS 帳戶中資源的彈性 IP 地址。
  - EC2 公有 IP：當執行個體啟動到預設子網路，或者當執行個體啟動到已設定為自動指派公有 IPv4 地址的子網路時，指派給 EC2 執行個體的公有 IPv4 地址。
  - BYOIP：您已 AWS 使用自有 IP 地址 (BYOIP) 帶至 的公有 IPv4 地址。
  - 服務受管 IPs：由 AWS 服務佈建和管理的公有 IPv4 地址。
  - 服務受管 BYOIP：將公有 IPv4 地址帶到 AWS 服務 AWS 並由 管理。
  - Amazon 擁有的連續 EIP：從 Amazon 提供的連續公有 IPv4 IPAM 集區配置的彈性 IP 位址。
- EIP 使用量：彈性 IP 地址的使用方式組織的數目。
  - 關聯的 Amazon 擁有 EIPs：您在 AWS 帳戶中佈建的彈性 IP 地址，以及與 EC2 執行個體、網路介面或 AWS 資源相關聯的彈性 IP 地址。
  - 關聯的 BYOIP：您已 AWS 使用與網路介面相關聯的 BYOIP 帶到 的公有 IPv4 地址。
  - 未關聯的 Amazon 擁有EIPs：您在 AWS 帳戶中佈建但尚未與網路介面相關聯的彈性 IP 地址。
  - 未關聯的 BYOIP：您已 AWS 使用 BYOIP 帶到 的公有 IPv4 地址，但尚未與網路介面建立關聯。
  - 關聯的 Amazon 擁有的連續 EIP：從 Amazon 提供的連續公有 IPv4 IPAM 集區配置並與資源相關聯的彈性 IP 位址。
  - 未關聯的 Amazon 擁有的連續 EIP：從 Amazon 提供的連續公有 IPv4 IPAM 集區配置的彈性 IP 位址，並且未與資源建立關聯。
- Amazon 擁有的 IPv4 連續 IP 用量：顯示一段時間內連續公有 IPv4 地址用量和相關 Amazon 擁有的 IPv4 IPAM 集區的資料表。
- 公有 IP 地址：公有 IPv4 地址及其屬性的表格。
  - IP 地址：公有 IPv4 地址。
  - 已關聯：地址是否與 EC2 執行個體、網路介面或 AWS 資源相關聯。
    - 已關聯：公有 IPv4 地址與 EC2 執行個體、網路介面或 AWS 資源相關聯。
    - 未關聯：公有 IPv4 地址未與任何資源建立關聯，且在您的 AWS 帳戶中處於閒置狀態。
  - 地址類型：IP 地址類型。

  - Amazon 擁有的 EIP：公有 IPv4 地址是彈性 IP 地址。
  - BYOIP： AWS 使用 BYOIP 將公有 IPv4 地址帶到 。
  - EC2 公有 IP：自動指派給 EC2 執行個體的公有 IPv4 地址。
  - 服務受管 BYOIP：公有 IPv4 地址是 AWS 使用自有 IP (BYOIP) 帶至 。
  - 服務受管 IP：公有 IPv4 地址已佈建，並由 AWS 服務管理。
- 服務：與 IP 地址相關聯的服務。
  - AGA： AWS Global Accelerator如果使用自訂路由加速器，則不會列出其公有 IP。若要檢視這些公有 IP，請參閱檢視您的自訂路由加速器。
  - Database Migration Service：An AWS Database Migration Service (DMS) 複寫執行個體。
  - Redshift：Amazon Redshift 叢集。
  - RDS：Amazon Relational Database Service (RDS) 執行個體。
  - 負載平衡器 (EC2)：Application Load Balancer 或 Network Load Balancer。
  - NAT 閘道 (VPC)：Amazon VPC 公有 NAT 閘道。
  - Site-to-Site VPN： AWS Site-to-Site VPN 虛擬私有閘道。
  - 其他：目前無法識別的其他服務。
- 名稱 (EIP ID)：如果此公有 IPv4 地址是彈性 IP 地址配置，則這是 EIP 配置的名稱和 ID。
- 網路界面 ID：如果此公有 IPv4 地址與網路界面相關聯，則這是網路界面的 ID。
- 執行個體 ID：如果此公有 IPv4 地址與 EC2 執行個體相關聯，則這是執行個體 ID。
- 安全群組：如果此公有 IPv4 地址與 EC2 執行個體相關聯，則這是指派給執行個體之安全群組的名稱和 ID。
- 公有 IPv4 集區：如果這是來自 Amazon 擁有並管理之 IP 地址集區的彈性 IP 地址，則值為「-」。如果這是來自您擁有並帶到 Amazon (使用 BYOIP) 之 IP 地址範圍的彈性 IP 地址，則值為公有 IPv4 集區 ID。
- 網路邊界群組：如果公告 IP 地址，這是公告 IP 地址 AWS 的區域。
- 擁有者 ID：資源擁有者的 AWS 帳號。
- 範例時間：上次成功檢索資源的時間。
- 資源探索 ID：探索到此公有 IPv4 地址的資源探索 ID。
- 服務資源：資源 ARN 或 ID。

如果彈性 IP 地址分配到您的帳戶，但與網路界面沒有關聯，則會出現一個橫幅，通知您帳戶中有未關聯的 EIP，且您應該釋出這些 EIP。

> **Important**
>
> 公共 IP 洞察功能最近已更新。如果看到與沒有呼叫 GetIpamDiscoveredPublicAddresses 的許可相關的錯誤，則需要更新連接到與您共用之資源探索的受管許可。聯絡建立資源探索的人員，並要求他們將受管許可 `AWSRAMPermissionIpamResourceDiscovery` 更新為預設版本。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的更新資源共用。

AWS Management Console

若要檢視公有 IP 地址深入解析

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇 Public IP insights (公有 IP 深入解析)。
3. 若要檢視公有 IP 地址的詳細資訊，請按一下 IP 地址以選取該 IP 地址。
4. 檢視 IP 地址的下列相關資訊：
   - 詳細資訊：可以在「主要公有 IP 深入解析」窗格欄位中看到的相同資訊，例如 Address type (地址類型) 和 Service (服務)。
   - 傳入安全群組規則：如果此 IP 地址與 EC2 執行個體相關聯，則這些是控制執行個體傳入流量的安全群組規則。
   - 傳出安全群組規則：如果此 IP 地址與 EC2 執行個體相關聯，則這些是控制執行個體傳出流量的安全群組規則。
   - 標籤：做為中繼資料以組織 AWS 資源的金鑰和值對。

Command line

使用下列命令取得 IPAM 探索到的公有 IP 地址：get-ipam-discovered-public-addresses

Amazon VPC IP 地址管理員教學課程

以下教學課程說明如何使用 AWS CLI 執行常見的 IPAM 任務。若要取得 AWS CLI，請參閱 存取 IPAM。如需有關這些教學課程中提及之 IPAM 概念的詳細資訊，請參閱 IPAM 的運作方式。

目錄

透過 AWS CLI 開始使用 IPAM

本教學課程引導您在單一 AWS 帳戶中，透過 AWS CLI 設定與使用 Amazon VPC IP 位址管理器 (IPAM)。到本教學課程結束時，您將已建立 IPAM、IP 位址集區階層，並將 CIDR 配置給 VPC。

必要條件

在開始本教學課程之前，請確認已滿足以下條件：

- 具有建立與管理 IPAM 資源之許可的 AWS 帳戶。
- 已安裝 AWS CLI，並已使用正確的憑證完成設定。如需有關安裝 AWS CLI 的資訊，請參閱 Installing or updating the latest version of the AWS CLI。如需有關設定 AWS CLI 的資訊，請參閱 Configuration basics。
- 基本了解 IP 定址與 CIDR 標記法。
- 基本了解 Amazon VPC 概念。
- 完成本教學課程大約需要 30 分鐘。

建立 IPAM

第一步是建立具有作業區域的 IPAM。IPAM 可協助規劃、追蹤與監控 AWS 工作負載的 IP 位址。

建立在 us-east-1 與 us-west-2 中具有作業區域的 IPAM：

```
aws ec2 create-ipam \
  --description "My IPAM" \
  --operating-regions RegionName=us-east-1 RegionName=us-west-2
```

此命令會建立 IPAM，並使其能夠管理指定區域中的 IP 位址。作業區域是允許 IPAM 管理 IP 位址 CIDR 的 AWS 區域。

確認您的 IPAM 已建立：

```
aws ec2 describe-ipams
```

請記下輸出中的 IPAM ID，因為後續步驟會需要它。

等待 IPAM 完全建立並可用 (約 20 秒)：

```
sleep 20
```

取得 IPAM 範圍 ID

您建立 IPAM 時，AWS 會自動建立一個私有範圍和一個公有範圍。在本教學課程中，我們將使用私有範圍。

擷取 IPAM 詳細資訊與私有範圍 ID：

```
aws ec2 describe-ipams --ipam-id ipam-0abcd1234
```

將 `ipam-0abcd1234` 取代為實際的 IPAM ID。

根據輸出內容，識別並記下 `PrivateDefaultScopeId` 欄位中的私有範圍 ID。這看起來會像是 `ipam-scope-0abcd1234`。

建立頂層 IPv4 集區

現在，在私有範圍內建立頂層集區。此集區將作為階層中所有其他集區的父集區。

建立頂層 IPv4 集區：

```
aws ec2 create-ipam-pool \
  --ipam-scope-id ipam-scope-0abcd1234 \
  --address-family ipv4 \
  --description "Top-level pool"
```

將 ipam-scope-0abcd1234 取代為實際的私有範圍 ID。

等待集區完全建立並可用：

```
aws ec2 describe-ipam-pools --ipam-pool-ids ipam-pool-0abcd1234 --query
 'IpamPools[0].State' --output text
```

將 ipam-pool-0abcd1234 取代為實際的頂層集區 ID。狀態變為 create-complete 後，再繼續操作。

集區可用後，為其佈建 CIDR 區塊：

```
aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id ipam-pool-0abcd1234 \
  --cidr 10.0.0.0/8
```

等待 CIDR 完全佈建：

```
aws ec2 get-ipam-pool-cidrs --ipam-pool-id ipam-pool-0abcd1234 --query "IpamPoolCidrs[?
Cidr=='10.0.0.0/8'].State" --output text
```

狀態變為 provisioned 後，再繼續操作。

建立區域 IPv4 集區

然後，在最上層集區內建立一個區域集區。此集區將專屬於特定 AWS 區域。

建立區域 IPv4 集區：

```
aws ec2 create-ipam-pool \
  --ipam-scope-id ipam-scope-0abcd1234 \
  --source-ipam-pool-id ipam-pool-0abcd1234 \
  --locale us-east-1 \
  --address-family ipv4 \
```

```
  --description "Regional pool in us-east-1"
```

將 ipam-scope-0abcd1234 取代為實際的私有範圍 ID，並將 ipam-pool-0abcd1234 取代為頂層集區 ID。

等待區域集區完全建立並可用：

```
aws ec2 describe-ipam-pools --ipam-pool-ids ipam-pool-1abcd1234 --query
 'IpamPools[0].State' --output text
```

將 ipam-pool-1abcd1234 取代為實際的區域集區 ID。狀態變為 create-complete 後，再繼續操作。

集區可用後，為其佈建 CIDR 區塊：

```
aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id ipam-pool-1abcd1234 \
  --cidr 10.0.0.0/16
```

等待 CIDR 完全佈建：

```
aws ec2 get-ipam-pool-cidrs --ipam-pool-id ipam-pool-1abcd1234 --query "IpamPoolCidrs[?
Cidr=='10.0.0.0/16'].State" --output text
```

狀態變為 provisioned 後，再繼續操作。

建立開發 IPv4 集區

現在，在區域集區內建立開發集區。此集區將用於開發環境。

建立開發 IPv4 集區：

```
aws ec2 create-ipam-pool \
  --ipam-scope-id ipam-scope-0abcd1234 \
  --source-ipam-pool-id ipam-pool-1abcd1234 \
  --locale us-east-1 \
  --address-family ipv4 \
  --description "Development pool"
```

將 ipam-scope-0abcd1234 取代為實際的私有範圍 ID，並將 ipam-pool-1abcd1234 取代為區域集區 ID。

注意：請務必包含 `--locale` 參數，以符合父集區的地區設定。

等待開發集區完全建立並可用：

```
aws ec2 describe-ipam-pools --ipam-pool-ids ipam-pool-2abcd1234 --query
 'IpamPools[0].State' --output text
```

將 `ipam-pool-2abcd1234` 取代為實際的開發集區 ID。狀態變為 `create-complete` 後，再繼續操作。

集區可用後，為其佈建 CIDR 區塊：

```
aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id ipam-pool-2abcd1234 \
  --cidr 10.0.0.0/24
```

等待 CIDR 完全佈建：

```
aws ec2 get-ipam-pool-cidrs --ipam-pool-id ipam-pool-2abcd1234 --query "IpamPoolCidrs[?
Cidr=='10.0.0.0/24'].State" --output text
```

狀態變為 `provisioned` 後，再繼續操作。

建立使用 IPAM 集區 CIDR 的 VPC

最後，建立使用 IPAM 集區 CIDR 的 VPC。下面示範如何使用 IPAM 將 IP 位址空間配置給 AWS 資源。

建立使用 IPAM 集區 CIDR 的 VPC：

```
aws ec2 create-vpc \
  --ipv4-ipam-pool-id ipam-pool-2abcd1234 \
  --ipv4-netmask-length 26 \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=IPAM-VPC}]'
```

將 `ipam-pool-2abcd1234` 取代為實際的開發集區 ID。

`--ipv4-netmask-length 26` 參數表示您希望從集區配置 /26 CIDR 區塊 (64 個 IP 位址)。系統會選擇此網路遮罩長度，確保其小於集區的 CIDR 區塊 (/24)。

確認您的 VPC 已建立：

```
aws ec2 describe-vpcs --filters "Name=tag:Name,Values=IPAM-VPC"
```

驗證 IPAM 集區配置

檢查 CIDR 是否已從 IPAM 集區配置：

```
aws ec2 get-ipam-pool-allocations \
  --ipam-pool-id ipam-pool-2abcd1234
```

將 `ipam-pool-2abcd1234` 取代為實際的開發集區 ID。

此命令會顯示來自指定 IPAM 集區的所有配置，包括您剛建立的 VPC。

疑難排解

以下是使用 IPAM 時可能遇到的一些常見問題：

- 許可錯誤：確保您的 IAM 使用者或角色具有建立與管理 IPAM 資源所需的許可。您可能需要 `ec2:CreateIpam`、`ec2:CreateIpamPool` 及其他相關許可。
- 超過資源限制：依預設，每個帳戶只能建立一個 IPAM。如果您已經有 IPAM，則需要先將其刪除，然後再建立新的 IPAM，或使用現有的 IPAM。
- CIDR 配置失敗：將 CIDR 佈建至集區時，請確保您嘗試佈建的 CIDR 不會與其他集區中的現有配置重疊。
- API 請求逾時：如果您遇到 "RequestExpired" 錯誤，可能是因為網路延遲或時間同步問題。再次嘗試命令。
- 狀態錯誤：如果您收到 "IncorrectState" 錯誤，可能是因為您嘗試對未處於正確狀態的資源執行操作。等待資源完全建立或佈建，然後再繼續。
- 配置大小錯誤：如果您收到有關配置大小的 "InvalidParameterValue" 錯誤，請確保您請求的網路遮罩長度適合集區大小。例如，您無法從 /24 集區配置 /25 CIDR。
- 相依性違規：清除資源時，您可能會遇到 "DependencyViolation" 錯誤。這是因為資源彼此具有相依性。刪除集區之前，請務必以建立和取消佈建 CIDR 的相反順序刪除資源。

清除資源

完成本教學課程後，您應該清理所建立的資源，以避免產生不必要的費用。

1. 刪除 VPC

```
aws ec2 delete-vpc --vpc-id vpc-0abcd1234
```

2. 取消佈建開發集區的 CIDR：

```
aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id ipam-pool-2abcd1234 --cidr
 10.0.0.0/24
```

3. 刪除開發集區：

```
aws ec2 delete-ipam-pool --ipam-pool-id ipam-pool-2abcd1234
```

4. 取消佈建區域集區的 CIDR：

```
aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id ipam-pool-1abcd1234 --cidr
 10.0.0.0/16
```

5. 刪除區域集區：

```
aws ec2 delete-ipam-pool --ipam-pool-id ipam-pool-1abcd1234
```

6. 取消佈建頂層集區的 CIDR：

```
aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id ipam-pool-0abcd1234 --cidr
 10.0.0.0/8
```

7. 刪除頂層集區：

```
aws ec2 delete-ipam-pool --ipam-pool-id ipam-pool-0abcd1234
```

8. 刪除 IPAM：

```
aws ec2 delete-ipam --ipam-id ipam-0abcd1234
```

將所有 ID 取代為實際的資源 ID。

> **Note**
>
> 在這些操作之間，您可能需要等待資源完全刪除，然後再繼續進行下一個步驟。如果您遇到相依性違規，請等待幾秒鐘，然後再試一次。

後續步驟

現在您已了解如何透過 AWS CLI 建立與使用 IPAM，您可能想要探索更進階的功能：

- 規劃 IP 地址佈建 – 了解如何有效地規劃 IP 位址空間
- 依資源監控 CIDR 使用情況 – 了解如何監控 IP 位址用量
- 透過 AWS RAM 共用 IPAM 集區 – 了解如何跨 AWS 帳戶共用 IPAM 集區
- 將 IPAM 與 AWS Organizations 中的帳戶整合 – 探索如何在組織中使用 IPAM

教學課程：使用主控台建立 IPAM 和集區

在本教學課程中，您會建立 IPAM、與 整合 AWS Organizations、建立 IP 地址集區，以及從 IPAM 集區建立具有 CIDR 的 VPC。

本教學課程將說明如何根據不同的開發需求，使用 IPAM 組織 IP 地址空間。完成本教學課程後，您將會擁有適用於生產前資源的 IP 地址集區。接著，您可以根據路由和安全性需求 (例如，適用於生產資源的集區) 來建立其他集區。

雖然您可以使用 IPAM 做為單一使用者，但與 整合 AWS Organizations 可讓您管理組織中跨帳戶的 IP 地址。本教學課程涵蓋如何將 IPAM 與組織中的帳戶整合。其中未涵蓋如何 將 IPAM 與組織外的帳戶整合。

> **Note**
>
> 針對本教學課程的用途部分，我們將說明如何以特定方式為 IPAM 資源命名、在特定區域建立 IPAM 資源，以及針對集區使用特定 IP 地址 CIDR 範圍。其目的在於簡化 IPAM 中可用的選擇，讓您能夠快速開始使用 IPAM。完成本教學課程後，您可決定以不同方式建立新的 IPAM 並加以設定。

目錄

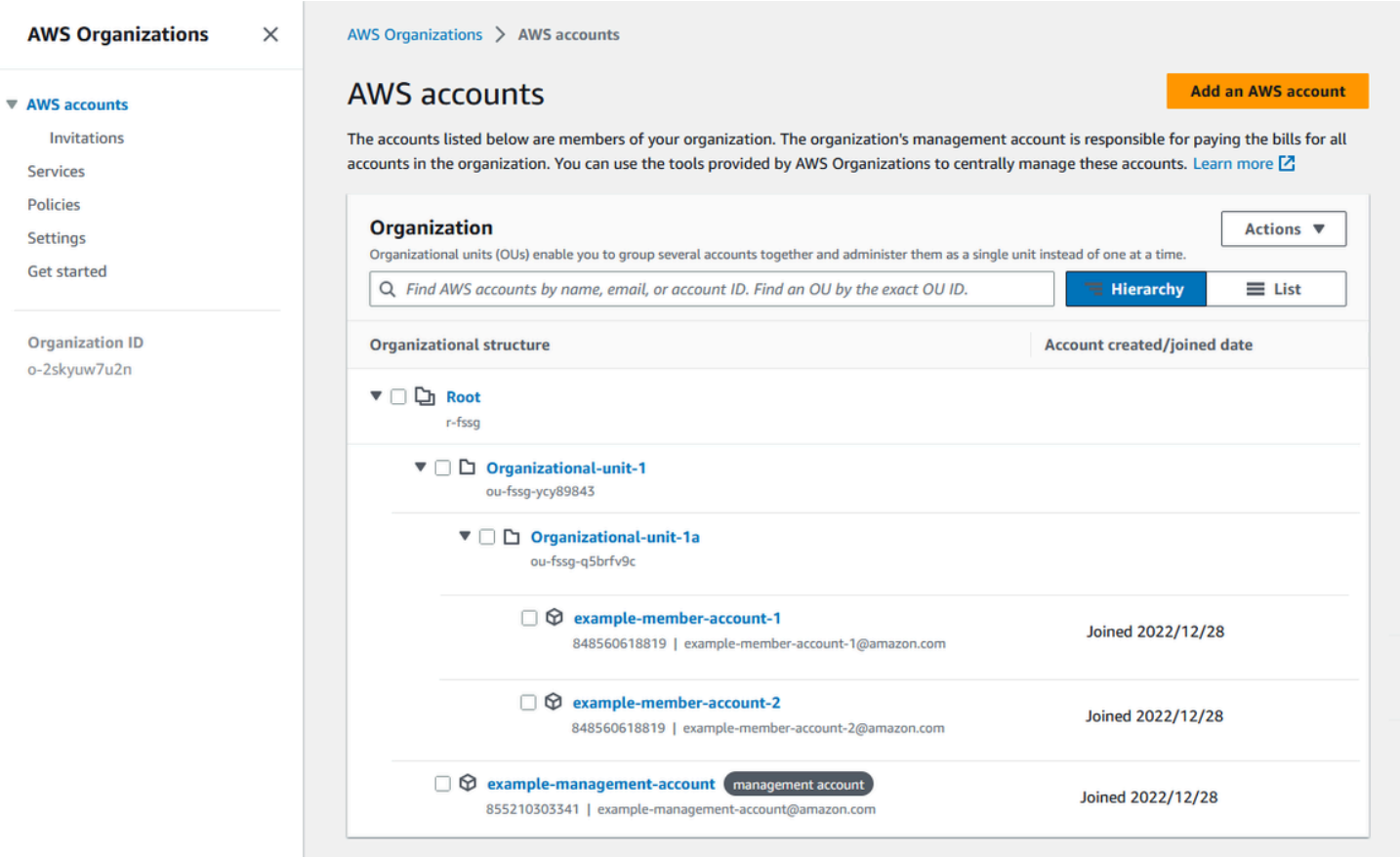
先決條件

開始之前，您必須已設定具有至少一個成員 AWS Organizations 帳戶的 帳戶。如需操作方式說明，請參閱《AWS Organizations 使用者指南》中的建立和管理組織。

如何與 IPAM AWS Organizations 整合

本節顯示您在本教學課程中使用 AWS Organizations 的帳戶範例。以下將說明您會在本教學課程中整合 IPAM 時使用的三個組織中帳戶：

- 用於登入 IPAM 主控台和委派 IPAM 管理員的管理帳戶 (下圖中稱為 example-management-account)。您無法使用組織的管理帳戶作為 IPAM 管理員。
- 作為 IPAM 管理員帳戶的成員帳戶 (下圖中稱為 example-member-account-1)。IPAM 管理員帳戶負責建立 IPAM，並使用 IPAM 管理和監控組織內 IP 地址使用情況。組織中的任何成員帳戶皆可以委派為 IPAM 管理員。
- 作為開發人員帳戶的成員帳戶 (下圖上方稱為 example-member-account-2)。此帳戶會使用從 IPAM 集區配置的 CIDR 建立 VPC。



除上述帳戶之外，您還需要組織單位的 ID (上圖的 ou-fssg-q5brfv9c)，其中包含您將用作為開發人員帳戶的成員帳戶。在後續分享 IPAM 集區的步驟中，您將會需要此 ID，才可與該 OU 進行分享。

> **Note**
>
> 如需管理和成員 AWS Organizations 帳戶等帳戶類型的詳細資訊，請參閱AWS Organizations 術語和概念。

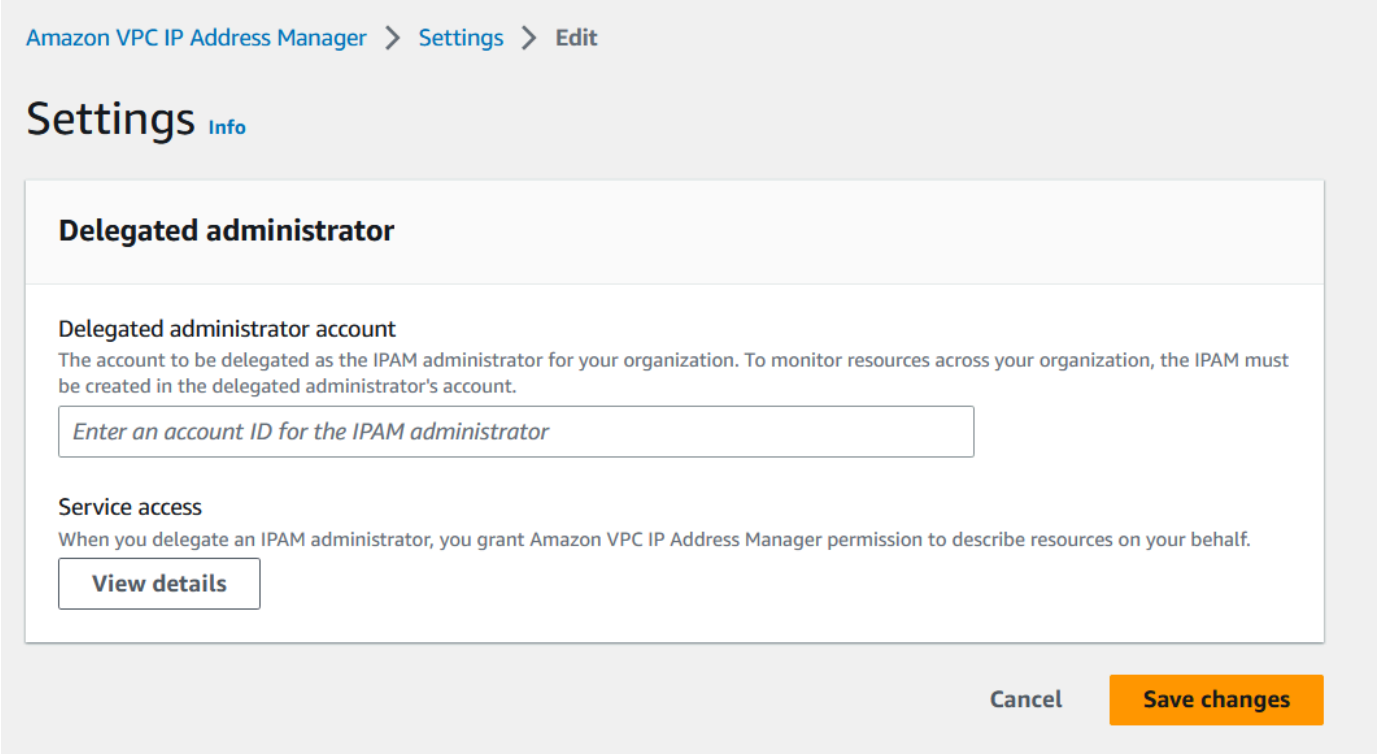
步驟 1：委派 IPAM 管理員

在此步驟中，您將委派 AWS Organizations 成員帳戶做為 IPAM 管理員。當您委派 IPAM 管理員時，服務連結角色會自動在每個 AWS Organizations 成員帳戶中建立。IPAM 會擔任每個成員帳戶中的服務連結角色，以監控這些帳戶中的 IP 地址使用情況。接著，無論其組織單位為何，IPAM 皆可以探索資源與其 CIDR。

除非您具有必要的 AWS Identity and Access Management (IAM) 許可，否則無法完成此步驟。如需詳細資訊，請參閱將 IPAM 與 AWS Organizations 中的帳戶整合。

委派 IPAM 管理員帳戶

1. 使用 AWS Organizations 管理帳戶，在 https：//https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在 中 AWS 管理主控台，選擇您要在其中使用 IPAM AWS 的區域。
3. 在導覽窗格中，選擇 Organization settings (組織設定)。
4. 選擇委派。委派選項只有在您以 AWS Organizations 管理帳戶身分登入 主控台時才能使用。
5. 輸入組織成員 AWS 帳戶的帳戶 ID。IPAM 管理員必須是 AWS Organizations 成員帳戶，而不是管理帳戶。



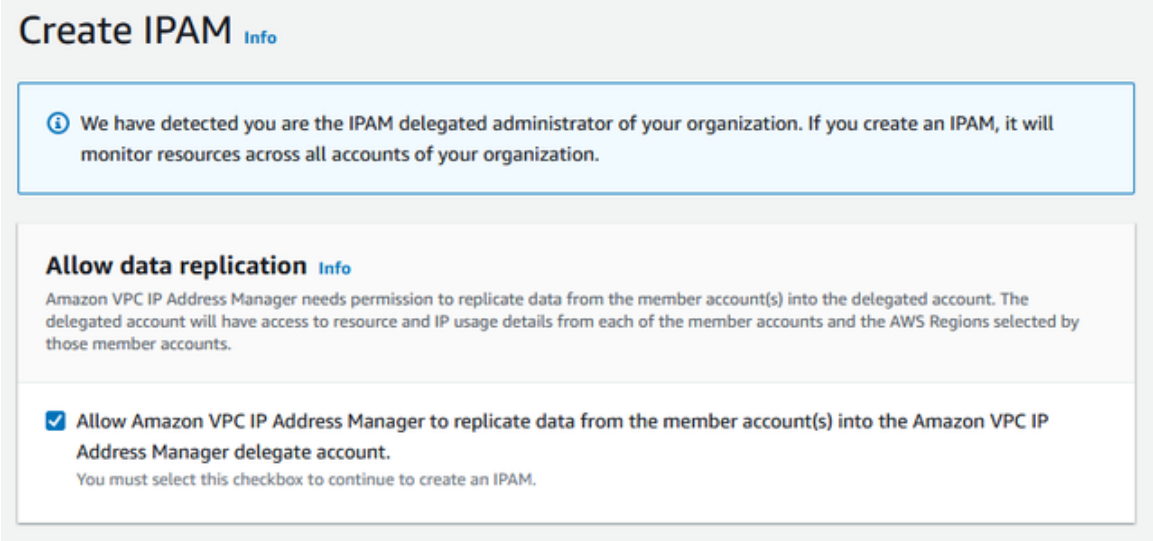
6. 選擇儲存變更。委派的管理員資訊會填入與成員帳戶相關的詳細資料。

步驟 2：建立 IPAM

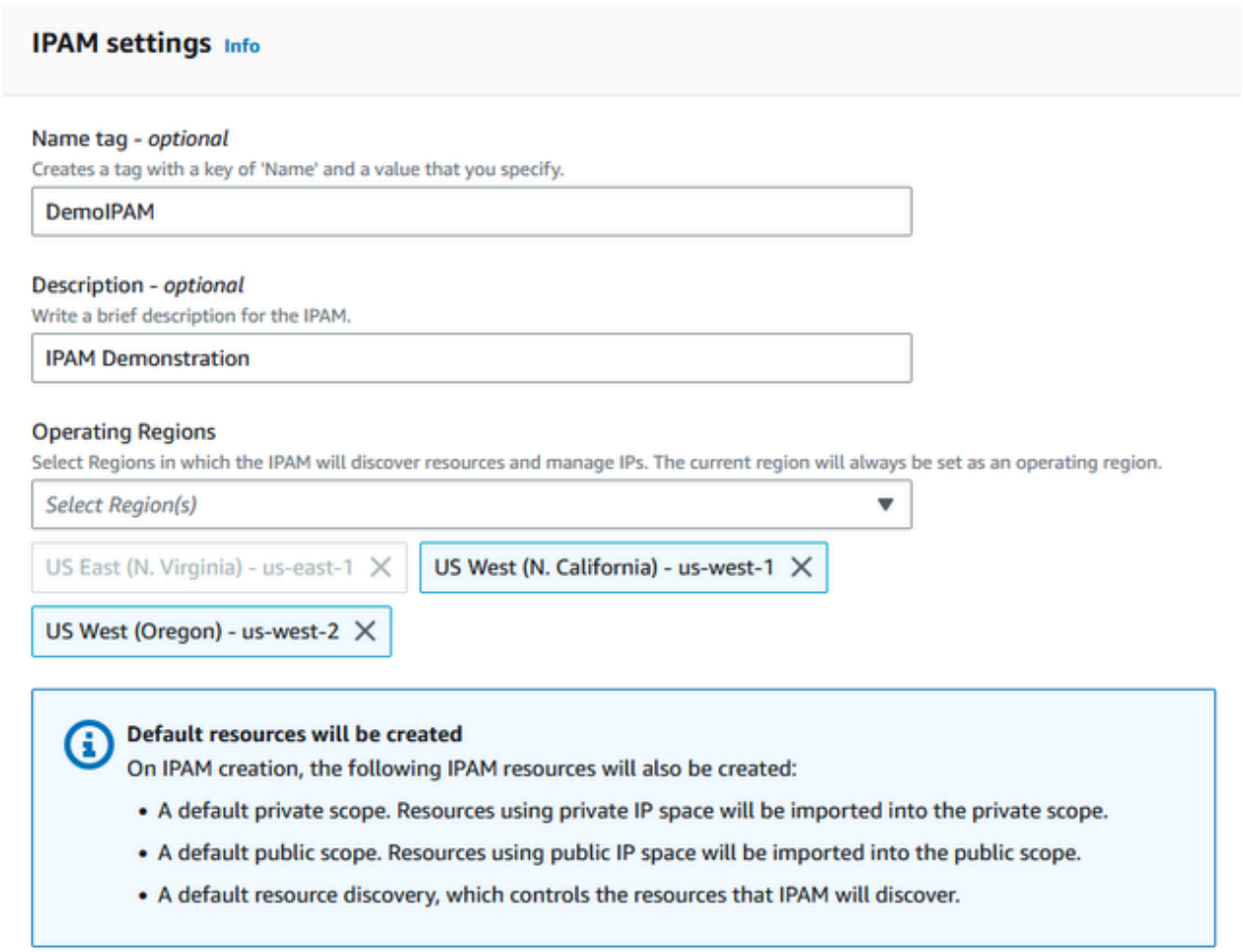
在本步驟中，您將會建立 IPAM。建立 IPAM 時，IPAM 會自動為 IPAM 建立兩個範圍：適用於所有私有空間的私有範圍，以及適用於所有公有空間的公有範圍。範圍以及集區和配置是 IPAM 的主要元件。如需詳細資訊，請參閱IPAM 的運作方式。

建立 IPAM

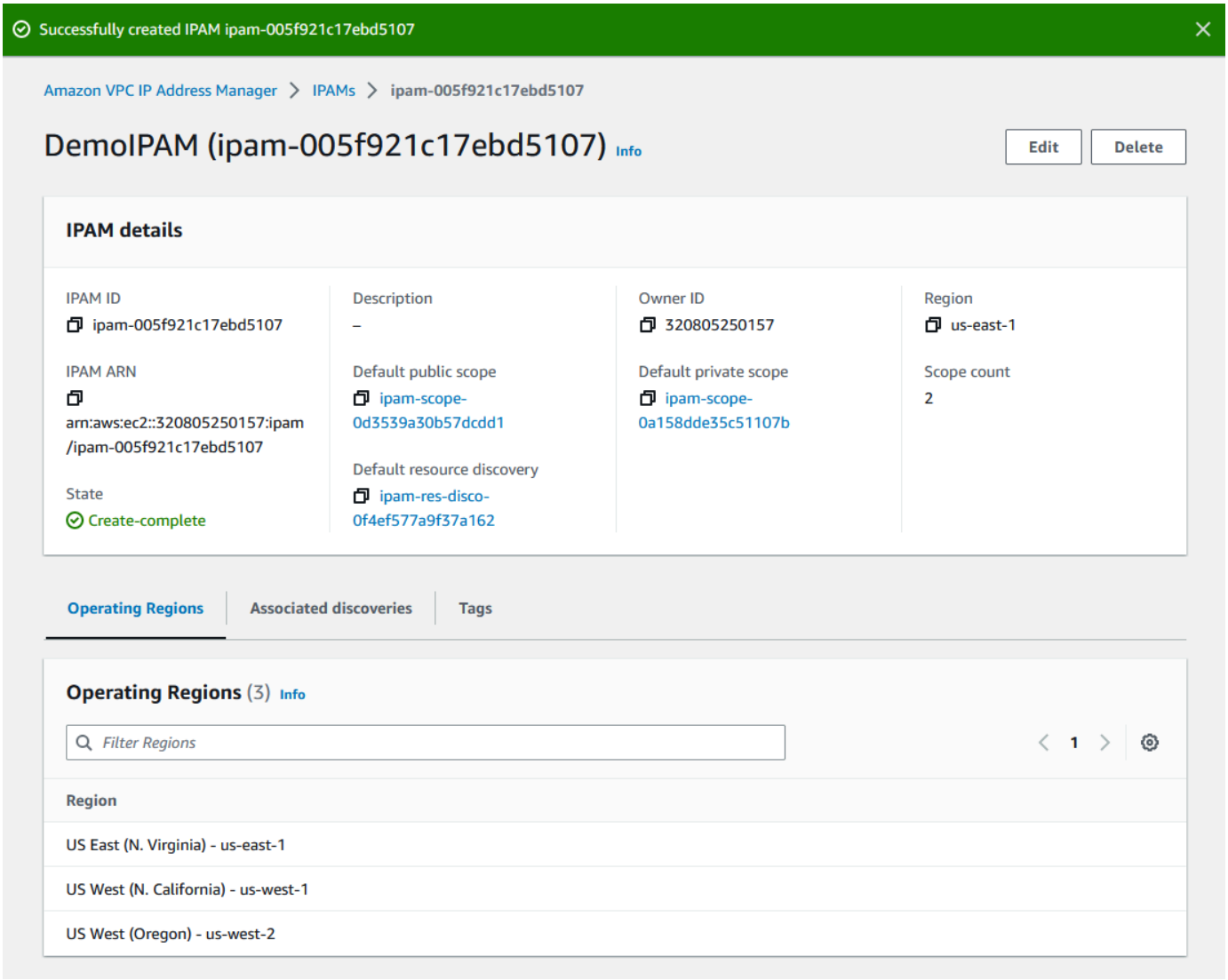
1. 使用上一個步驟中委派為 IPAM 管理員 AWS Organizations 的成員帳戶，在 https：//https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在 AWS 管理主控台中，選擇您要在其中建立 IPAM AWS 的區域。在您的主要作業區域中建立 IPAM。
3. 在服務首頁選擇 Create IPAM (建立 IPAM)。
4. 選擇 Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (允許 Amazon VPC IP 地址管理員將來源帳戶的資料複寫到 IPAM 委託帳戶)。若未選取此選項，即無法建立 IPAM。



5. 在操作區域下，選擇此 IPAM 可以管理和探索資源 AWS 的區域。您建立 IPAM AWS 的區域會自動選取為其中一個操作區域。在本教學課程中，IPAM 的主區域為 us-east-1，因此我們會選擇 us-west-1 和 us-west-2 作為其他作業區域。如果您忘記作業區域，稍後可以編輯 IPAM 設定，並新增或移除區域。



6. 選擇 Create IPAM (建立 IPAM)。



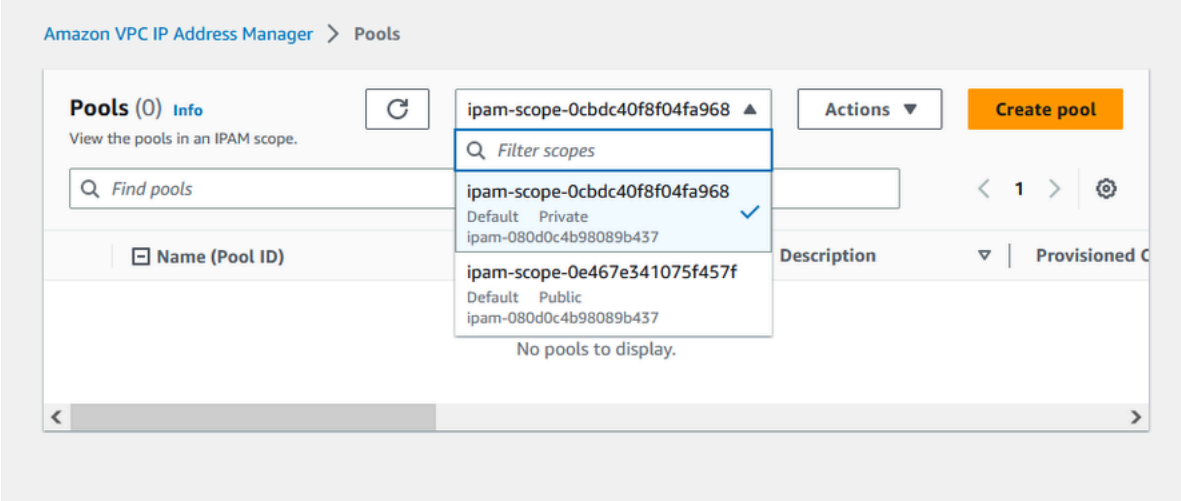
步驟 3：建立最上層 IPAM 集區

在本教學課程中，您將會建立從頂層 IPAM 集區開始的集區階層。在後續步驟中，您將在其中一個區域集區中建立一對區域集區和一個生產前開發集區。

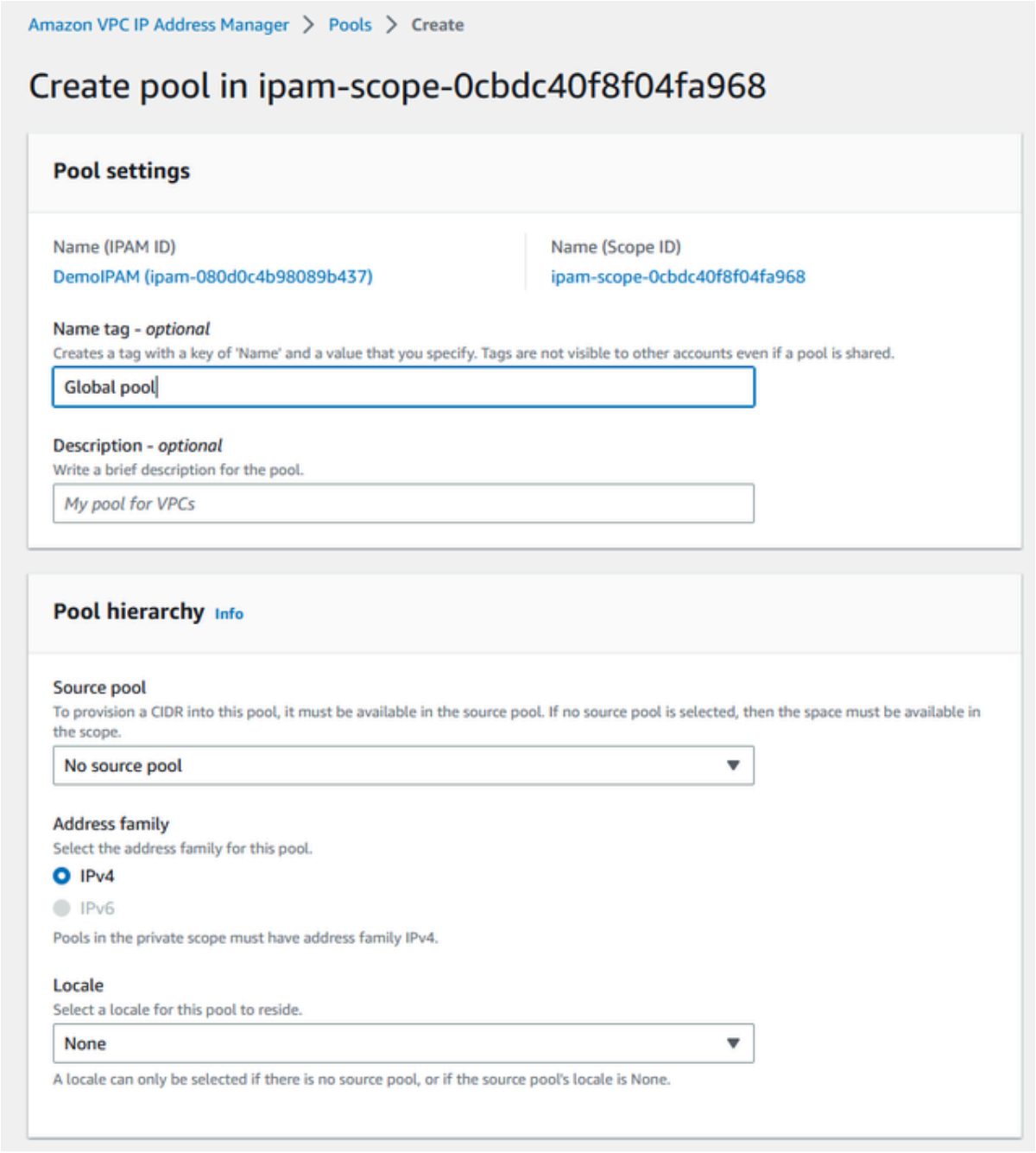
如需有關可使用 IPAM 建置之集區階層的詳細資訊，請參閱 IPAM 集區計畫範例。

建立頂層集區

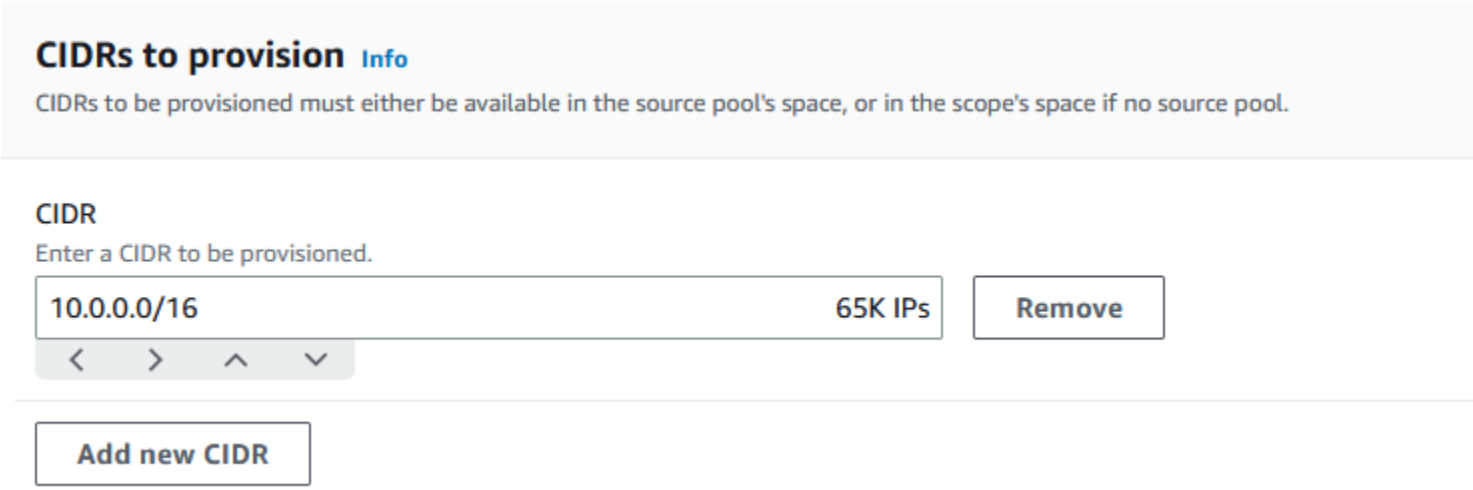
1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍。



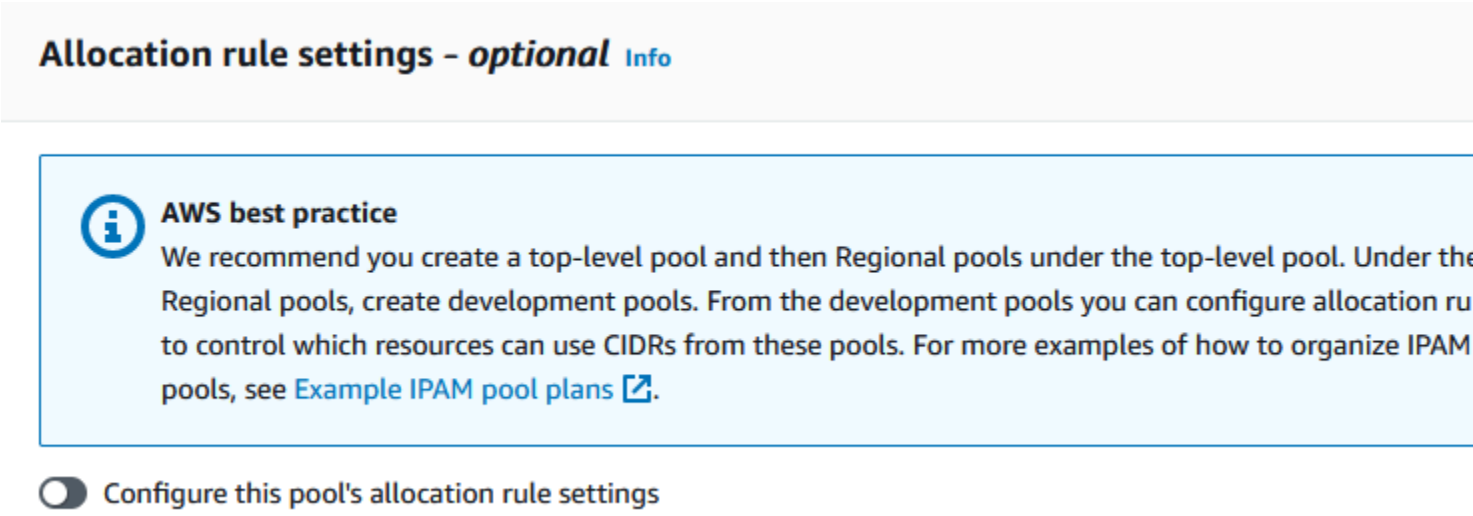
4. 選擇建立集區。
5. 在 IPAM 範圍下，保持選取的私有範圍。
6. (選用) 新增集區的名稱標籤和集區的說明 (例如 “Global pool”)。
7. 在 Source (來源) 下，選擇 IPAM scope (IPAM 範圍)。由於此為頂層集區，因此不具有來源集區。
8. 在 Address family (地址系列) 下，選擇 IPv4。
9. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
10. 針對 Locale (地區設定)，選擇 None (無)。區域是您希望此 IPAM 集區可用於配置 AWS 的區域。您將會針對在本教學課程下一節中建立的區域集區設定地區設定。



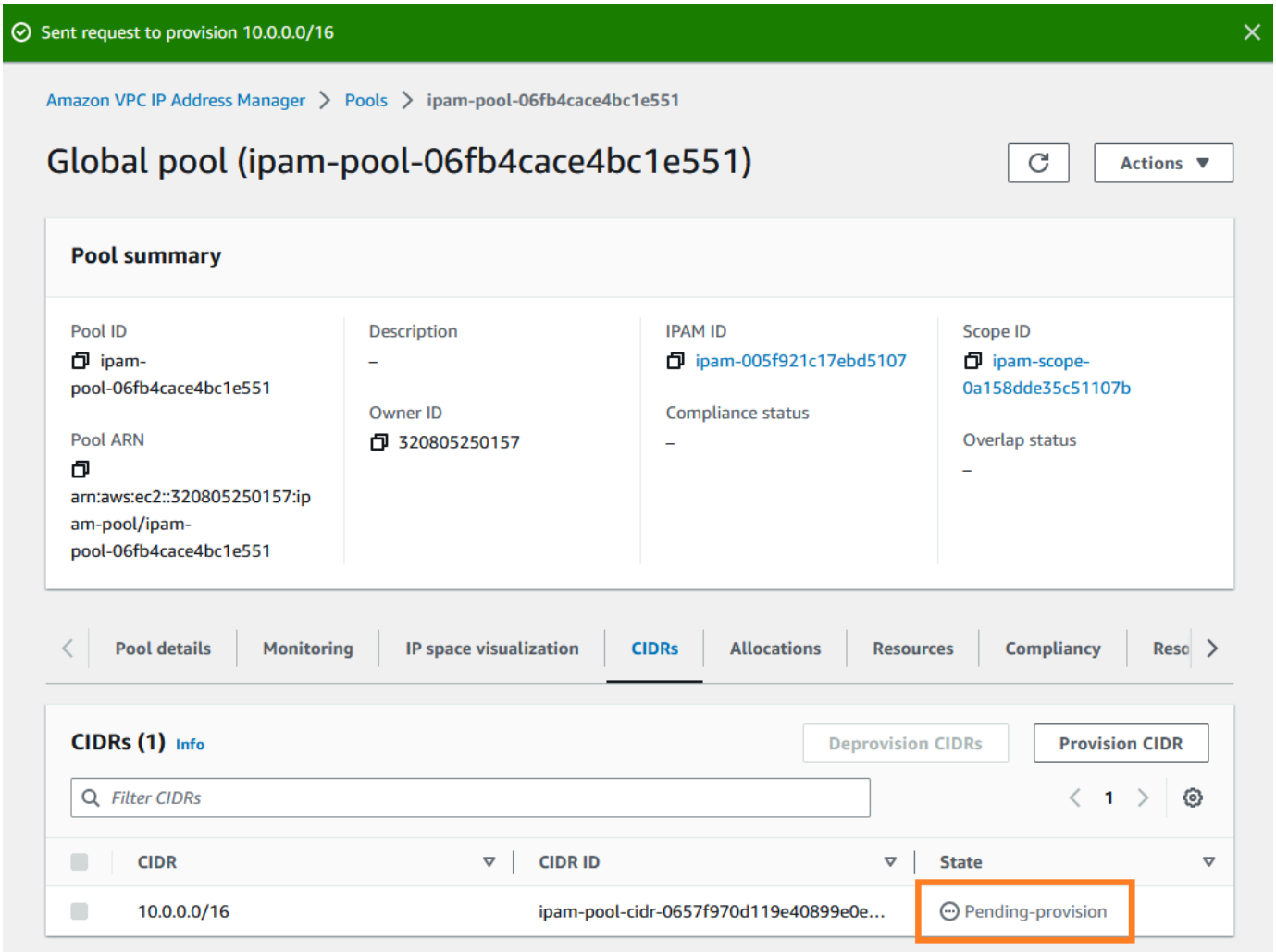
11. 選擇要為集區佈建的 CIDR。在本範例中，我們會佈建 10.0.0.0/16。



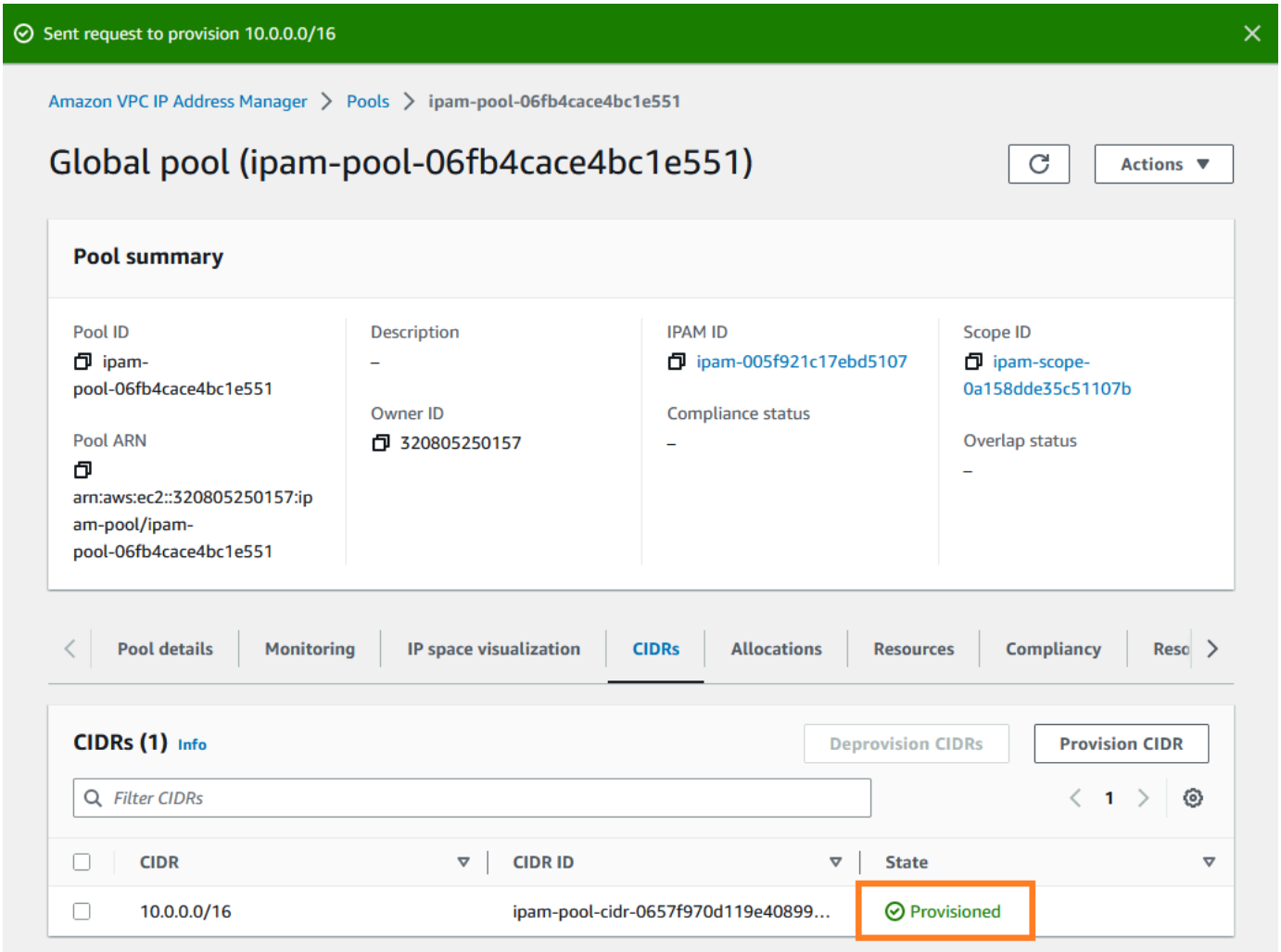
12. 將設定此集區的配置規則設定保持停用。此為頂層集區，您將無法直接從此集區將 CIDR 配置到 VPC。相反地，您可能須從自己在此集區建立的子集區進行配置。



13. 選擇建立集區。集區已建立，且 CIDR 處於待佈建狀態：



14. 等待狀態變為已佈建後，即可前往下一個步驟。



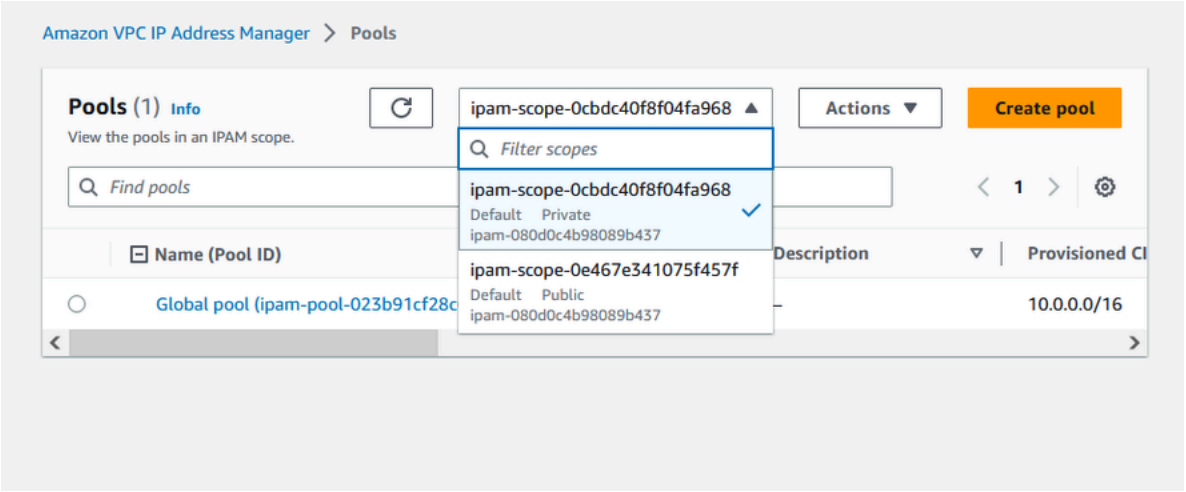
現在您已建立頂層集區，將可在 us-west-1 和 us-west-2 中建立區域集區。

步驟 4：建立區域 IPAM 集區

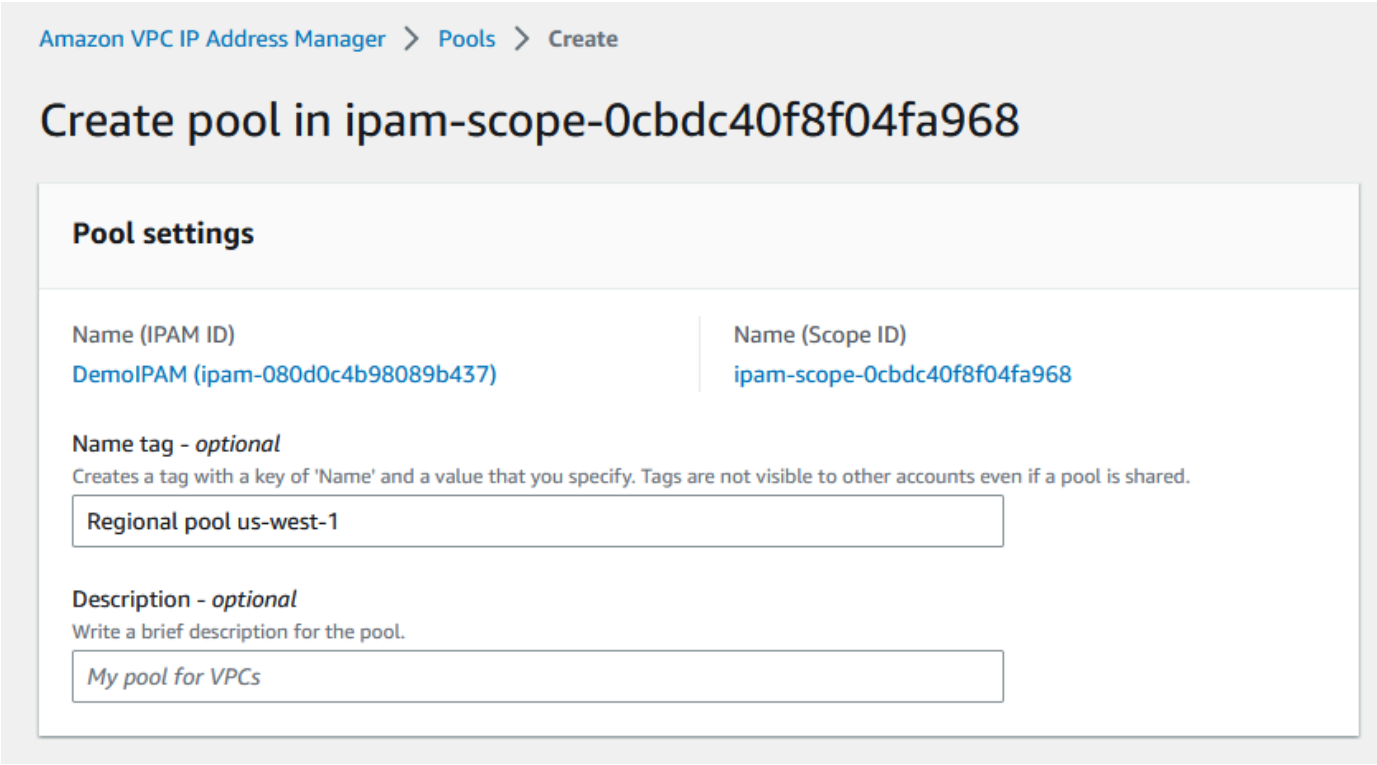
本節將會說明如何使用兩個區域集區來組織 IP 地址。在本教學課程中，我們將按照其中一個 IPAM 集區計劃範例，建立兩個區域集區 (這兩個區域集區可供組織中的成員帳戶使用，以將 CIDR 配置給其 VPC)。

建立區域集區

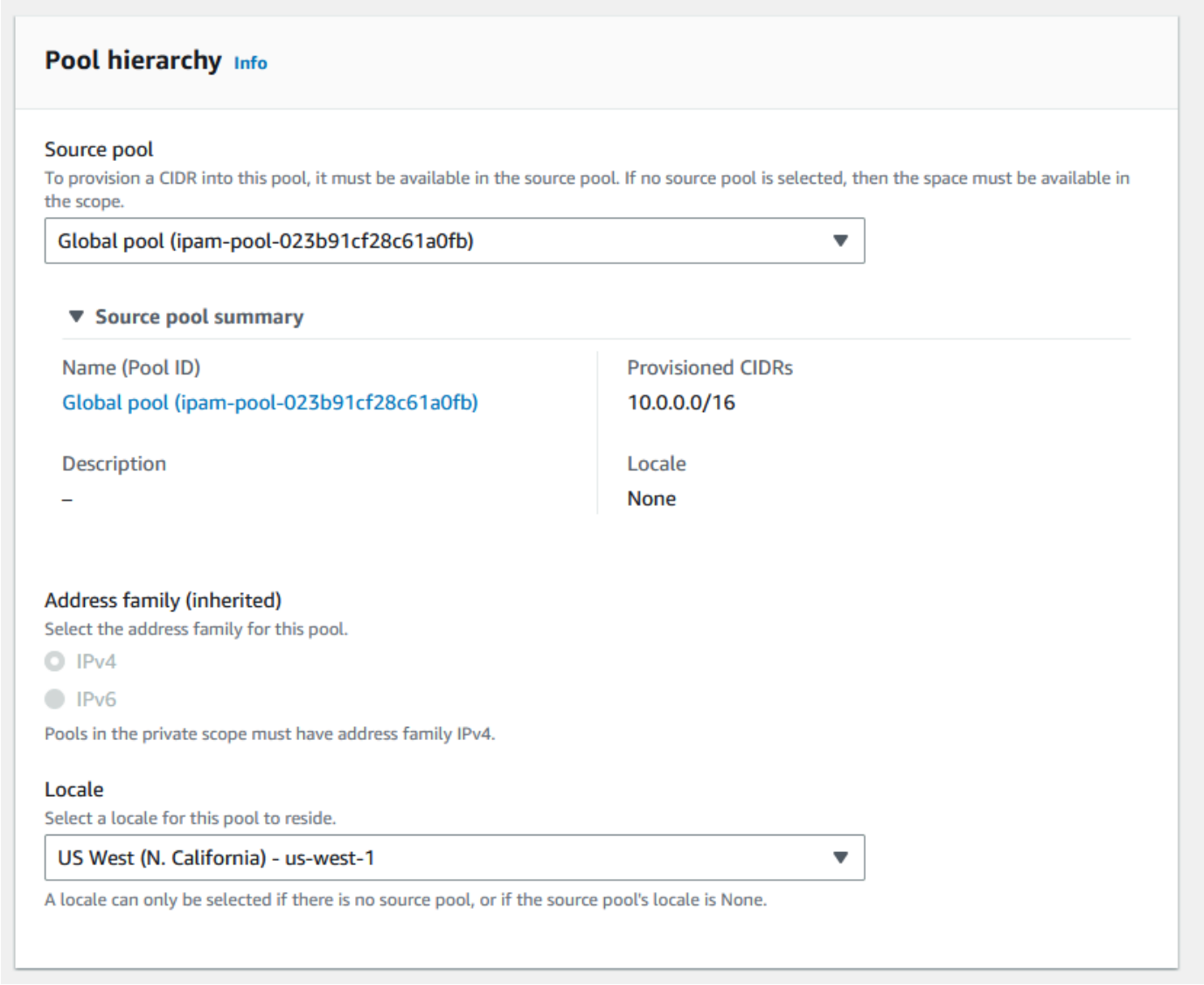
1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍。



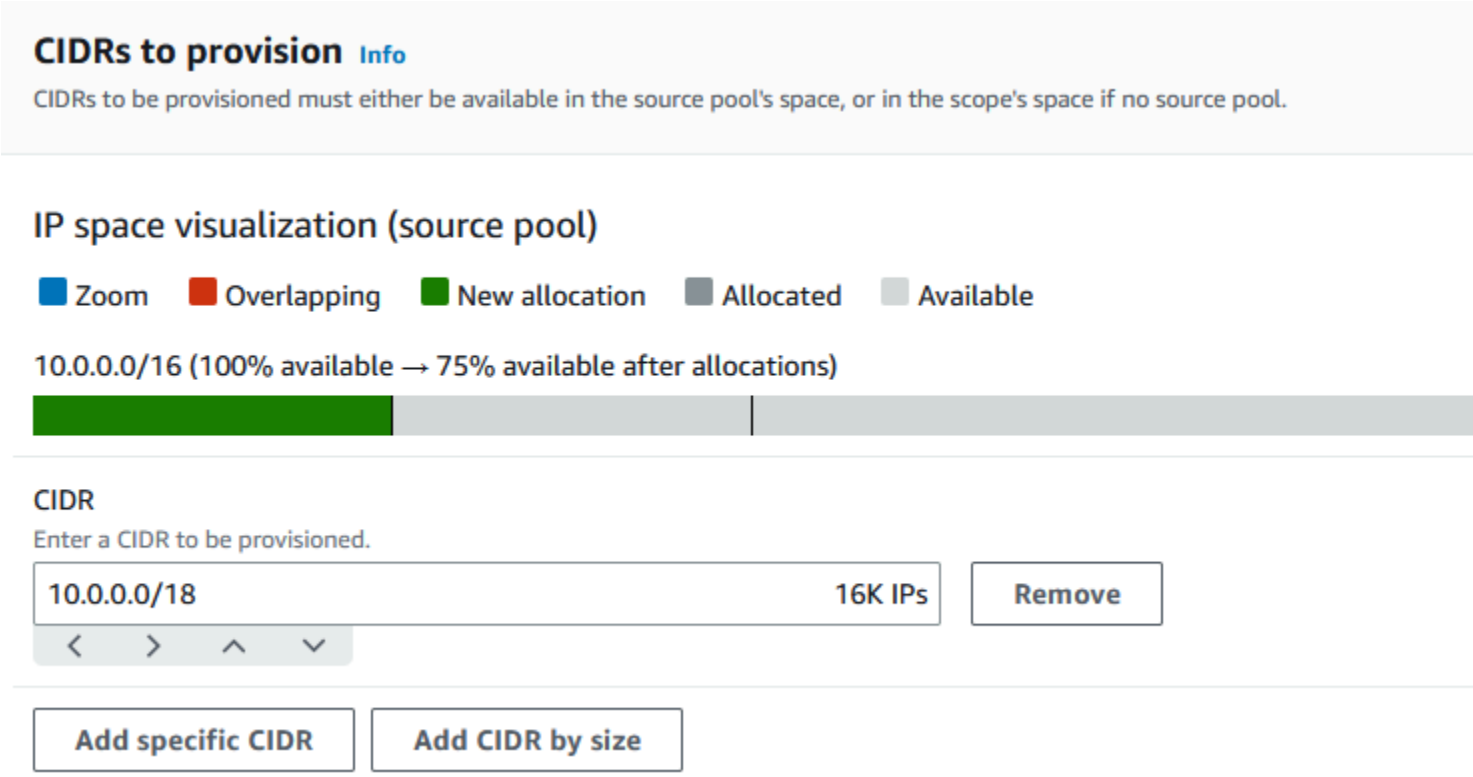
4. 選擇建立集區。
5. 在 IPAM 範圍下，保持選取的私有範圍。
6. (選用) 新增集區的名稱標籤和集區的說明 (例如區域集區 us-west-1)。



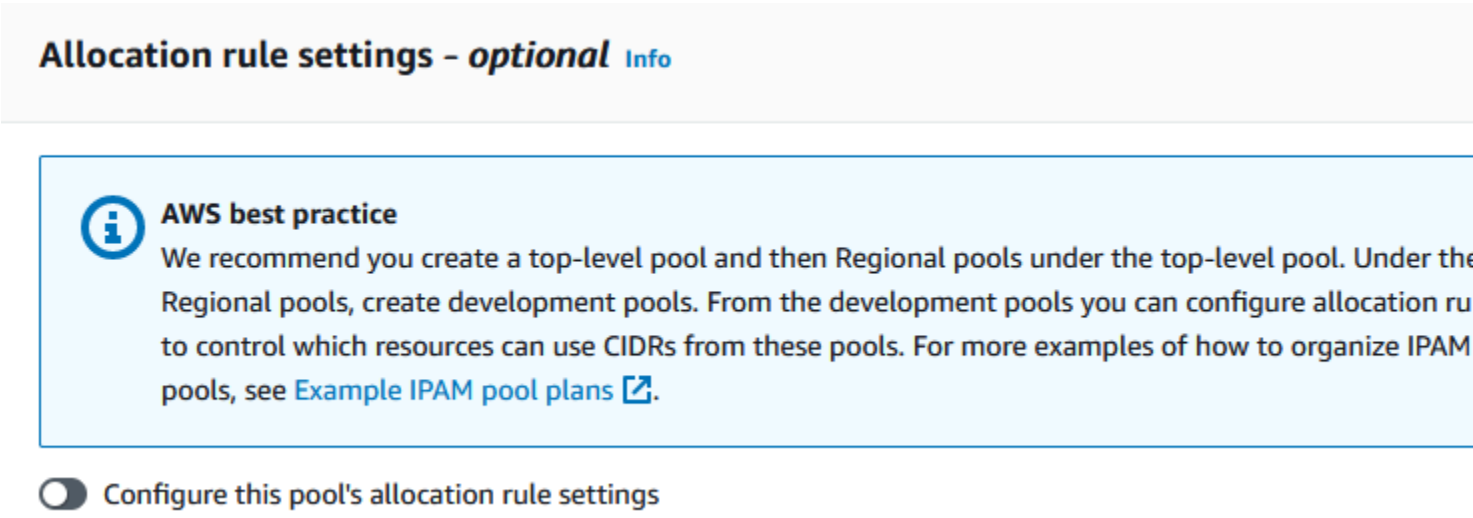
7. 在 Source (來源) 下，選取 IPAM pool (IPAM 集區)，然後選取在 步驟 3：建立最上層 IPAM 集區 中建立的頂層集區 ("Global pool")。接著，在地區設定下，選擇 us-west-1。



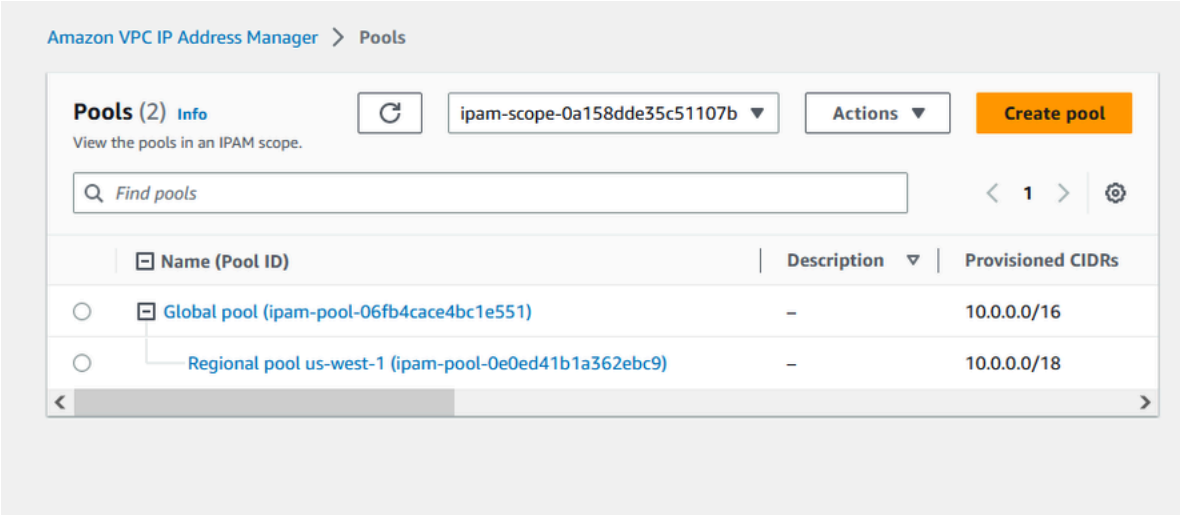
8. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
9. 在要佈建的 CIDR 下，輸入 10.0.0.0/18 (此 CIDR 將可為此集區提供約 16,000 個可用的 IP 地址)。



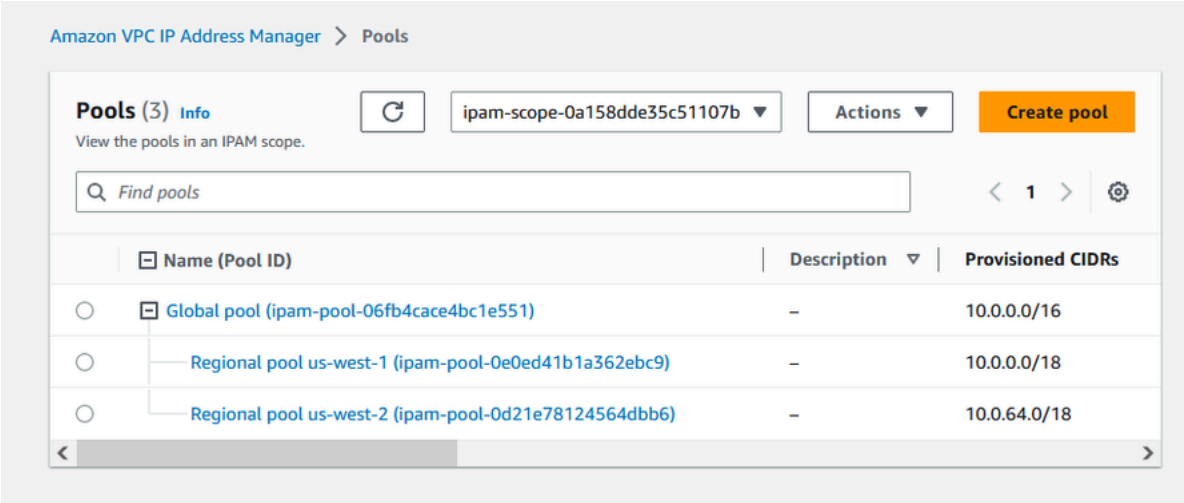
10. 將設定此集區的配置規則設定保持停用。您將無法直接從此集區將 CIDR 配置到 VPC。相反地，您可能須從自己在此集區建立的子集區進行配置。



11. 選擇建立集區。
12. 返回集區檢視，以查看您已建立的 IPAM 集區階層。



13. 重複本節中的步驟，並使用佈建於其中的 CIDR 10.0.64.0/18，在 us-west-2 地區設定中建立第二個區域集區。完成該程序後，您將會在以下類似的階層中擁有三個集區：

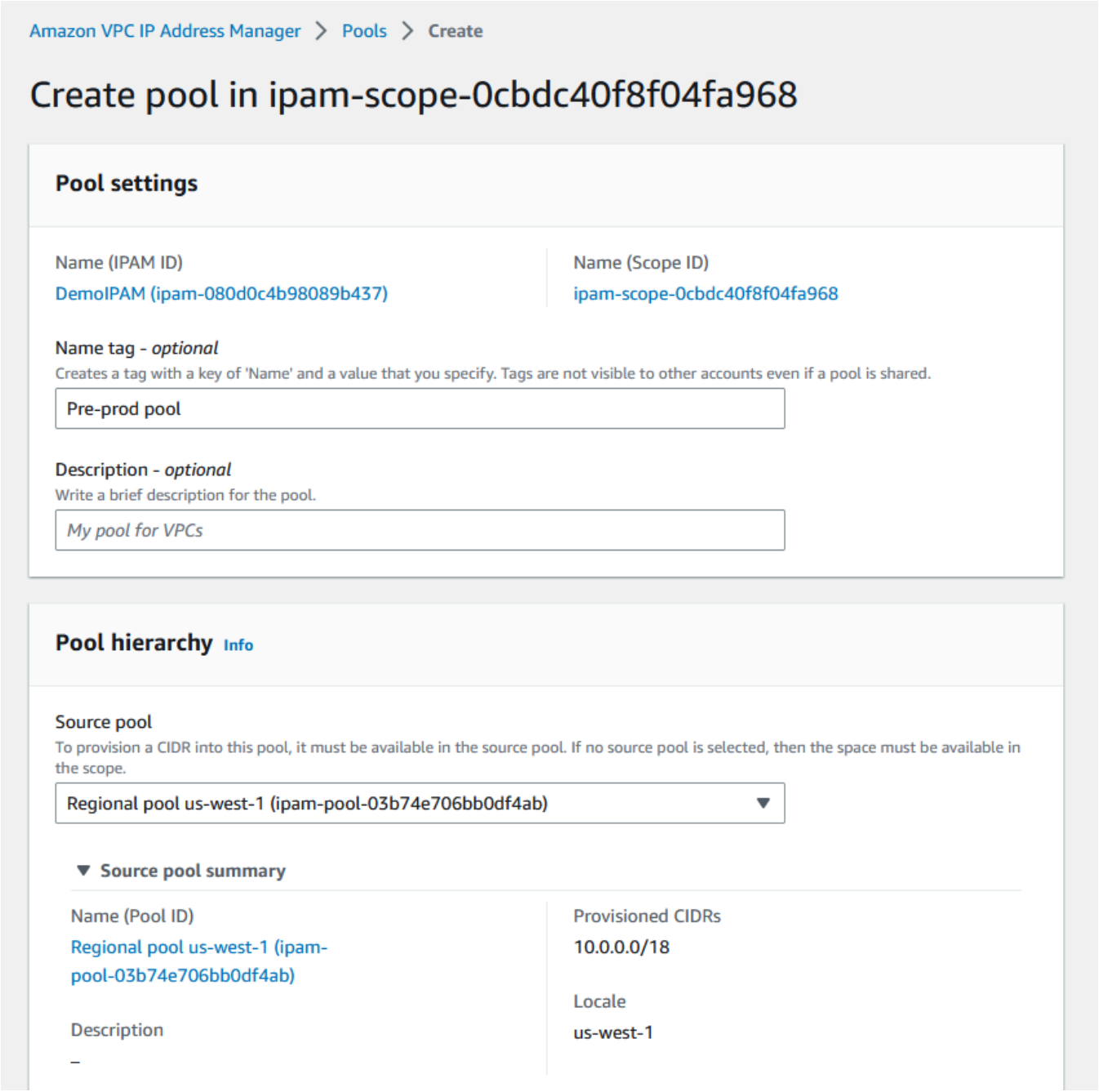


步驟 5：建立生產前開發集區

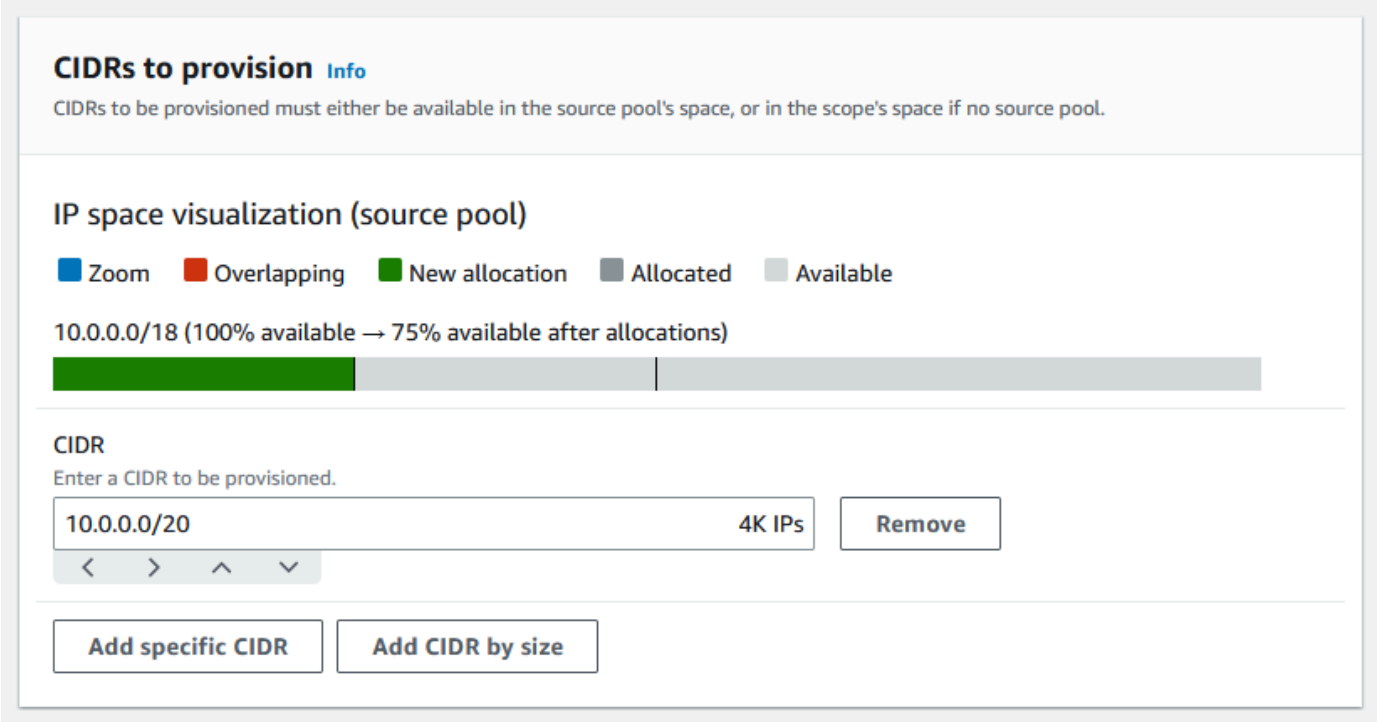
請按照本節中的步驟，在其中一個區域集區內，建立生產前資源的開發集區。

建立生產前開發集區

1. 如同上一節中所進行的方式，使用 IPAM 管理員帳戶，建立名為 Pre-prod pool 的集區，但此次請使用 Regional pool us-west-1 作為來源集區。

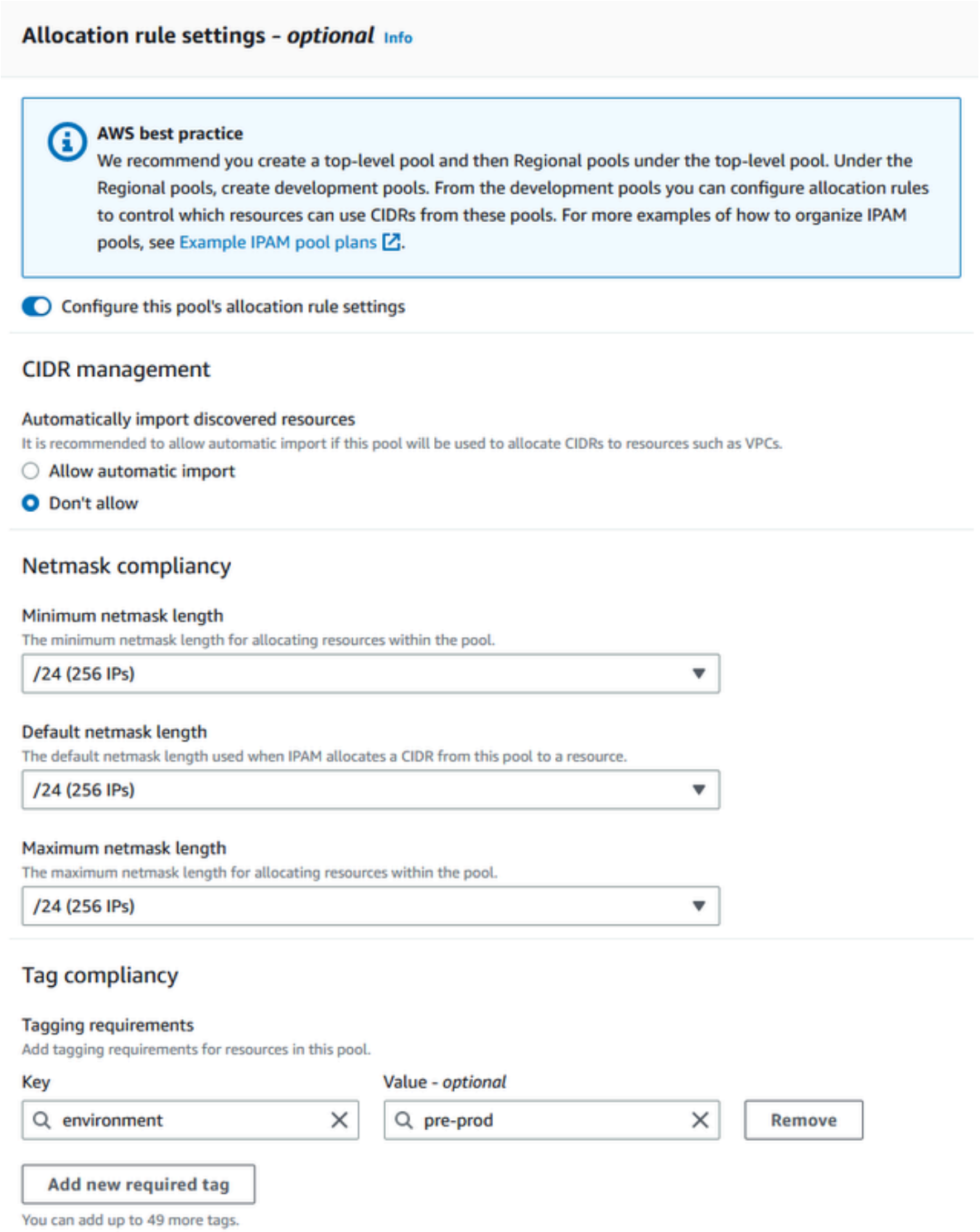


2. 指定要佈建的 10.0.0.0/20 CIDR (此 CIDR 將可為此集區提供約 4,000 個 IP 地址)。

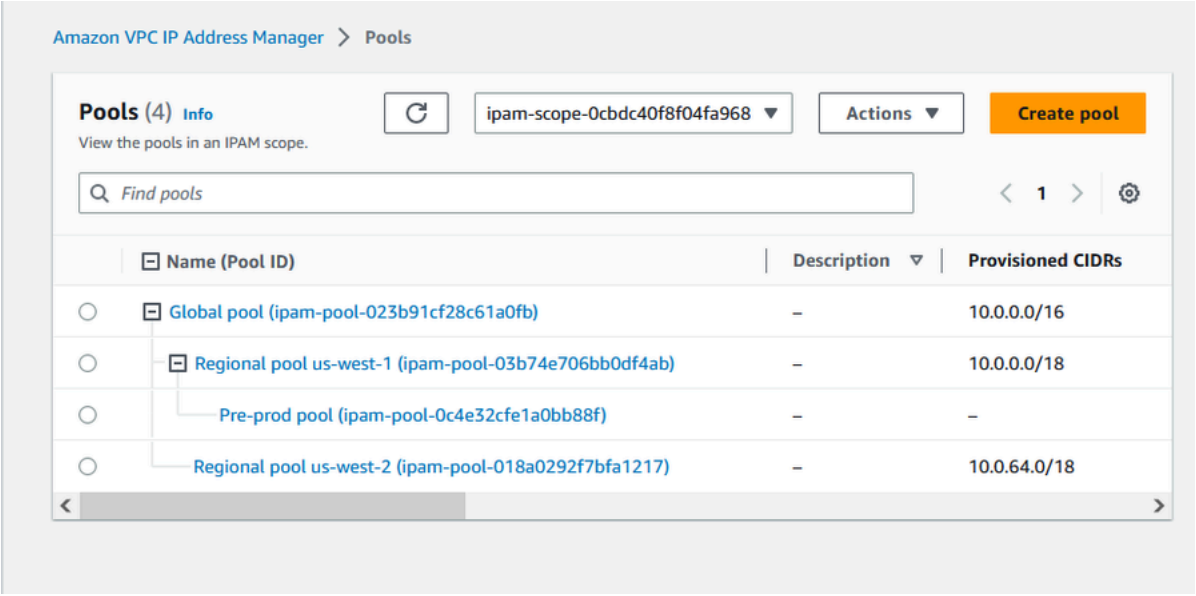


3. 切換設定此集區的配置規則設定選項。請執行下列操作：

   1. 在 CIDR 管理下的自動匯入探索到的資源，保持選取預設的不允許選項。此選項可讓 IPAM 自動匯入在集區地區設定中探索到的資源 CIDR。此選項的詳細說明未涵蓋在本教學課程的範圍內，但您可以在 建立頂層 IPv4 集區 中詳閱有關該選項的資訊。
   2. 在網路遮罩合規性下，選擇 /24 作為最小、預設和最大網路遮罩長度。此選項的詳細說明未涵蓋在本教學課程的範圍內，但您可以在 建立頂層 IPv4 集區 中詳閱有關該選項的資訊。需要注意的是，您稍後使用此集區中之 CIDR 建立的 VPC，將根據我們在此處設定限制為 /24。
   3. 在標籤合規下，輸入 environment/pre-prod。VPC 需要此標籤來配置集區的空間。我們將在稍後示範其運作方式。



4. 選擇建立集區。
5. 集區階層現在包含 Regional pool us-west-1 下的其他子集區：



現在，您可以開始與組織中的其他成員帳戶共用 IPAM 集區，並啟用該帳戶以從集區配置 CIDR 來建立 VPC。

步驟 6：共用 IPAM 集區

遵循本節中的步驟，使用 AWS Resource Access Manager (RAM) 共用生產前 IPAM 集區。

本節由兩個小節組成：

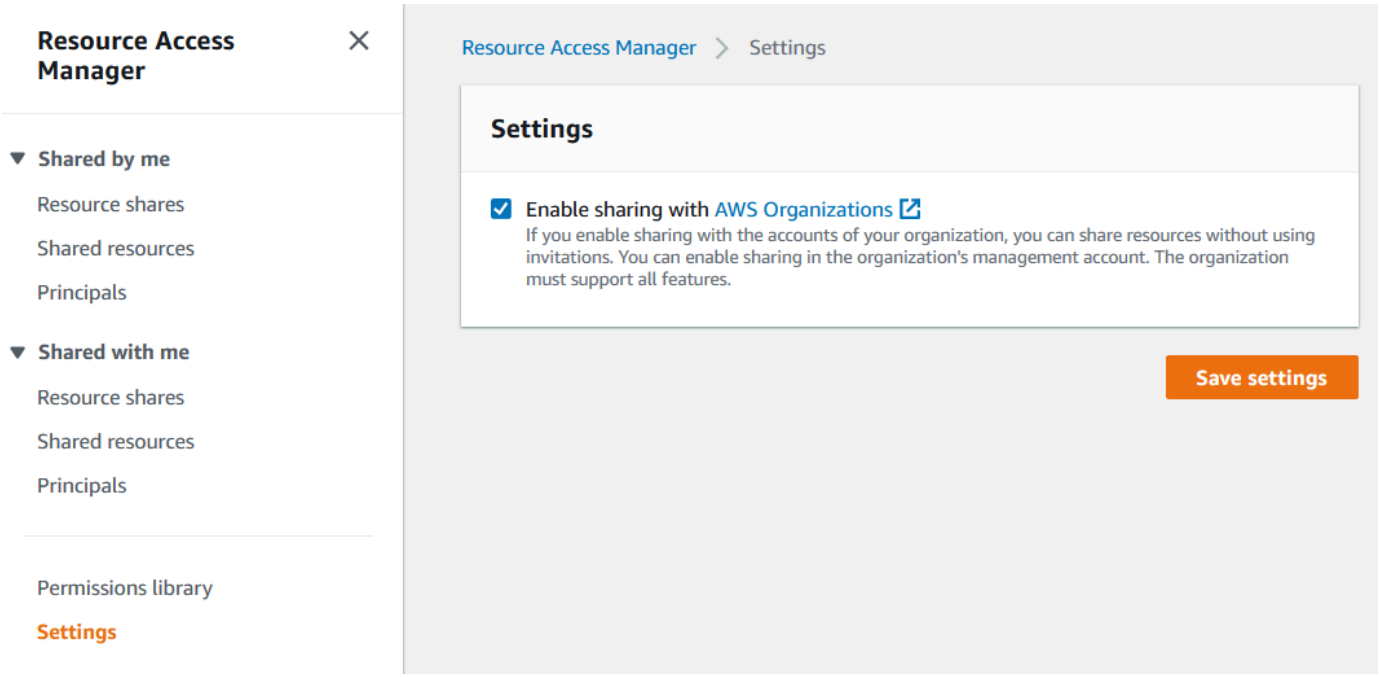
- 步驟 6.1. 在 中啟用資源共用 AWS RAM：此步驟必須由 AWS Organizations 帳戶完成。
- 步驟 6.2. 使用 共用 IPAM 集區 AWS RAM：此步驟必須由 IPAM 管理員完成。

步驟 6.1. 在 中啟用資源共用 AWS RAM

建立 IPAM 之後，您會想要與組織中的其他帳戶共用 IP 地址集區。在您共用 IPAM 集區之前，請完成本節中的步驟，以啟用與 共用資源 AWS RAM。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，在 https：//https://console.aws.amazon.com/ram/ 開啟 AWS RAM 主控台。
2. 在左側導覽窗格中，選擇設定，選擇啟用共用 AWS Organizations，然後選擇儲存設定。



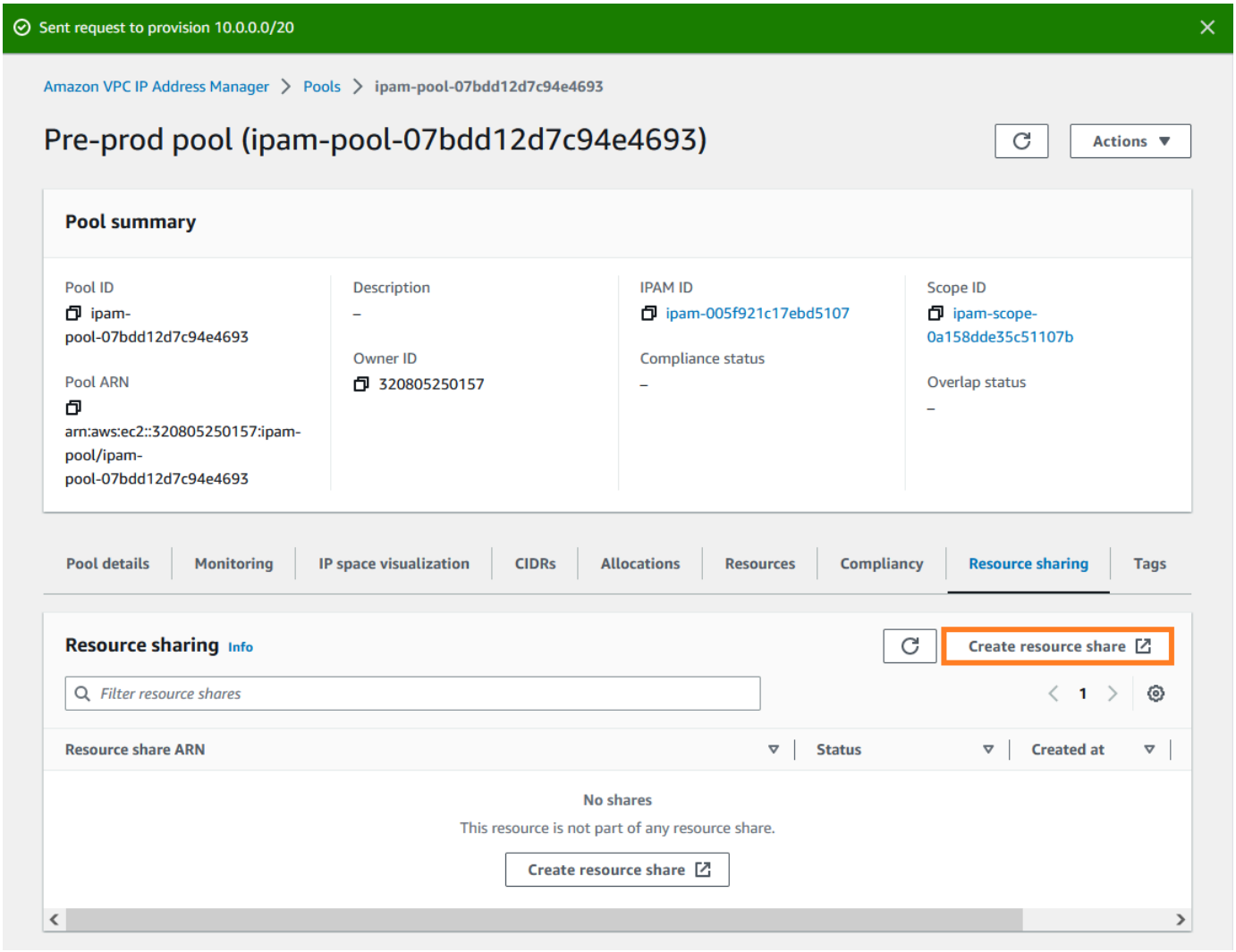
您現在可以與組織的其他成員共用 IPAM 集區。

步驟 6.2. 使用 共用 IPAM 集區 AWS RAM

在本節中，您將與其他 AWS Organizations 成員帳戶共用生產前開發集區。如需共用 IPAM 集區的完整說明 (包括所需 IAM 許可的相關資訊)，請參閱 透過 AWS RAM 共用 IPAM 集區。

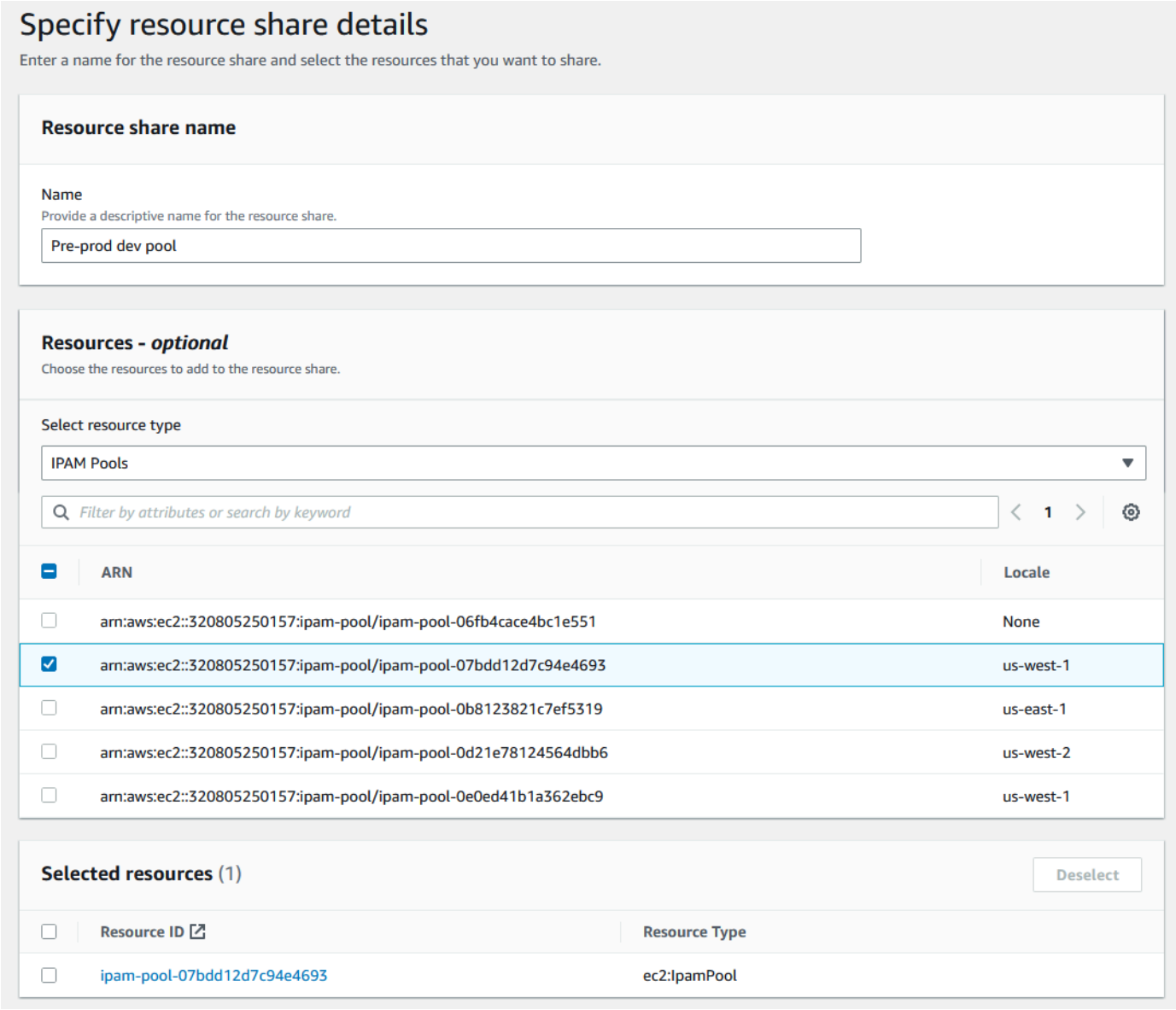
使用 共用 IPAM 集區 AWS RAM

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍，選擇生產前 IPAM 集區，然後選擇動作 > 檢視詳細資料。
4. 在 Resource sharing (資源共用) 底下，選擇 Create resource share (建立資源共用)。 AWS RAM 主控台隨即開啟。您將使用 共用集區 AWS RAM。
5. 選擇 Create a resource share (建立資源共用)。

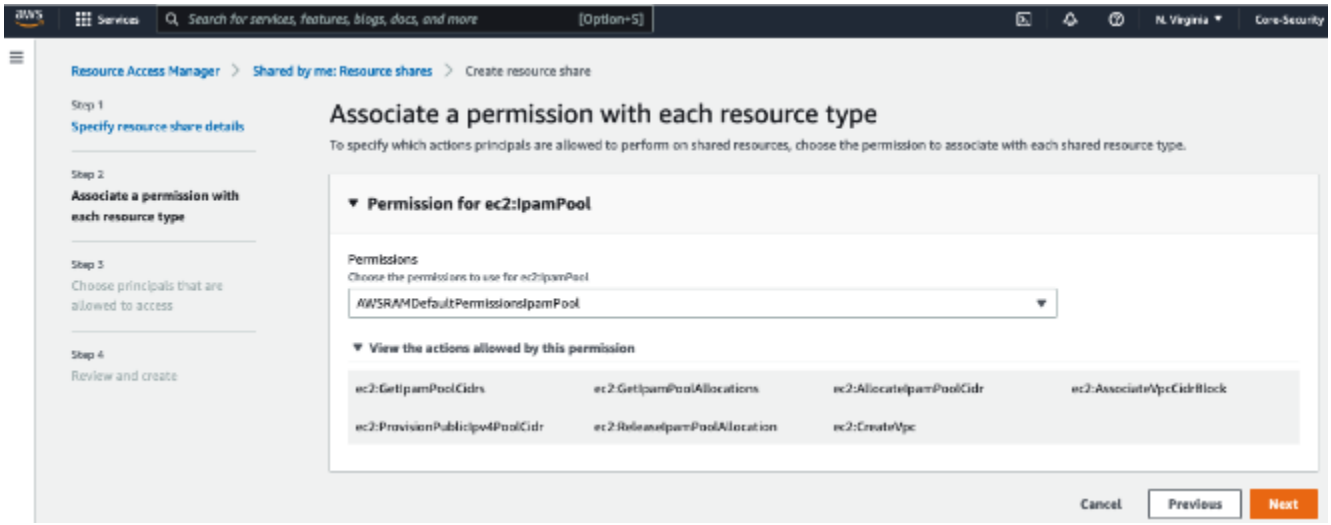


AWS RAM 主控台隨即開啟。

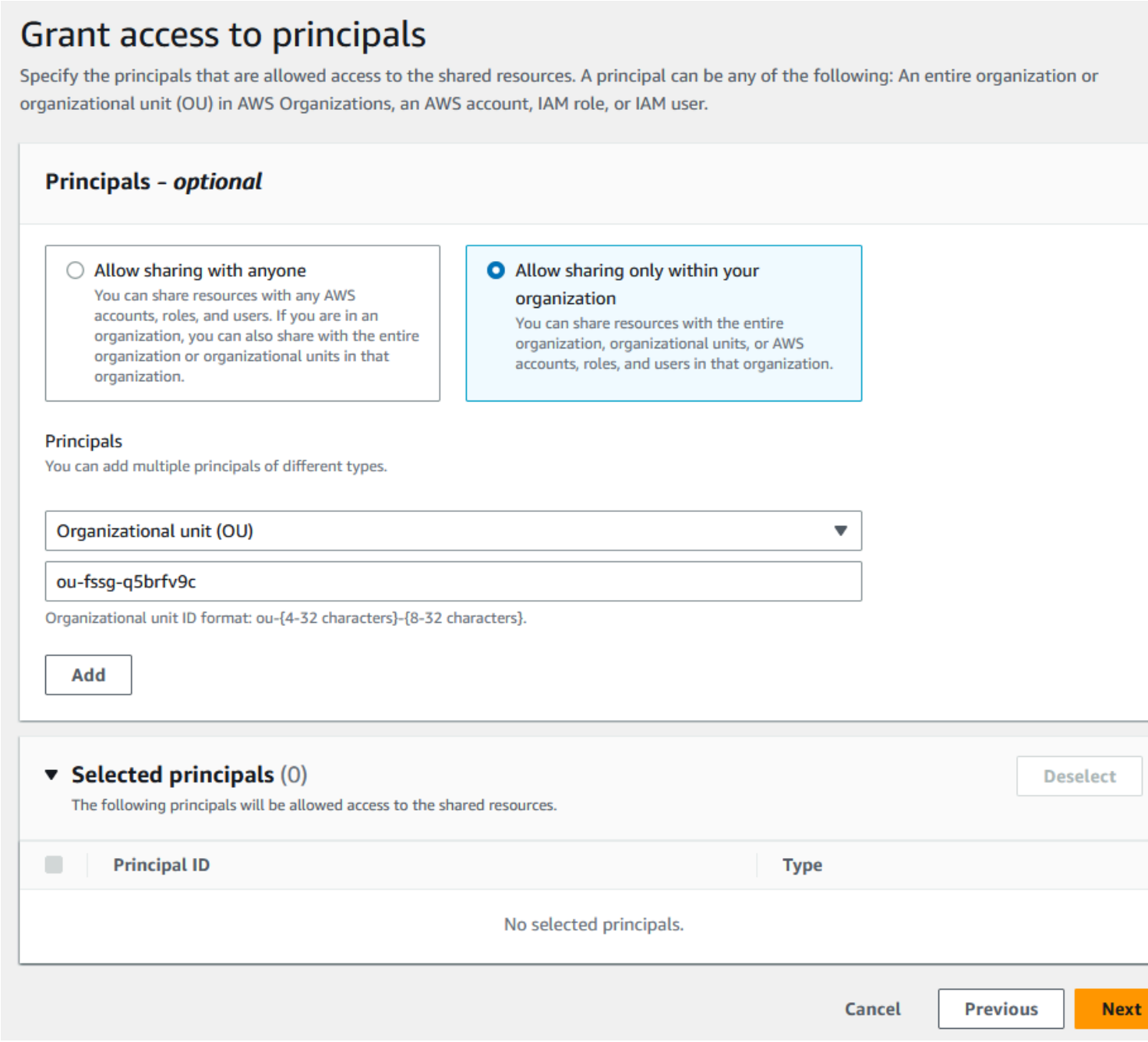
6. 在 AWS RAM 主控台中，再次選擇建立資源共享。
7. 新增共用集區的名稱。
8. 在選取資源類型下，選擇 IPAM 集區，然後選擇生產前開發集區的 ARN。



9. 選擇下一步。
10. 保持選取預設的 AWSRAMDefaultPermissionsIpamPool 許可。許可選項的詳細資料未涵蓋在本教學課程的範圍，但您可以在 透過 AWS RAM 共用 IPAM 集區 中了解有關這些選項的詳細資訊。



11. 選擇下一步。
12. 在主體下，選擇僅允許在組織內共用。輸入您的 AWS Organizations 組織單位 ID （如 中所述如何與 IPAM AWS Organizations 整合，然後選擇新增 。



13. 選擇下一步。
14. 檢閱資源共用選項，以及您要與其共用的主體，然後選擇建立。

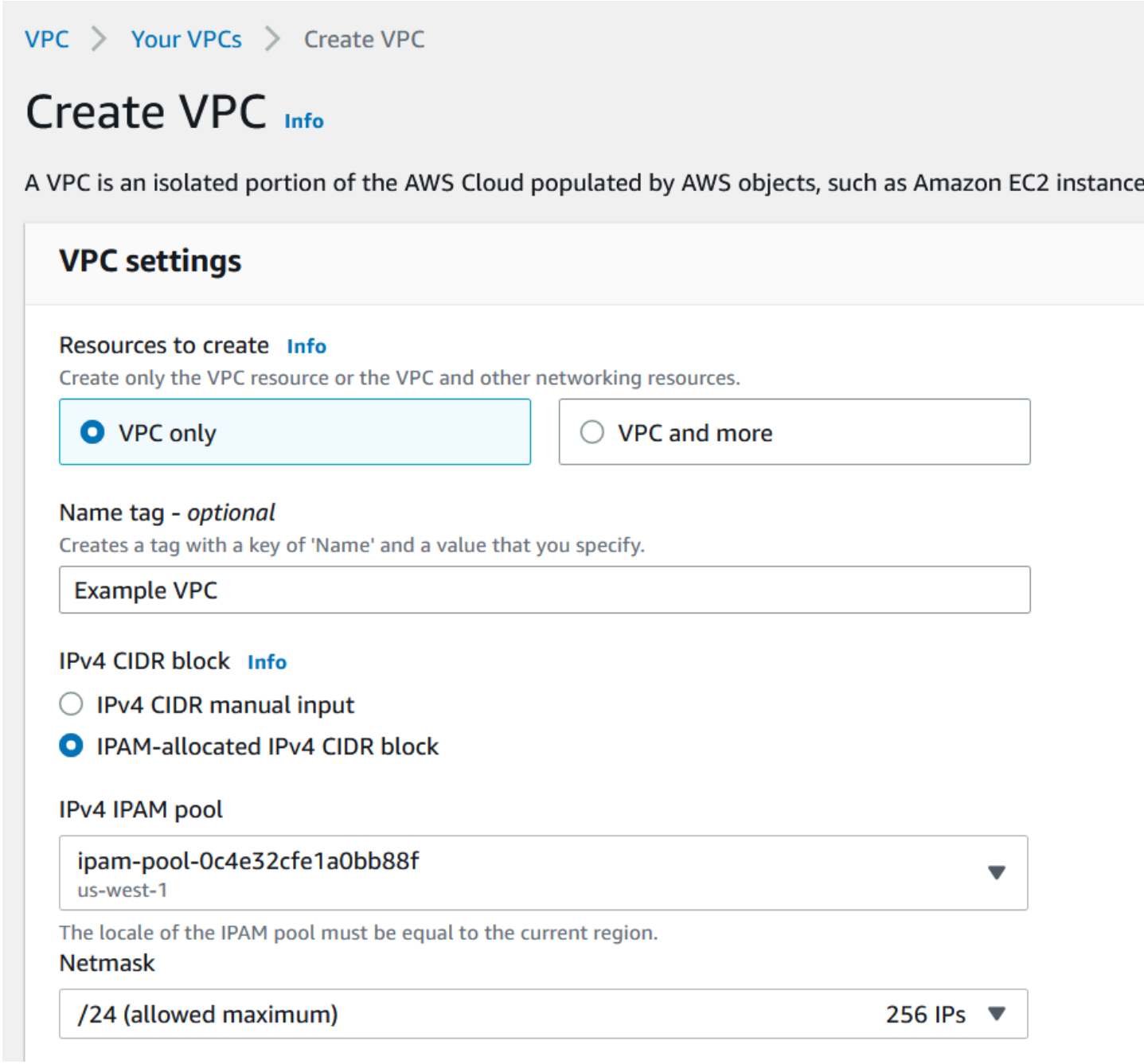
既然已共用集區，請前往下一個步驟，以建立 VPC (其中包含從 IPAM 集區配置的 CIDR)。

步驟 7：使用從 IPAM 集區配置的 CIDR 建立 VPC

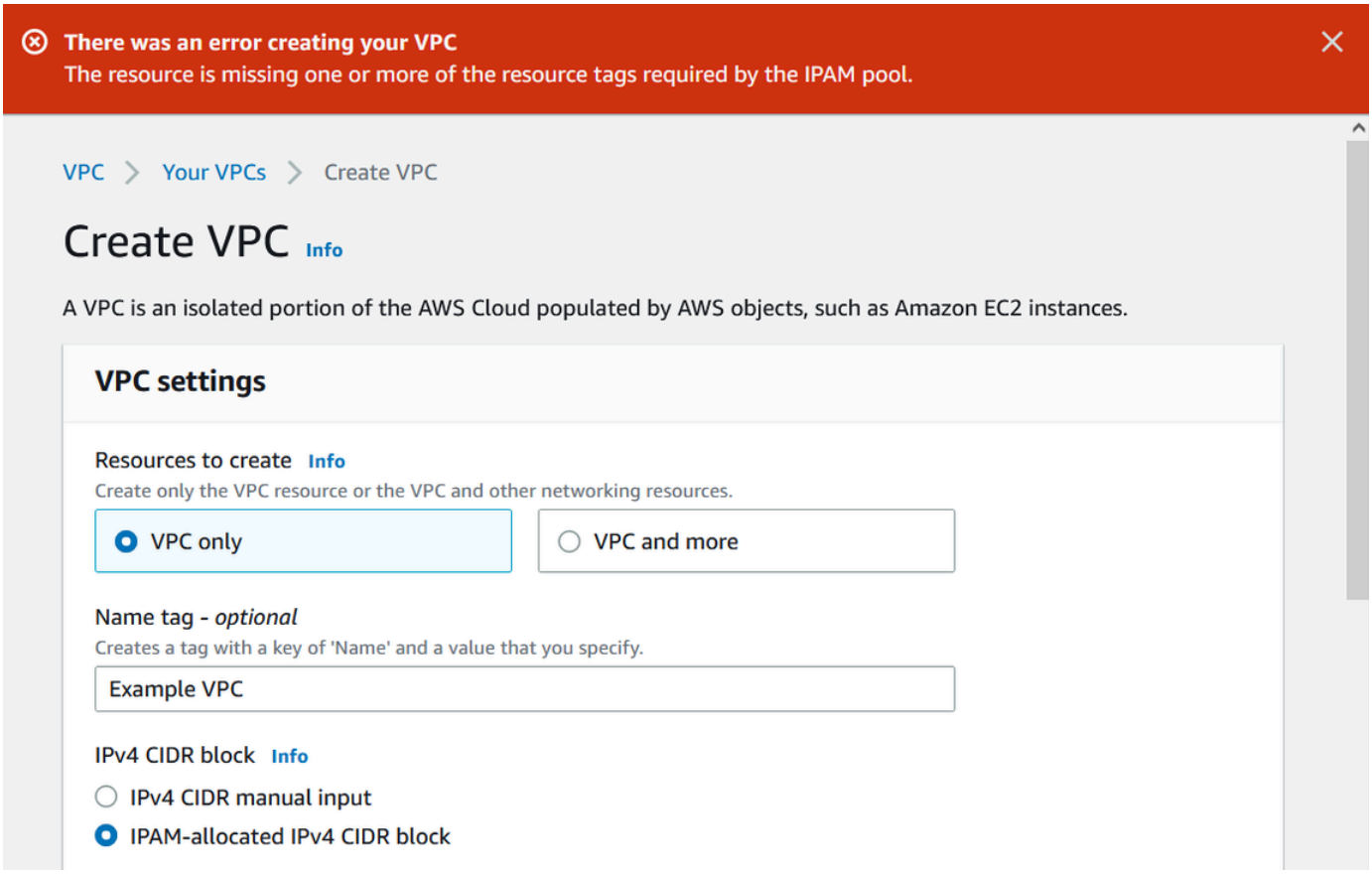
請按照本節中的步驟，透過從生產前集區配置 CIDR 來建立 VPC。此步驟應由上一節中與 IPAM 集區共用之 OU 中的成員帳戶完成 (在 如何與 IPAM AWS Organizations 整合 中稱為 example-member-account-2)。如需建立 VPC 所需的 IAM 許可的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 政策範例。

使用從 IPAM 集區配置的 CIDR 建立 VPC

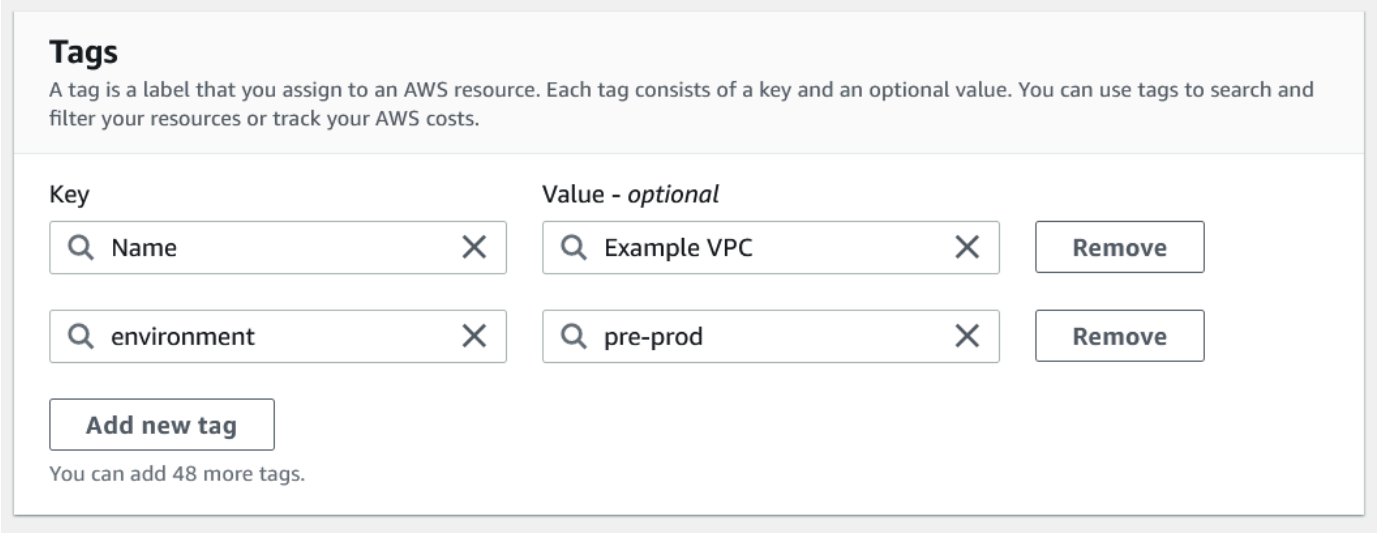
1. 使用成員帳戶，在 https://console.aws.amazon.com/vpc/ 開啟 VPC 主控台，作為您將用作開發人員帳戶的成員帳戶。
2. 選擇建立 VPC。
3. 請執行下列操作：
    1. 輸入名稱 (例如 Example VPC)。
    2. 選擇 IPAM 配置的 IPv4 CIDR 區塊。
    3. 在 IPv4 IPAM 集區下，選擇生產前集區的 ID。
    4. 選擇網路遮罩長度。由於您將此集區的可用網路遮罩長度限制為 /24 (在 步驟 5：建立生產前開發集區 中)，因此唯一可用的網路遮罩選項是 /24。



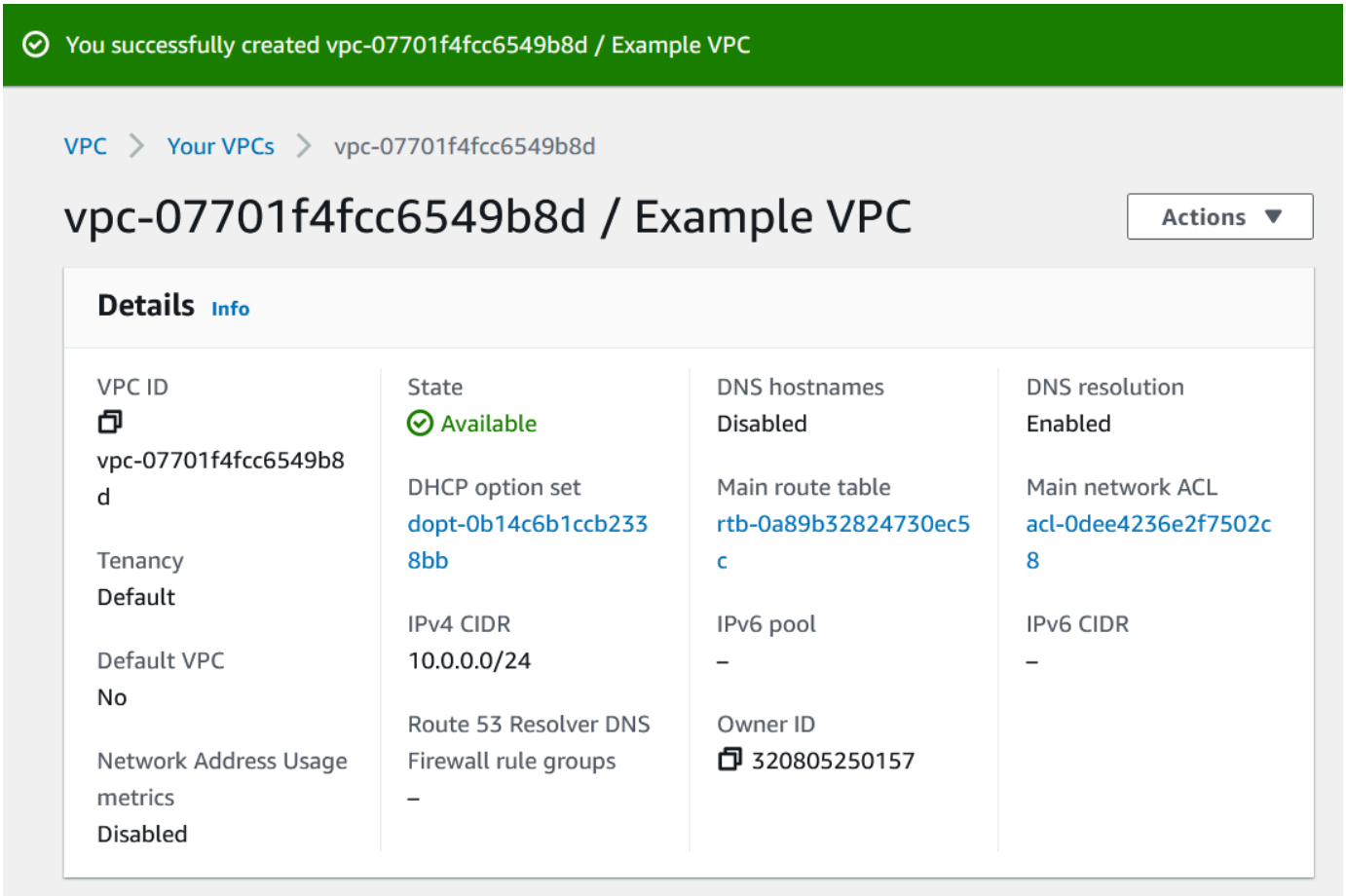
4. 作為示範用途，目前請勿在標籤下，新增任何其他標籤。建立生產前集區時 (在 步驟 5：建立生產前開發集區 中)，您會新增配置規則，以要求使用此集區之 CIDR 建立的任何 VPC 具有 environment/pre-prod 標籤。暫時關閉 environment/pre-prod 標籤，即可看到錯誤訊息出現，告訴您尚未新增必要的標籤。
5. 選擇建立 VPC。
6. 系統會顯示錯誤訊息，告訴您尚未新增必要的標籤。由於您在建立生產前集區 (在 步驟 5：建立生產前開發集區中) 時已設定配置規則，因此系統出現錯誤。配置規則會要求使用此集區之 CIDR 建立的任何 VPC 具有 environment/pre-prod 標籤。



7. 現在，在標籤下，新增 environment/pre-prod 標籤，然後再次選擇建立 VPC。



8. VPC 已成功建立，且 VPC 符合生產前集區上的標籤規則：



在 IPAM 主控台的資源窗格中，IPAM 管理員將能夠查看和管理 VPC 與其配置的 CIDR。請注意，VPC 需要一些時間才會顯示在資源窗格中。

步驟 8：清除

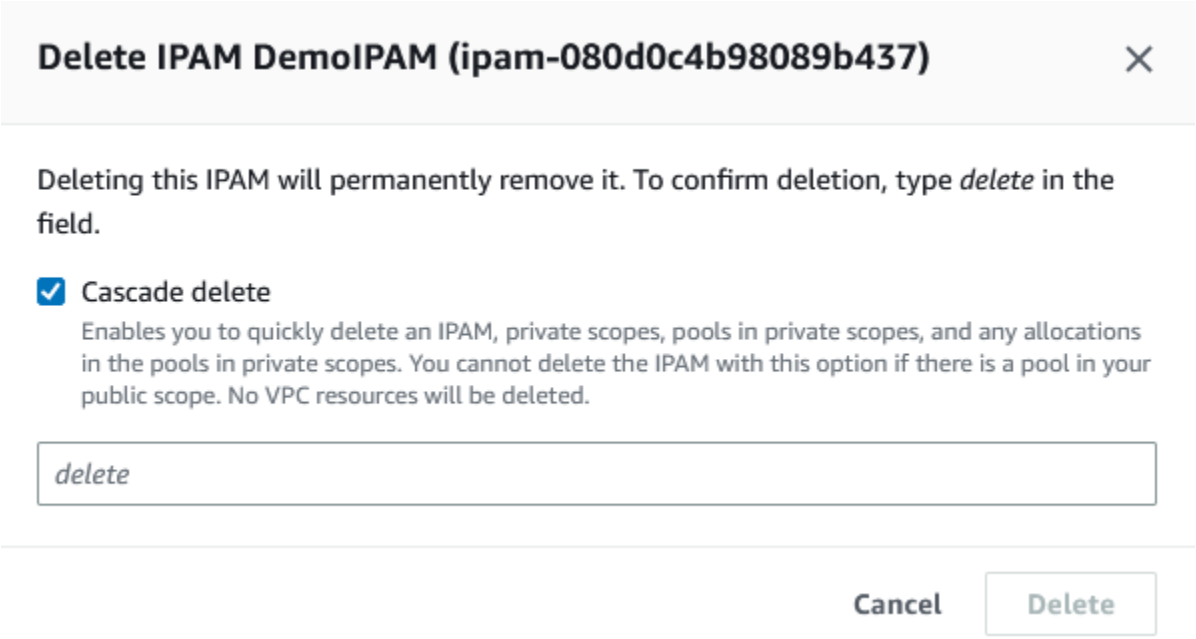
在本教學課程中，您使用委派的管理員建立 IPAM、建立多個集區，並啟用組織中的成員帳戶，以從集區配置 VPC CIDR。

請按照本節中的步驟，清除您在本教學課程中建立的資源。

清除在本教學課程中建立的資源

1. 使用建立範例 VPC 的成員帳戶刪除 VPC。如需詳細指示，請參閱《Amazon Virtual Private Cloud 使用者指南》中的刪除 VPC。
2. 使用 IPAM 管理員帳戶，刪除 AWS RAM 主控台中的範例資源共用。如需詳細指示，請參閱《AWS Resource Access Manager 使用者指南》中的在 AWSAWS RAM中刪除資源共用。

3. 使用 IPAM 管理員帳戶，登入 RAM 主控台，然後停用在 步驟 6.1. 在 中啟用資源共用 AWS RAM 中啟用的與 AWS Organizations 共用功能。
4. 使用 IPAM 管理員帳戶，透過在 IPAM 主控台中選取 IPAM，然後選擇 動作 > 刪除，以刪除 IPAM 範例。如需詳細說明，請參閱 刪除 IPAM。
5. 當系統提示您刪除 IPAM 時，請選擇串聯刪除。如此會先刪除 IPAM 內的所有範圍和集區，然後再刪除 IPAM。



6. 輸入 delete，然後選擇刪除。
7. 使用 AWS Organizations 管理帳戶登入 IPAM 主控台，選擇設定，然後移除委派的管理員帳戶。
8. （選用）當您整合 IPAM 與 時 AWS Organizations，IPAM 會自動在每個成員帳戶中建立服務連結角色。使用每個 AWS Organizations 成員帳戶登入 IAM，並刪除每個成員帳戶中的 AWSServiceRoleForIPAM 服務連結角色。
9. 清理完成。

教學課程：使用 建立 IPAM 和集區 AWS CLI

遵循本教學課程中的步驟，使用 AWS CLI 來建立 IPAM、建立 IP 地址集區，以及使用來自 IPAM 集區的 CIDR 配置 VPC。

只要依照本節中的步驟，即可建立如下的集區結構階層範例：

- 在 AWS 區域 1、 AWS 區域 2 中操作的 IPAM

- 私有範圍
  - 最上層集區
    - AWS 區域 2 中的區域集區
      - 開發集區
        - VPC 的配置

> **Note**
>
> 在本節中，您會建立 IPAM。預設情況下，只能建立一個 IPAM。如需詳細資訊，請參閱IPAM 的配額。如果已委派 IPAM 帳戶並建立 IPAM，則可略過步驟 1 和 2。

目錄

步驟 1：在您的組織中啟用 IPAM

此為選擇性步驟。完成此步驟以在組織中啟用 IPAM，並使用 CLI AWS 設定委派 IPAM。如需有關 IPAM 帳戶角色的詳細資訊，請參閱 將 IPAM 與 AWS Organizations 中的帳戶整合。

此請求必須從 AWS Organizations 管理帳戶提出。執行下列命令時，請務必使用具備 IAM 政策的角色，如此才能執行下列動作：

- `ec2:EnableIpamOrganizationAdminAccount`
- `organizations:EnableAwsServiceAccess`
- `organizations:RegisterDelegatedAdministrator`

- iam:CreateServiceLinkedRole

```
aws ec2 enable-ipam-organization-admin-account --region us-east-1 --delegated-admin-
account-id 11111111111
```

您應會看到表示啟用成功的以下輸出結果。

```
{
    "Success": true
}
```

步驟 2：建立 IPAM

請按照本節中的步驟來建立 IPAM，並檢視與建立之範圍有關的更多資訊。在稍後的步驟中為這些集區建立集區並佈建 IP 地址範圍時，將會用到此 IPAM。

> **Note**
>
> 操作區域選項會決定 IPAM 集區可用於哪些 AWS 區域。如需有關作業區域的詳細資訊，請參閱 建立 IPAM。

使用 建立 IPAM AWS CLI

1. 執行下列命令以建立 IPAM 執行個體。

   ```
   aws ec2 create-ipam --description my-ipam --region us-east-1 --operating-
   regions RegionName=us-west-2
   ```

   當您建立 IPAM 時， AWS 會自動執行下列動作：

   - 傳回 IPAM 的全域唯一資源 ID (IpamId)。
   - 建立預設的公有範圍 (PublicDefaultScopeId) 和預設的私有範圍 (PrivateDefaultScopeId)。

   ```
   {

       "Ipam": {
   ```

```
        "OwnerId": "123456789012",
        "IpamId": "ipam-0de83dba6694560a9",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
        "PublicDefaultScopeId": "ipam-scope-02a24107598e982c5",
        "PrivateDefaultScopeId": "ipam-scope-065e7dfe880df679c",
        "ScopeCount": 2,
        "Description": "my-ipam",
        "OperatingRegions": [
            {
                "RegionName": "us-west-2"
            },
            {
                "RegionName": "us-east-1"
            }
        ],
        "Tags": []
    }
}
```

2. 執行下列命令以檢視與範圍相關的更多資訊。公有範圍專用於要透過公有網際網路存取的 IP 位址。私有範圍專用於不透過公有網際網路存取的 IP 位址。

```
aws ec2 describe-ipam-scopes --region us-east-1
```

輸出結果會顯示可用的範圍。您將在下一個步驟中用到私有範圍 ID。

```
{
    "IpamScopes": [
        {
            "OwnerId": "123456789012",
            "IpamScopeId": "ipam-scope-02a24107598e982c5",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-02a24107598e982c5",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
            "IpamScopeType": "public",
            "IsDefault": true,
            "PoolCount": 0
        },
        {
            "OwnerId": "123456789012",
            "IpamScopeId": "ipam-scope-065e7dfe880df679c",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-065e7dfe880df679c",
```

```
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
            "IpamScopeType": "private",
            "IsDefault": true,
            "PoolCount": 0
        }
    ]
}
```

步驟 3：建立 IPv4 地址集區

請依照本節中的步驟來建立 IPv4 地址集區。

> **Important**
>
> 您不會在此頂層集區使用 `--locale` 選項。您稍後會設定區域集區上的地區設定選項。地區設定為您希望集區可供 CIDR 分配使用的 AWS 區域。由於未在頂層集區上設定地區設定，地區設定會預設為 None。如果集區具有 的地區設定None，則集區將無法供任何 AWS 區域中的 VPC 資源使用。您只能在集區中手動分配 IP 地址空間以保留空間。

使用 為所有 AWS 資源建立 IPv4 地址集區 AWS CLI

1. 執行下列命令以建立 IPv4 地址集區。使用您在上一個步驟中建立的 IPAM 私有範圍 ID。

   ```
   aws ec2 create-ipam-pool --ipam-scope-id ipam-scope-065e7dfe880df679c --
   description "top-level-pool" --address-family ipv4
   ```

   輸出結果會顯示集區的 `create-in-progress` 狀態。

   ```
   {
       "IpamPool": {
           "OwnerId": "123456789012",
           "IpamPoolId": "ipam-pool-0008f25d7187a08d9",
           "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
   pool-0008f25d7187a08d9",
           "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
   scope-065e7dfe880df679c",
           "IpamScopeType": "private",
           "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
           "Locale": "None",
   ```

```
        "PoolDepth": 1,
        "State": "create-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "AddressFamily": "ipv4",
        "Tags": []
    }
}
```

2. 執行下列命令，直到輸出結果顯示 `create-complete` 的狀態為止。

```
aws ec2 describe-ipam-pools
```

下例的輸出結果顯示正確狀態。

```
{
    "IpamPools": [
        {
            "OwnerId": "123456789012",
            "IpamPoolId": "ipam-pool-0008f25d7187a08d9",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0008f25d7187a08d9",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-065e7dfe880df679c",
            "IpamScopeType": "private",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
            "Locale": "None",
            "PoolDepth": 1,
            "State": "create-complete",
            "Description": "top-level-pool",
            "AutoImport": false,
            "AddressFamily": "ipv4"
        }
    ]
}
```

步驟 4：在最上層集區佈建 CIDR

依照本節中的步驟來佈建最上層集區的 CIDR，然後確認 CIDR 已佈建。如需詳細資訊，請參閱佈建集區的 CIDR。

使用 將 CIDR 區塊佈建至集區 AWS CLI

1. 執行下列命令以佈建 CIDR。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0008f25d7187a08d9 --cidr 10.0.0.0/8
```

您可在輸出結果中確認佈建的狀態。

```
{
    "IpamPoolCidr": {
        "Cidr": "10.0.0.0/8",
        "State": "pending-provision"
    }
}
```

2. 執行下列命令，直到輸出結果顯示 provisioned 的狀態為止。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0008f25d7187a08d9
```

下例的輸出結果顯示正確狀態。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "10.0.0.0/8",
            "State": "provisioned"
        }
    ]
}
```

步驟 5. 利用最上層集區中的 CIDR 建立區域集區

當您建立 IPAM 集區時，集區預設屬於 IPAM AWS 的區域。用來建立 VPC 的集區需與該 VPC 位於相同的區域。建立集區時若使用 --locale 選項，則 IPAM 區域以外之其他區域內的服務可使用該集區。請依照本節中的步驟，以其他地區設定建立區域集區。

使用 建立具有來自先前集區的 CIDR 的集區 AWS CLI

1. 執行下列命令以建立集區並插入空間，該空間包含先前集區的已知可用 CIDR。

```
aws ec2 create-ipam-pool --description "regional--pool" --region us-east-1 --ipam-
scope-id ipam-scope-065e7dfe880df679c --source-ipam-pool-id
ipam-pool-0008f25d7187a08d9 --locale us-west-2 --address-family ipv4
```

輸出結果會顯示您所建立之集區的 ID。下一個步驟需要用到此 ID。

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0da89c821626f1e4b",
        "SourceIpamPoolId": "ipam-pool-0008f25d7187a08d9",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0da89c821626f1e4b",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-065e7dfe880df679c",
        "IpamScopeType": "private",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
        "Locale": "us-west-2",
        "PoolDepth": 2,
        "State": "create-in-progress",
        "Description": "regional--pool",
        "AutoImport": false,
        "AddressFamily": "ipv4",
        "Tags": []
    }
}
```

2. 執行下列命令，直到輸出結果顯示 `create-complete` 的狀態為止。

```
aws ec2 describe-ipam-pools
```

您會在輸出結果中看到 IPAM 內的集區。在本教學課程中，我們建立了最上層和區域集區，所以這兩種集區您都會看到。

```
{
    "IpamPools": [
        {
```

```
            "OwnerId": "123456789012",
            "IpamPoolId": "ipam-pool-0008f25d7187a08d9",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0008f25d7187a08d9",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-065e7dfe880df679c",
            "IpamScopeType": "private",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
            "Locale": "None",
            "PoolDepth": 1,
            "State": "create-complete",
            "Description": "top-level-pool",
            "AutoImport": false,
            "AddressFamily": "ipv4"
        },
        {
            "OwnerId": "123456789012",
            "IpamPoolId": "ipam-pool-0da89c821626f1e4b",
            "SourceIpamPoolId": "ipam-pool-0008f25d7187a08d9",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0da89c821626f1e4b",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-065e7dfe880df679c",
            "IpamScopeType": "private",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
            "Locale": "us-west-2",
            "PoolDepth": 2,
            "State": "create-complete",
            "Description": "regional--pool",
            "AutoImport": false,
            "AddressFamily": "ipv4"
        }
    ]
}
```

步驟 6：在區域集區中佈建 CIDR

依照本節中的步驟將 CIDR 區塊指派給集區，並確認佈建成功。

使用 將 CIDR 區塊指派給區域集區 AWS CLI

1. 執行下列命令以佈建 CIDR。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0da89c821626f1e4b --cidr 10.0.0.0/16
```

輸出結果會顯示集區的狀態。

```
{
    "IpamPoolCidr": {
        "Cidr": "10.0.0.0/16",
        "State": "pending-provision"
    }
}
```

2. 執行下列命令，直到輸出結果顯示 provisioned 的狀態為止。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0da89c821626f1e4b
```

下例的輸出結果顯示正確狀態。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "10.0.0.0/16",
            "State": "provisioned"
        }
    ]
}
```

3. 執行下列命令以查詢最上層集區，藉此檢視配置。區域集區會被視為是最上層集區內的配置。

```
aws ec2 get-ipam-pool-allocations --region us-east-1 --ipam-pool-id ipam-
pool-0008f25d7187a08d9
```

輸出結果會顯示區域集區配置於最上層集區中。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "10.0.0.0/16",
```

```
            "IpamPoolAllocationId": "ipam-pool-alloc-
fbd525f6c2bf4e77a75690fc2d93479a",
            "ResourceId": "ipam-pool-0da89c821626f1e4b",
            "ResourceType": "ipam-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

步驟 7. 建立 RAM 共用以啟用跨帳戶的 IP 指派

此為選用步驟。必須先完成 將 IPAM 與 AWS Organizations 中的帳戶整合 才能完成此步驟。

當您建立 IPAM 集區 AWS RAM 共用時，它會啟用跨帳戶的 IP 指派。RAM 共用僅適用於您的主要 AWS 區域。請注意，此共用是在 IPAM 所在的區域中建立，而不是在集區的本機區域中建立。IPAM 資源的一切管理作業都是透過 IPAM 的主區域進行。本教學課程中的範例會為單一集區建立單一共用，但您可在單一共用中新增多個集區。如需詳細資訊 (包括必須輸入之選項的相關說明)，請參閱 透過 AWS RAM 共用 IPAM 集區。

執行下列命令以建立資源共用。

```
aws ram create-resource-share --region us-east-1 --name pool_share --resource-
arns arn:aws:ec2::123456789012:ipam-pool/ipam-pool-0dec9695bca83e606 --
principals 123456
```

輸出結果會顯示集區已建立。

```
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-west-2:123456789012:resource-
share/3ab63985-99d9-1cd2-7d24-75e93EXAMPLE",
        "name": "pool_share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565295733.282
    }
}
```

步驟 8. 建立 VPC

執行下列命令以建立 VPC，並將新建 IPAM 集區的 CIDR 區塊指派給 VPC。

```
aws ec2 create-vpc --region us-east-1 --ipv4-ipam-pool-id ipam-pool-04111dca0d960186e
 --cidr-block 10.0.0.0/24
```

輸出結果會顯示 VPC 已建立。

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/24",
        "DhcpOptionsId": "dopt-19edf471",
        "State": "pending",
        "VpcId": "vpc-0983f3c454f3d8be5",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-00b24cc1c2EXAMPLE",
                "CidrBlock": "10.0.0.0/24",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false
    }
}
```

步驟 9. 清除

請依照本節中的步驟刪除您在本教學課程中建立的 IPAM 資源。

1. 刪除 VPC。

   ```
   aws ec2 delete-vpc --vpc-id vpc-0983f3c454f3d8be5
   ```

2. 刪除 IPAM 集區 RAM 共用。

```
aws ram delete-resource-share --resource-share-arn arn:aws:ram:us-
west-2:123456789012:resource-share/3ab63985-99d9-1cd2-7d24-75e93EXAMPLE
```

3. 解除佈建區域集區的集區 CIDR。

```
 aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id ipam-pool-0da89c821626f1e4b --
region us-east-1
```

4. 解除佈建最上層集區的集區 CIDR。

```
 aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id ipam-pool-0008f25d7187a08d9 --
region us-east-1
```

5. 刪除 IPAM

```
aws ec2 delete-ipam --region us-east-1
```

教學課程：使用 檢視 IP 地址歷史記錄 AWS CLI

本節中的方案將會顯示如何使用 AWS CLI來分析及稽核 IP 地址使用情況。如需使用 的一般資訊 AWS CLI，請參閱《 AWS 命令列界面使用者指南》中的使用 AWS CLI 。

目錄

概要

IPAM 最長可自動保留您的 IP 地址監控資料三年。您可使用歷程資料來分析和稽核網路安全和路由政策。您可搜尋下列資源類型的歷程深入洞察：

- VPC
- VPC 子網路
- 彈性 IP 位址
- 正在執行的 EC2 執行個體
- 連接至執行個體的 EC2 網路介面

Important

雖然 IPAM 不會監控 Amazon EC2 執行個體或連接至介面的 EC2 網路介面，但您可使用搜尋 IP 歷史記錄功能來搜尋 EC2 執行個體和網路介面 CIDR 的相關歷程資料。

Note

- 本教學課程中的命令必須使用擁有 IPAM 的帳戶和託管 IPAM AWS 的區域來執行。
- CIDR 的變更記錄會從定期快照中取用，這表示記錄的顯示或更新可能需要一些時間，而 SampledStartTime 和 SampledEndTime 的值可能與其實際發生時間不同。

案例

本節中的方案將會顯示如何使用 AWS CLI來分析及稽核 IP 地址使用情況。如需有關本教學課程中所提及值 (如抽樣結束時間和開始時間) 的詳細資訊，請參閱 檢視 IP 位址歷程記錄。

方案 1：在 2021 年 12 月 27 日（UTC）上午 1:00 到晚上 9:00 之間，哪些資源與 **10.2.1.155/32** 相關聯？

1. 執行以下命令：

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 10.2.1.155/32 --ipam-scope-id ipam-scope-05b579a1909c5fc7a --start-time 2021-12-20T01:00:00.000Z --end-time 2021-12-27T21:00:00.000Z
```

2. 檢視分析的結果。於下方範例中，CIDR 在這段時間中被分配給網路介面和 EC2 執行個體。請注意，無 SampledEndTime 值表示記錄仍然有效。如需有關下列輸出結果中顯示值的詳細資訊，請參閱 檢視 IP 位址歷程記錄。

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "network-interface",
            "ResourceId": "eni-0b4e53eb1733aba16",
            "ResourceCidr": "10.2.1.155/32",
```

```
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "instance",
            "ResourceId": "i-064da1f79baed14f3",
            "ResourceCidr": "10.2.1.155/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

如果連接網路介面的執行個體擁有者 ID 與網路介面的擁有者 ID 不同 (NAT 閘道、VPCs 中的 Lambda 網路介面和其他 AWS 服務也是如此），則 `ResourceOwnerId`amazon-aws不是網路介面擁有者的帳戶 ID。下列範例顯示 CIDR 的記錄與 NAT 閘道相關聯：

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "network-interface",
            "ResourceId": "eni-0b4e53eb1733aba16",
            "ResourceCidr": "10.0.0.176/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "amazon-aws",
            "ResourceRegion": "us-east-1",
            "ResourceType": "instance",
            "ResourceCidr": "10.0.0.176/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

方案 2：從 2021 年 12 月 1 日到 2021 年 12 月 27 日之間，哪些資源與 **10.2.1.0/24** 相關聯？

1. 執行以下命令：

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 10.2.1.0/24 --ipam-scope-id ipam-scope-05b579a1909c5fc7a --start-time 2021-12-01T00:00:00.000Z --end-time 2021-12-27T23:59:59.000Z
```

2. 檢視分析的結果。於下方範例中，CIDR 在這段時間被分配給子網路和 VPC。請注意，無 SampledEndTime 值表示記錄仍然有效。如需有關下列輸出結果中顯示值的詳細資訊，請參閱 檢視 IP 位址歷程記錄。

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0864c82a42f5bffed",
            "ResourceCidr": "10.2.1.0/24",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0f5ee7e1ba908a378",
            "ResourceCidr": "10.2.1.0/24",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

方案 3：從 2021 年 12 月 1 日到 2021 年 12 月 27 日 (UTC) 之間，哪些資源與 **2605:9cc0:409::/56** 相關聯？

1. 執行下列命令，其中 --region 是 IPAM 主區域：

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 2605:9cc0:409::/56 --
ipam-scope-id ipam-scope-07cb485c8b4a4d7cc --start-time 2021-12-01T01:00:00.000Z --
end-time 2021-12-27T23:59:59.000Z
```

2. 檢視分析的結果。於下方範例中，在 IPAM 主區域之外的區域中，CIDR 在一段時間內被分配給兩個不同的 VPC。請注意，無 SampledEndTime 值表示記錄仍然有效。如需有關下列輸出結果中顯示值的詳細資訊，請參閱 檢視 IP 位址歷程記錄。

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-01d967bf3b923f72c",
            "ResourceCidr": "2605:9cc0:409::/56",
            "ResourceName": "First example VPC",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-01d967bf3b923f72c",
            "SampledStartTime": "2021-12-23T20:02:00.701000+00:00",
            "SampledEndTime": "2021-12-23T20:12:59.848000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-03e62c7eca81cb652",
            "ResourceCidr": "2605:9cc0:409::/56",
            "ResourceName": "Second example VPC",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-03e62c7eca81cb652",
            "SampledStartTime": "2021-12-27T15:11:00.046000+00:00"
        }
    ]
}
```

方案 4：在過去 24 小時內 (假設目前時間為 2021 年 12 月 27 日 (UTC) 的午夜)，哪些資源與 10.0.0.0/24 相關聯？

1. 執行以下命令：

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 10.0.0.0/24 --ipam-
scope-id ipam-scope-05b579a1909c5fc7a --start-time 2021-12-27T00:00:00.000Z
```

2. 檢視分析的結果。於下方範例中，CIDR 已在此期間內被分配給了許多子網路和 VPC。請注意，無 SampledEndTime 值表示記錄仍然有效。如需有關下列輸出結果中顯示值的詳細資訊，請參閱檢視 IP 位址歷程記錄。


```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0d1b8f899725aa72d",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "VpcId": "vpc-042b8a44f64267d67",
            "SampledStartTime": "2021-12-11T16:35:59.074000+00:00",
            "SampledEndTime": "2021-12-28T15:34:00.017000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-09754dfd85911abec",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-09754dfd85911abec",
            "SampledStartTime": "2021-12-27T20:07:59.947000+00:00",
            "SampledEndTime": "2021-12-28T15:34:00.017000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-west-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0a8347f594bea5901",
```

```
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-0a8347f594bea5901",
            "SampledStartTime": "2021-12-11T16:35:59.318000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0af7eadb0798e9148",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "VpcId": "vpc-03298ba16756a8736",
            "SampledStartTime": "2021-12-14T21:07:22.357000+00:00"
        }
    ]
}
```

方案 5：哪些資源目前與 **10.2.1.155/32** 相關聯？

1. 執行以下命令：

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 10.2.1.155/32 --ipam-
scope-id ipam-scope-05b579a1909c5fc7a
```

2. 檢視分析的結果。於下方範例中，CIDR 在這段時間被分配給網路介面和 EC2 執行個體。請注意，無 SampledEndTime 值表示記錄仍然有效。如需有關下列輸出結果中顯示值的詳細資訊，請參閱 檢視 IP 位址歷程記錄。

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "network-interface",
            "ResourceId": "eni-0b4e53eb1733aba16",
            "ResourceCidr": "10.2.1.155/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
```

```
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "instance",
            "ResourceId": "i-064da1f79baed14f3",
            "ResourceCidr": "10.2.1.155/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

方案 6：哪些資源目前與 **10.2.1.0/24** 相關聯？

1. 執行以下命令：

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 10.2.1.0/24 --ipam-
scope-id ipam-scope-05b579a1909c5fc7a
```

2. 檢視分析的結果。在下方範例中，CIDR 在一段時間段內被分配給 VPC 和子網路。僅傳回與此 /24 CIDR 完全相符的結果，而非 /24 CIDR 中的所有 /32 。請注意，無 SampledEndTime 值表示記錄仍然有效。如需有關下列輸出結果中顯示值的詳細資訊，請參閱 檢視 IP 位址歷程記錄。

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0864c82a42f5bffed",
            "ResourceCidr": "10.2.1.0/24",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0f5ee7e1ba908a378",
            "ResourceCidr": "10.2.1.0/24",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
```

```
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

方案 7：哪些資源目前與 **54.0.0.9/32** 相關聯？

在此範例中，54.0.0.9/32 會指派給彈性 IP 地址，該地址不屬於與您的 IPAM 整合 AWS 的組織。

1. 執行以下命令：

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 54.0.0.9/32 --ipam-
scope-id ipam-scope-05b579a1909c5fc7a
```

2. 由於 54.0.0.9/32 指派給的彈性 IP 地址不屬於此範例中與 IPAM 整合 AWS 的組織，因此不會傳回任何記錄。

```
{
    "HistoryRecords": []
}
```

教學課程：將 ASN 帶入 IPAM

如果您的應用程式使用的是合作夥伴或客戶允許在其網路中列出的受信任 IP 地址和自治系統編號 (ASN)，您可以在 AWS 中執行這些應用程式，而不需要合作夥伴或客戶變更其允許清單。

自治系統編號 (ASN) 是一個全域唯一編號，可透過網際網路識別一組網路，並使用邊界閘道協定動態地與其他網絡交換路由資料。例如，網際網路服務供應商 (ISP) 會使用 ASN 來識別網路流量來源。並非所有組織都會購買自己的 ASN，但對於購買的組織，他們可以將其 ASN 帶入 AWS。

帶入自有自治系統編號 (BYOASN) 後，可使用自有的公開 ASN (而不是 AWS ASN) 公告帶入 AWS 的 IPv4 或 IPv6 地址。使用 BYOASN 時，源自 IP 地址的流量會承載 ASN (而不是 AWS ASN)；根據您的 IP 地址和 ASN，允許列出流量的客戶或合作夥伴可以存取您的工作負載。

Important

- 使用 IPAM 主區域中的 IPAM 管理員帳戶完成本教學課程。

- 本教學課程假設您擁有要帶入 IPAM 的公開 ASN、已將 BYOIP CIDR 帶入 AWS 並且已將其佈建到公有範圍中的集區。您可以隨時將 ASN 帶入 IPAM，但必須與您帶入 AWS 帳戶的 CIDR 建立關聯才能使用。此教學課程假設您已執行下列作業：如需更多詳細資訊，請參閱教學課程：將 IP 地址帶入 IPAM。
- 您可以立即在公告自有 ASN 或 AWS ASN 之間變更，但僅限於每小時從 AWS ASN 變更為自有 ASN 一次。
- 如果目前已公告 BYOIP CIDR，則不需要將其從公告中撤銷，就能與您的 ASN 建立關聯。

ASN 加入先決條件

完成本教學課程需要以下各項：

- 公開的 2 位元組或 4 位元組 ASN。
- 如果您已使用 教學課程：將 IP 地址帶入 IPAM 將 IP 位址範圍帶入 AWS，則需要 IP 位址 CIDR 範圍。您也需要私有金鑰。您可以使用在將 IP 位址 CIDR 範圍帶入 AWS 時建立的私有金鑰，也可以按照 Amazon EC2 User Guide 中的 Create a private key and generate an X.509 certificate 中所述建立新的私有金鑰。
- 當您使用 教學課程：將 IP 地址帶入 IPAM 將 IPv4 或 IPv6 地址範圍帶入 AWS 時，您會建立 X.509 憑證，並將 X.509 憑證上傳到 RIR 中的 RDAP 記錄。您必須將您所建立的相同憑證上傳到 ASN 的 RIR 中的 RDAP 記錄。請務必包含 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 字串之前和之後的編碼部分。所有這些內容都必須在單獨的長線上。更新 RDAP 的程序取決於您的 RIR：
  - 對於 ARIN，請使用客戶經理入口網站，藉由使用「修改 ASN」選項，在代表您 ASN 的「網路資訊」物件的「Public Comments」區段中新增憑證。請勿將其新增至您組織的評論區段。
  - 對於 RIPE，請將憑證作為新的「descr」欄位新增至代表您 ASN 的「aut-num」物件。您通常可以在

    RIPE 資料庫入口網站的「我的資源」區段找到這些內容。請勿將其新增至組織的註解區段，或「aut-num」物件的「備註」欄位。
  - 對於 APNIC，請透過電子郵件將憑證傳送至 helpdesk@apnic.net，以手動將其新增至 ASN 的「備註」欄位。使用 ASN 的 APNIC 授權聯絡人傳送電子郵件。
- 當您將 IP 位址範圍帶入 IPAM 時，您需要建立 ROA，以驗證您對所帶入 IPAM 的 IP 位址空間擁有控制權。除了該 ROA 之外，您還必須在 RIR 中建立第二個 ROA，其中包含您要帶入 IPAM 的 ASN。如果您在 RIR 中尚未擁有針對 ASN 的第二個 ROA，請完成 3. 在 RIR 中建立一個 ROA 物件。忽略其他步驟。

教學步驟

使用 AWS 主控台或 AWS CLI 完成以下步驟。

AWS Management Console

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在左側導覽窗格中，選擇 IPAMs (IPAM)。
3. 選擇您的 IPAM。
4. 選擇 BYOASNs (BYOASN) 索引標籤，然後選擇 Provision BYOASNs (佈建 BYOASN)。
5. 輸入 ASN。因此，Message (訊息) 欄位會自動填入下一個步驟中需要登入的訊息。

   - 訊息的格式如下，其中 ACCOUNT 是您的 AWS 帳號，ASN 是要帶入 IPAM 的 ASN，而 YYYYMMDD 是訊息的到期日期 (預設為下個月的最後一天)。範例：

   ```
   text_message="1|aws|ACCOUNT|ASN|YYYYMMDD|SHA256|RSAPSS"
   ```

6. 複製訊息並根據需要將到期日期替換為您自己的值。
7. 使用私有金鑰來簽署訊息。範例：

   ```
   signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
    rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform
    PEM | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
   ```

8. 在 簽章 下，輸入簽章。
9. (可選) 若要佈建其他 ASN，選擇 佈建其他 ASN。最多可以佈建 5 個 ASN。若要增加此配額，請參閱 IPAM 的配額。
10. 選擇 Provision (佈建)。
11. 在 BYOASNs 索引標籤中檢視佈建程序。等待 State (狀態) 從 Pending-provision (待佈建) 變更為 Provisioned (已佈建)。處於 Failed-provision (佈建失敗) 狀態的 BYOASN 會在 7 天後自動移除。成功佈建 ASN 後，您可以將其與 BYOIP CIDR 關聯。
12. 在左側導覽窗格中，選擇 Pools (集區)。
13. 選擇公有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
14. 選擇已佈建 BYOIP CIDR 的區域集區。必須將集區的 Service (服務) 設定為 EC2 並且必須為其選擇地區設定。
15. 選擇 CIDRs (CIDR) 索引標籤，然後選取 BYOIP CIDR。

16. 選擇 Actions (動作) > Manage BYOASN associations (管理 BYOASN 關聯)。
17. 在 Associated BYOASNs (關聯的 BYOASN) 下，選擇已帶入 AWS 的 ASN。如有多個 ASN，可以將多個 ASN 與 BYOIP CIDR 關聯。可以關聯的 ASN 與可帶入 IPAM 的一樣多。請注意，依預設，最多可以將 5 個 ASN 帶入 IPAM。如需更多詳細資訊，請參閱 IPAM 的配額。
18. 選擇關聯。
19. 等候 ASN 關聯完成。ASN 與 BYOIP CIDR 成功關聯後，就可以再次公告 BYOIP CIDR。
20. 選擇 CIDRs (CIDR) 索引標籤。
21. 選取 BYOIP CIDR，然後選擇 Actions (動作) > Advertise (公告)。因此，會顯示 ASN 選項：Amazon ASN 以及已帶入 IPAM 的任何 ASN。
22. 選取已帶入 IPAM 的 ASN，然後選擇 Advertise CIDR (公告 CIDR)。因此，BYOIP CIDR 會進行公告，並將 Advertising (公告) 欄位中的值從 Withdrawn (已撤回) 變更為 Advertised (已公告)。Autonomous System Number (自治系統編號) 欄位會顯示與 CIDR 相關聯的 ASN。
23. (可選) 如果決定要將 ASN 關聯變更回 Amazon ASN，選取 BYOIP CIDR，然後再次選擇 Actions (動作) > Advertise (公告)。這次選擇 Amazon ASN。您可以隨時切換回 Amazon ASN，但每小時只能變更一次自訂 ASN。

此教學課程完成。

清除

1. 取消 ASN 與 BYOIP CIDR 的關聯
   - 若要從公告中撤銷 BYOIP CIDR，在公有範圍的集區中選擇 BYOIP CIDR，然後選擇 Actions (動作) > Withdraw from advertising (從公告中撤回)。
   - 若要取消 ASN 與 CIDR 的關聯，選擇 Actions (動作) > Manage BYOASN associations (管理 BYOASN 關聯)。
2. 取消佈建 ASN
   - 若要取消佈建 ASN，在 BYOASNs (BYOASN) 索引標籤中選擇 ASN，然後選擇 Deprovision ASN (取消佈建 ASN)。即會取消佈建 ASN。處於 Deprovisioned (已取消佈建) 狀態的 BYOASN 會在 7 天後自動移除。

清理完成。

Command line

1. 透過提供您的 ASN 和授權訊息來佈建 ASN。簽章是使用私有金鑰簽署的訊息。

```
aws ec2 provision-ipam-byoasn --ipam-id $ipam_id --asn 12345 --asn-
authorization-context Message="$text_message",Signature="$signed_message"
```

2. 描述 ASN 以追蹤佈建程序。如果請求成功，應會在幾分鐘後看到 ProvisionStatus (佈建狀態) 已設定為 provisioned (已佈建)。

```
aws ec2 describe-ipam-byoasn
```

3. 將 ASN 與 BYOIP CIDR 關聯。想要公告的任何自訂 ASN 都必須先與 CIDR 關聯。

```
aws ec2 associate-ipam-byoasn --asn 12345 --cidr xxx.xxx.xxx.xxx/n
```

4. 描述 CIDR 以追蹤關聯程序。

```
aws ec2 describe-byoip-cidrs --max-results 10
```

5. 使用 ASN 公告 CIDR。如果已公告 CIDR，則會將原始 ASN 從 Amazon 交換為自有 ASN。

```
aws ec2 advertise-byoip-cidr --asn 12345 --cidr xxx.xxx.xxx.xxx/n
```

6. 描述 CIDR，以查看 ASN 狀態從 associated (已關聯) 至 advertised (已公告) 的變更。

```
aws ec2 describe-byoip-cidrs --max-results 10
```

此教學課程完成。

清除

1. 執行以下任意一項：

   - 如果希望僅撤回 ASN 公告並重新使用 Amazon ASN，同時保持公告 CIDR，必須為 asn 參數呼叫具有特殊 AWS 值的 advertise-byoip-cidr。您可以隨時切換回 Amazon ASN，但每小時只能變更一次自訂 ASN。

     ```
     aws ec2 advertise-byoip-cidr --asn AWS --cidr xxx.xxx.xxx.xxx/n
     ```

- 要同時撤回 CIDR 和 ASN 公告，可以呼叫 withdraw-byoip-cidr。

```
aws ec2 withdraw-byoip-cidr --cidr xxx.xxx.xxx.xxx/n
```

2. 若要清除 ASN，必須先取消其與 BYOIP CIDR 的關聯。

```
aws ec2 disassociate-ipam-byoasn --asn 12345 --cidr xxx.xxx.xxx.xxx/n
```

3. ASN 與相關聯的所有 BYOIP CIDR 取消關聯後，可以將其取消佈建。

```
aws ec2 deprovision-ipam-byoasn --ipam-id $ipam_id --asn 12345
```

4. 移除所有 ASN 關聯之後，也可以取消佈建 BYOIP CIDR。

```
aws ec2 deprovision-ipam-pool-cidr --ipam-pool-id ipam-pool-1234567890abcdef0 --
cidr xxx.xxx.xxx.xxx/n
```

5. 確認取消佈建。

```
aws ec2 get-ipam-pool-cidrs --ipam-pool-id ipam-pool-1234567890abcdef0
```

清理完成。

教學課程：將 IP 地址帶入 IPAM

本節中的教學課程會逐步解說如何使用 IPAM 將公有 IP 地址空間帶入 AWS 和管理空間的程序。

使用 IPAM 的公有 IP 地址空間有如下優點：

- 改善您的組織的公有 IP 地址使用率：透過 IPAM 可跨多個 AWS 帳戶共用 IP 地址空間。如果不使用 IPAM，就無法跨多個 AWS Organizations 帳戶共用公有 IP 空間。
- 簡化將公有 IP 空間帶到以下位置的程序 AWS：您可以使用 IPAM 一次加入公有 IP 地址空間，然後使用 IPAM 將公有 IPs 分佈到區域之間的資源，例如 EC2 執行個體和應用程式負載平衡器。如果沒有 IPAM，您必須為每個 AWS 區域加入公IPs。

目錄

- 使用 AWS 管理主控台和 AWS CLI 兩者，自攜 IP 至 IPAM
- 僅使用 AWS CLI，自攜 IP CIDR 至 IPAM
- 使用 IPAM 將您自己的 IP 帶到 CloudFront （支援 IPv4 和 IPv6)

驗證網域控制

在將 IP 地址範圍帶入目的地之前 AWS，您必須使用本節所述的其中一個選項來驗證您是否控制 IP 地址空間。這同時適用於 IPv4 和 IPv6 地址範圍。稍後，當您將 IP 地址範圍設為 時 AWS， 會 AWS 驗證您是否控制 IP 地址範圍。此驗證可確保客戶無法使用屬於其他人的 IP 範圍，從而防止路由和安全性問題。

您可以使用兩種方法來驗證您控制此範圍：

- X.509 憑證：如果您的 IP 位址範圍已向支援 RDAP 的網際網路註冊機構 (例如 ARIN、RIPE 和 APNIC) 註冊，您可以使用 X.509 憑證驗證網域所有權。
- DNS TXT 記錄：無論您的網際網路登錄檔是否支援 RDAP，您都可以使用驗證符記和 DNS TXT 記錄來驗證網域所有權。

目錄

使用 X.509 憑證驗證網域

本節介紹如何在將 IP 位址範圍帶入 IPAM 前使用 X.509 憑證驗證網域。

使用 X.509 憑證驗證網域

1. 請完成 Amazon EC2 User Guide 的 Prerequisites for BYOIP in Amazon EC2 中的這三個步驟。

> **Note**
>
> 建立 ROA 時，必須將 IPv4 CIDR 的 IP 地址字首的長度上限設定為 /24。若要將 IPv6 CIDR 新增至可公告集區，則 IP 地址字首的長度上限必須為 /48。這可確保您擁有將公有 IP 地址跨 AWS 區域分割的完整彈性。IPAM 會強制執行您設定的長度上限。此長度上限是您宣告的此路由的允許字首最小長度。例如，如果您自攜 /20 CIDR 區塊至 AWS，那麼只要將長度上限設為 /24，即可任意分割更大的區塊 (例如 /21、/22 或 /24)，並將那

些更小的 CIDR 區塊分配給任何區域。若要將長度上限設定為 /23，便無法從更大的區塊分割和公告 /24。另請注意，/24 是最小的 IPv4 區塊，/48 則是您可從區域公告到網際網路的最小 IPv6 區塊。

2. 僅完成《Amazon EC2 使用者指南》中的在 AWS中的佈建可公開公告的地址範圍下的第 1 步和第 2 步，暫時不要佈建地址範圍 (第 3 步)。儲存 `text_message` 和 `signed_message`。您稍後在此過程中會需要這些資訊。

完成這些步驟後，請繼續執行 使用 AWS 管理主控台和 AWS CLI 兩者，自攜 IP 至 IPAM 或 僅使用 AWS CLI，自攜 IP CIDR 至 IPAM。

使用 DNS TXT 記錄驗證網域

完成本節中的步驟，在將 IP 位址範圍帶入 IPAM 之前，使用 DNS TXT 記錄驗證網域。

您可以使用 DNS TXT 記錄來驗證您是否控制公有 IP 位址範圍。DNS TXT 記錄是一種 DNS 記錄類型，其中包含關於您網域名稱的資訊。此功能允許您將註冊於任何網際網路註冊機構 (例如 JPNIC、LACNIC 和 AFRINIC) 的 IP 位址帶入，而不限於支援基於 RDAP（註冊資料存取通訊協定) 驗證的機構 (例如 ARIN、RIPE 和 APNIC)。

> **Important**
>
> 必須先在免費或進階方案中建立 IPAM，才能繼續。如果您沒有 IPAM，請先完成建立 IPAM。

目錄

第 1 步：如果您尚未建立 ROA，請先建立 ROA

您必須在區域網際網路登記機構 (RIR) 中擁有路由來源授權 (ROA)，以公告您希望使用的 IP 位址範圍。如果您的 RIR 中沒有 ROA，請完成 3. 在 RIR 中建立 ROA 物件 (該步驟載於《Amazon EC2 使用者指南》。忽略其他步驟。

您可以使用的最特定 IPv4 位址範圍是 /24。針對可公開公告的 CIDR，您可以使用的最特定 IPv6 地址範圍是 /48，而針對不可公開公告的 CIDR，則是 /60。

步驟 2. 建立驗證符記

驗證字符是 AWS產生的隨機值，可用來證明對外部資源的控制。例如，當您將 IP 地址範圍帶至 AWS (BYOIP) 時，您可以使用驗證字符來驗證您是否控制公有 IP 地址範圍。

完成本節的步驟以建立驗證符記，您在本教學稍後的步驟中將需要此字符來將 IP 位址範圍帶入 IPAM。針對 AWS 主控台或 使用下列指示 AWS CLI。

AWS Management Console

建立驗證符記

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在 AWS 管理主控台中，選擇您建立 IPAM AWS 的區域。
3. 在左側導覽窗格中，選擇 IPAMs (IPAM)。
4. 選擇您的 IPAM，然後選擇 驗證符記標籤。
5. 選取 建立驗證符記。
6. 建立符記之後，請保持此瀏覽器索引標籤開啟。接下來的步驟您需要用到 符記值、符記名稱，以及後續步驟中需要的 符記 ID。

注意下列事項：

- 建立驗證符記後，您可以在 72 小時內重複使用該符記，用於從 IPAM 中佈建的多個 BYOIP CIDR。若超過 72 小時仍需佈建更多 CIDR，則需要建立新的驗證符記。
- 您最多可以建立 100 個符記。如果您達到限制，請刪除過期的符記。

Command line

- 使用 create-ipam-external-resource-verification-token 請求 IPAM 建立驗證符記，該字符將用於 DNS 組態：

```
aws ec2 create-ipam-external-resource-verification-token --ipam-id ipam-id
```

這將傳回具有 TokenName 和 TokenValue 的 IpamExternalResourceVerificationTokenId 和字符，以及符記的過期時間 (NotAfter)。

```
{
```

```
    "IpamExternalResourceVerificationToken": {
        "IpamExternalResourceVerificationTokenId": "ipam-ext-res-ver-
token-0309ce7f67a768cf0",
        "IpamId": "ipam-0f9e8725ac3ae5754",
        "TokenValue": "a34597c3-5317-4238-9ce7-50da5b6e6dc8",
        "TokenName": "86950620",
        "NotAfter": "2024-05-19T14:28:15.927000+00:00",
        "Status": "valid",
        "Tags": [],
        "State": "create-in-progress" }
}
```

注意下列事項：

- 建立驗證符記後，您可以在 72 小時內重複使用該符記，用於從 IPAM 中佈建的多個 BYOIP CIDR。若超過 72 小時仍需佈建更多 CIDR，則需要建立新的驗證符記。
- 您可以使用 describe-ipam-external-resource-verification-tokens 檢視符記。
- 您最多可以建立 100 個符記。如果您達到限制，您可以使用 delete-ipam-external-resource-verification-token 刪除過期的符記。

步驟 3。設定 DNS 區域與 TXT 記錄

完成本節中的步驟，以設定 DNS 區域和 TXT 記錄。如果您未使用 Route53 作為 DNS，請參閱您的 DNS 提供商提供的文檔來設定 DNS 區域並新增 TXT 記錄。

如果您使用的是 Route53，請注意下列事項：

- 若要在 AWS 主控台中建立反向查詢區域，請參閱《Amazon Route 53 開發人員指南》中的建立公有託管區域或使用 AWS CLI 命令 create-hosted-zone。
- 若要在 AWS 主控台的反向查詢區域中建立記錄，請參閱《Amazon Route 53 開發人員指南》中的使用 Amazon Route 53 主控台建立記錄或使用 AWS CLI 命令 change-resource-record-sets。
- 建立託管區域後，請將 RIR 中的託管區域委派給 Route53 提供的名稱伺服器 (例如 LACNIC 或 APNIC)。

無論您是使用其他 DNS 供應商或 Route53，當您設定 TXT 記錄時，請注意下列事項：

- 記錄名稱應為符記名稱。
- 記錄類型應為 TXT。

- ResourceRecord 值應為符記值。

範例：

- 名稱: 86950620.113.0.203.in-addr.arpa
- Type (類型)：TXT
- ResourceRecords 值：a34597c3-5317-4238-9ce7-50da5b6e6dc8

其中：

- 86950620 是驗證符記名稱。
- 113.0.203.in-addr.arpa 是反向查詢區域名稱。
- TXT 是記錄類型。
- a34597c3-5317-4238-9ce7-50da5b6e6dc8 是驗證符記值。

> **Note**
>
> 根據使用 BYOIP 帶入 IPAM 的字首大小，必須在 DNS 中建立一或多個身分驗證記錄。這些身分驗證記錄屬於 TXT 記錄類型，並且必須放置在字首本身或其父字首的反向區域中。
>
> - 對於 IPv4，身分驗證記錄需要與構成字首的八位元組界限範圍對齊。
>   - 範例
>   - 對於已在八位元組界限對齊的 198.18.123.0/24，您需要在以下位置建立單一身分驗證記錄：
>   - *token-name*.123.18.198.in-addr.arpa. IN TXT “*token-value*”
>   - 對於 198.18.12.0/22，其本身未與八位元組界限對齊，您將需要建立四個身分驗證記錄。這些記錄必須涵蓋在八位元組界限對齊的子網路 198.18.12.0/24、198.18.13.0/24、198.18.14.0/24 和 198.18.15.0/24。對應的 DNS 項目必須是：
>   - *token-name*.12.18.198.in-addr.arpa. IN TXT “*token-value*”
>   - *token-name*.13.18.198.in-addr.arpa. IN TXT “*token-value*”
>   - *token-name*.14.18.198.in-addr.arpa. IN TXT “*token-value*”
>   - *token-name*.15.18.198.in-addr.arpa. IN TXT “*token-value*”
>   - 對於已在八位元組界限對齊的 198.18.0.0/16，您需要建立單一身分驗證記錄：

    - *token-name*.18.198.in-addr.arpa. IN TXT *“token-value”*
- 對於 IPv6，身分驗證記錄需要與構成字首的半位元組界限範圍對齊。有效的小數位值為 32、36、40、44、48、52、56 和 60。
  - 範例
    - 對於已在半位元組界限對齊的 2001:0db8::/40，您需要建立單一身分驗證記錄：
      - *token-name*.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT *“token-value”*
    - 對於 2001:0db8:80::/42，其本身未對齊半位字節界限，您需要建立四個身分驗證記錄。這些記錄必須涵蓋在半位字節界限對齊的子網路 2001:db8:80::/44、2001:db8:90::/44、2001:db8:a0::/44 和 2001:db8:b0::/44。對應的 DNS 項目必須是：
      - *token-name*.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT *“token-value”*
      - *token-name*.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT *“token-value”*
      - *token-name*.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT *“token-value”*
      - *token-name*.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT *“token-value”*
    - 對於本身未在半位界限對齊的非廣告範圍 2001:db8:0:1000::/54，您需要建立四個身分驗證記錄。這些記錄必須涵蓋在半位字節界限對齊的子網路 2001:db8:0:1000::/56、2001:db8:0:1100::/56、2001:db8:0:1200::/56 和 2001:db8:0:1300::/56。對應的 DNS 項目必須是：
      - *token-name*.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT *“token-value”*
      - *token-name*.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT *“token-value”*
      - *token-name*.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT *“token-value”*
      - *token-name*.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT *“token-value”*
    - 若要驗證 token-name 與 "ip6.arpa" 字串之間的正確十六進位數字，請將該數字乘以四。結果應符合字首長度。例如，對於 /56 字首，您應該有 14 個十六進位數字。

完成這些步驟後，請繼續執行 使用 AWS 管理主控台和 AWS CLI 兩者，自攜 IP 至 IPAM 或 僅使用 AWS CLI，自攜 IP CIDR 至 IPAM。

使用 AWS 管理主控台和 AWS CLI 兩者，自攜 IP 至 IPAM

將自備 IP (BYOIP) 帶至 IPAM 可讓您在 AWS 中使用組織的現有 IPv4 和 IPv6 地址範圍。這可讓您在您自己的 IP 位址空間下整合內部部署和雲端環境，從而維持一致的品牌、提升網路效能、增強安全性並簡化管理。

按照這些步驟，使用 AWS 管理主控台和 AWS CLI 兩者，將 IPv4 或 IPv6 CIDR 帶至 IPAM。

> **Note**
>
> 開始之前，您必須先驗證網域控制。

將 IPv4 地址範圍帶至 AWS 後，您可以使用範圍內的所有 IP 位址，包括第一個地址 (網路地址) 和最後一個地址 (廣播地址)。

目錄

使用 AWS 管理主控台和 CLI 將您自己的 IPv4 CIDR AWS 帶到 IPAM

請依照下列步驟，將 IPv4 CIDR 帶到 IPAM，並使用 管理主控台和 CLI 配置彈性 IP 地址 AWS (EIP) AWS 。

> **Important**
>
> - 此教學課程假設您已完成下列各節中的步驟：
>   - 將 IPAM 與 AWS Organizations 中的帳戶整合.
>   - 建立 IPAM.
> - 本教學課程的每個步驟必須由三個 AWS Organizations 帳戶的其中一個完成：
>   - 管理帳戶。
>   - 在 將 IPAM 與 AWS Organizations 中的帳戶整合 中設定為您 IPAM 管理員的成員帳戶。在本教學課程中，此帳戶將稱為 IPAM 帳戶。
>   - 您組織中的成員帳戶將會從 IPAM 集區分配 CIDR。在本教學課程中，此帳戶將稱為成員帳戶。

目錄

步驟 1：建立 AWS CLI 具名設定檔和 IAM 角色

若要以單一 AWS 使用者身分完成本教學課程，您可以使用 AWS CLI 具名設定檔從一個 IAM 角色切換到另一個角色。具名設定檔是您在搭配 AWS CLI使用 `--profile` 選項時所參考的設定和憑證的集合。如需如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱《》中的使用 IAM 角色 AWS CLI。

為您將在本教學課程中使用的三個 AWS 帳戶各建立一個角色和一個具名設定檔：

- `management-account` 為 AWS Organizations 管理帳戶呼叫的設定檔。
- `ipam-account` 為 AWS Organizations 成員帳戶呼叫的設定檔，設定為您的 IPAM 管理員。
- 您組織中 `member-account` AWS Organizations 成員帳戶的 設定檔，將從 IPAM 集區配置 CIDRs。

建立 IAM 角色和具名設定檔後，請返回此頁面並繼續下一個步驟。在本教學課程的其餘部分，您會注意到範例 AWS CLI 命令使用 `--profile`選項搭配其中一個具名設定檔，以指出哪個帳戶必須執行 命令。

步驟 2：建立最上層 IPAM 集區

完成本節中的步驟來建立最上層 IPAM 集區。

此步驟必須由 IPAM 帳戶完成。

建立集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。選擇公有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇建立集區。
5. (選用) 新增集區的 Name tag (名稱標籤) 和集區的 Description (說明)。
6. 在 Source (來源) 下，選擇 IPAM scope (IPAM 範圍)。
7. 在 Address family (地址系列) 下，選擇 IPv4。
8. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
9. 在 Locale (地區設定) 下，選擇 None (無)。

   IPAM 與 BYOIP 整合需要在 BYOIP CIDR 使用的任何集區上設定地區設定。由於我們將要建立內含區域集區的最上層 IPAM 集區，且要從區域集區分配空間給彈性 IP 地址，因此您必須在區域集區 (而非最上層集區) 上設定地區設定。在稍後的步驟中建立區域集區時，您會新增區域集區的地區設定。

   > **Note**
   >
   > 如果您只建立單一集區，而不是在其中包含區域集區的頂層集區，則會想要為此區域選擇地區設定，以便集區可供配置使用。

10. 在 公有 IP 來源 下，選擇 BYOIP。
11. 在 要佈建的 CIDR 下，執行下列步驟：

    - 如果您使用 X.509 憑證驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 BYOIP 訊息和憑證簽章，以便我們能夠驗證您是否控制公有空間。
    - 如果您使用 DNS TXT 記錄驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 IPAM 驗證符記，以便我們能夠驗證您是否控制公有空間。

    請注意，在最上層集區內的某集區佈建 IPv4 CIDR 時，您可佈建的最小 IPv4 CIDR 為 /24；不得佈建更明確的 CIDR (例如 /25)。

> **Important**
>
> 大多數佈建會在兩個小時內完成，但公開可廣告範圍的佈建過程最多可能需要一週的時間。

12. 將調整此集區的分配規則設定保持在未選取的狀態。
13. (選用) 為集區選擇 Tags (標籤)。
14. 選擇建立集區。

請先確定此 CIDR 已佈建，然後再繼續。您可在集區詳細資訊頁面的 CIDRs (CIDR) 索引標籤中看到佈建狀態。

步驟 3。在最上層集區內建立一個區域集區

在最上層集區內建立一個區域集區。IPAM 與 BYOIP 整合需要在 BYOIP CIDR 使用的任何集區上設定地區設定。於本節中建立區域集區時，您會新增區域集區的地區設定。當您建立了 IPAM，`Locale` 必須是您設定的其中一個作業區域的一部分。例如，地區設定為 us-east-1 表示 us-east-1 必須是 IPAM 的操作區域。地區設定為 us-east-1-scl-1 (用於本地區域的網路邊界群組) 的表示 IPAM 必須具有 us-east-1 的操作區域。

此步驟必須由 IPAM 帳戶完成。

在頂層集區內建立一個區域集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。如果不想使用預設的私有範圍，請從內容窗格最上方的下拉式選單中選擇您要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇建立集區。
5. (選用) 新增集區的 Name tag (名稱標籤) 和集區的 Description (說明)。
6. 在 Source (來源) 下，選擇您在上一節建立的頂層集區。
7. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
8. 在 Locale (區域設定) 下，選擇該集區的區域設定。在本教學課程中，我們將會使用 `us-east-2` 作為區域集區的地區設定。可用選項來自您在建立 IPAM 時選擇的作業區域。

集區的地區設定應是下列其中一項：

- 您希望此 IPAM 集區可用於配置 AWS 的區域。
- 您希望此 IPAM 集區可用於配置的 AWS Local Zone 的網路邊界群組 (支援的 Local Zones)。此選項僅適用於公有範圍內的 IPAM IPv4 集區。
- AWS 專用本地區域。若要在 AWS 專用本機區域中建立集區，請在選取器輸入中輸入 AWS 專用本機區域。
- `Global` 當您想要在所有 AWS 區域全域使用 IP 地址時，例如 CloudFront 位置。`Global` 地區設定僅適用於公有 IPv4 集區。

例如，您只能從與 VPC 區域共用地區設定的 IPAM 集區為 VPC 配置 CIDR。請注意，當您為集區選擇地區時，您無法對其進行修改。如果 IPAM 的主區域因中斷而無法使用，且集區的地區設定與 IPAM 的主區域不同，則仍然可以使用集區來配置 IP 地址。

選擇地區設定可確保您的集區和從中分配的資源之間沒有跨區域的依賴關係。

9. 在 Service (服務) 下，選擇 EC2 (EIP/VPC)。您選取的服務會決定 CIDR 可公告 AWS 的服務。目前，唯一的選項是 EC2 (EIP/VPC)，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務 (適用於彈性 IP 地址) 和 Amazon VPC 服務 (適用於與 VPC 關聯的 CIDR) 進行公告。
10. 在 CIDRs to provision (要佈建的 CIDR) 下，選擇一個要為集區佈建的 CIDR。

> **Note**
>
> 在最上層集區內的某集區佈建 CIDR 時，您可佈建的最具體的 IPv4 CIDR 為 /24；不得佈建更具體的 CIDR (例如 /25)。建立區域集區後，您可以在同一區域集區內建立更小的集區 (例如 /25)。請注意，如果您共用區域集區或其中的集區，這些集區只能在相同區域集區的區域設定中使用。

11. 啟用調整此集區的分配規則設定。您在此處具有與建立頂層集區時相同的配置規則選項。請參閱建立頂層 IPv4 集區，以取得建立集區時可用選項的說明。區域集區的配置規則不是繼承自頂層集區。如果您未在此處套用任何規則，則不會為集區設定配置規則。
12. (選用) 為集區選擇 Tags (標籤)。
13. 當您完成集區的設定後，請選擇 Create pool (建立集區)。

請先確定此 CIDR 已佈建，然後再繼續。您可在集區詳細資訊頁面的 CIDRs (CIDR) 索引標籤中看到佈建狀態。

第 4 步：公告 CIDR

本節中的步驟必須由 IPAM 帳戶完成。將彈性 IP 地址 (EIP) 與執行個體或 Elastic Load Balancer 建立關聯後，您就可以開始公告您帶到的 CIDR AWS ，該 CIDR 位於已設定服務 EC2 (EIP/VPC) 的集區中。在本教學課程中是指您的區域集區。預設情況下不會公告 CIDR，亦即，不能透過網際網路公開存取它。

此步驟必須由 IPAM 帳戶完成。

> **Note**
>
> 廣告狀態不會限制您配置彈性 IP 位址的能力。即使您的 BYOIPv4 CIDR 沒有公告，您仍然可以從 IPAM 集區建立 EIP。

如要公告 CIDR

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。選擇公有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇您在本教學課程中建立的區域集區。
5. 選擇 CIDRs 索引標籤。
6. 選取 BYOIP CIDR，然後選擇 Actions (動作) > Advertise (公告)。
7. 選擇 Advertise CIDR (公告 CIDR)。

因此，BYOIP CIDR 會進行公告，並將 Advertising (公告) 欄位中的值從 Withdrawn (已撤回) 變更為 Advertised (已公告)。

步驟 5. 共用區域集區

遵循本節中的步驟，使用 AWS Resource Access Manager (RAM) 共用 IPAM 集區。

在 中啟用資源共用 AWS RAM

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在您共用 IPAM 集區之前，請完成本節中的步驟，以啟用與 共用資源 AWS RAM。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`management-account`**選項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，在 https：//https://console.aws.amazon.com/ram/ 開啟 AWS RAM 主控台。
2. 在左側導覽窗格中，選擇設定，選擇啟用共用 AWS Organizations，然後選擇儲存設定。

您現在可以與組織的其他成員共用 IPAM 集區。

使用 共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共用區域集區。如需共用 IPAM 集區的完整說明 (包括所需 IAM 許可的相關資訊)，請參閱 透過 AWS RAM 共用 IPAM 集區。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`ipam-account`**選項。

使用 共用 IPAM 集區 AWS RAM

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍，選擇 IPAM 集區，然後選擇 動作 > 檢視詳細資料。
4. 在 Resource sharing (資源共用) 底下，選擇 Create resource share (建立資源共用)。 AWS RAM 主控台隨即開啟。您可以使用 共用集區 AWS RAM。
5. 選擇 Create a resource share (建立資源共用)。
6. 在 AWS RAM 主控台中，再次選擇建立資源共享。
7. 新增共用集區的名稱。
8. 在 選取資源類型 下，選擇 IPAM 集區，然後選擇您要共用的集區 ARN。
9. 選擇下一步。
10. 選擇 AWSRAMPermissionIpamPoolByoipCidrImport 許可。許可選項的詳細資料未涵蓋在本教學課程的範圍，但您可以在 透過 AWS RAM 共用 IPAM 集區 中了解有關這些選項的詳細資訊。
11. 選擇下一步。
12. 在主體 > 選取主體類型下，選擇 AWS 帳戶並輸入要將 IP 地址範圍帶入 IPAM 之帳戶的帳戶 ID，然後選擇新增。
13. 選擇下一步。
14. 檢閱資源共用選項，以及您要與其共用的主體，然後選擇建立。
15. 若要允許 **`member-account`** 帳戶從 IPAM 集區配置 IP 位址 CIDRS，請使用 `AWSRAMDefaultPermissionsIpamPool` 建立第二個資源共用。`--resource-arns` 值為您

在上一節建立之 IPAM 集區的 ARN。`--principals` 的值是 **`member-account`** 的帳戶 ID。`--permission-arns` 值為 `AWSRAMDefaultPermissionsIpamPool` 許可的 ARN。

第 6 步：從集區配置彈性 IP 位址

按照本節中的步驟，從集區配置彈性 IP 位址。請注意，如果您使用公有 IPv4 集區來配置彈性 IP 位址，您可以使用 第 6 步的替代方案 中的替代步驟，而非本節中的步驟。

> **Important**
>
> 如果您看到與沒有呼叫 ec2：AllocateAddress 相關的錯誤，則需要更新目前指派給與您共用的 IPAM 集區的受管許可。聯絡建立資源共用的人員，並要求他們將受管許可 `AWSRAMPermissionIpamResourceDiscovery` 更新為預設版本。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的更新資源共用。

AWS Management Console

請依照《Amazon EC2 使用者指南》中的配置彈性 IP 位址中的步驟配置地址，但請注意下列事項：

- 此步驟必須由該成員帳戶完成。
- 請確定您在 EC2 主控台中的 AWS 區域符合您在建立區域集區時選擇的區域設定選項。
- 選擇地址集區時，請選擇使用 IPv4 IPAM 集區配置的選項，然後選擇您建立的區域集區。

Command line

使用 allocate-address 命令從集區配置地址。您使用的 `--region` 必須與您在步驟 2 中建立集區時所選擇的 `-locale` 選項相符。在 `--ipam-pool-id` 中包含您在第 2 步中建立的 IPAM 集區的 ID。您也可以選擇 IPAM 集區中的特定 `/32`，方法是使用 `--address` 選項。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

回應範例：

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
```

```
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的配置彈性 IP 位址。

第 7 步：建立彈性 IP 位址與 EC2 執行個體的關聯

完成本節中的步驟，建立彈性 IP 位址與 EC2 執行個體的關聯。

AWS Management Console

請遵循 Amazon EC2 使用者指南中的關聯彈性 IP 地址中的步驟，從 IPAM 集區配置彈性 IP 地址，但請注意下列事項：當您使用 AWS 管理主控台選項時，您在 中關聯彈性 IP 地址 AWS 的區域必須符合您在建立區域集區時選擇的區域設定選項。

此步驟必須由該成員帳戶完成。

Command line

此步驟必須由該成員帳戶完成。設定 `--profile` **`member-account`** 選項。

使用 associate-address 命令，建立彈性 IP 位址與 Outpost 執行個體的關聯。您在 `--region` 中關聯彈性 IP 位址的 `--locale` 選項必須與您創建區域集區時選擇的選項相符。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

回應範例：

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的將彈性 IP 位址與執行中的執行個體或網路介面建立關聯。

步驟 8：清除

請依照本節中的步驟清除您在本教學課程中佈建和建立的資源。

步驟 1：從公告中撤回 CIDR

此步驟必須由 IPAM 帳戶完成。

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。選擇公有範圍。
4. 選擇您在本教學課程中建立的區域集區。
5. 選擇 CIDRs 索引標籤。
6. 選取 BYOIP CIDR，然後選擇 Actions (動作) > Withdraw from advertising (從公告中撤回)。
7. 選擇 Withdraw CIDR (撤回 CIDR)。

因此，BYOIP CIDR 不再進行公告，並將 Advertising (公告) 欄位中的值從 Advertised (已公告) 變更為 Withdrawn (已撤回)。

步驟 2：取消與彈性 IP 地址的關聯

此步驟必須由該成員帳戶完成。如果您使用的是 AWS CLI，請使用 `--profile` **`member-account`**選項。

- 完成《Amazon EC2 使用者指南》中取消彈性 IP 位址的關聯中的步驟，以取消 EIP 的關聯。當您在 AWS 管理主控台中開啟 EC2 時，您在 中取消 EIP 關聯的 AWS 區域必須符合您在建立將用於 BYOIP CIDR 的集區時選擇`Locale`的選項。在本教學課程中，集區為區域集區。

步驟 3：釋出彈性 IP 地址

此步驟必須由該成員帳戶完成。如果您使用的是 AWS CLI，請使用 `--profile` **`member-account`**選項。

- 完成《Amazon EC2 使用者指南》中釋出彈性 IP 位址中的步驟，從公有 IPv4 集區釋出彈性 IP 位址 (EIP)。當您在 AWS 管理主控台中開啟 EC2 時，您在其中配置 EIP AWS 的區域必須符合您在建立將用於 BYOIP CIDR 的集區時選擇`Locale`的選項。

步驟 4：刪除任何 RAM 共用並停用與 AWS Organizations 的 RAM 整合

此步驟必須各自由 IPAM 帳戶和管理帳戶完成。如果您使用 AWS CLI 刪除 RAM 共用並停用 RAM 整合，請使用 `--profile` **`ipam-account`**和 `--profile` **`management-account`**選項。

- 完成 RAM AWS 使用者指南中的刪除 RAM 中的資源共用和停用與 AWS Organizations 的資源共用中的步驟，以刪除 RAM 共用並停用與 AWS Organizations 的 RAM 整合。 AWS

第 5 步：從區域集區和最上層集區解除佈建 CIDR

此步驟必須由 IPAM 帳戶完成。如果您使用 AWS CLI 共用集區，請使用 `--profile` **ipam-account**選項。

- 完成 從集區解除佈建 CIDR 中的步驟，依順序從區域集區和最上層集區解除佈建 CIDR。

第 6 步：刪除區域集區和最上層集區

此步驟必須由 IPAM 帳戶完成。如果您使用 AWS CLI 共用集區，請使用 `--profile` **ipam-account**選項。

- 完成 刪除集區 中的步驟，依順序刪除區域集區和最上層集區。

第 6 步的替代方案

如果您使用公有 IPv4 集區來配置彈性 IP 位址，您可以使用本節中的步驟，而非 第 6 步：從集區配置彈性 IP 位址 中的步驟。

目錄

第 1 步：建立公有 IPv4 集區

此步驟應由將佈建彈性 IP 地址的成員帳戶完成。

> **Note**
>
> - 此步驟必須使用 AWS CLI，由該成員帳戶完成。

- 公有 IPv4 集區和 IPAM 集區由 中的不同資源管理 AWS。公有 IPv4 集區是單一帳戶資源，可讓您將公有的 CIDR 轉換為彈性 IP 地址。使用 IPAM 集區可將公有空間配置給公有 IPv4 集區。

使用 建立公有 IPv4 集區 AWS CLI

- 執行下列命令以佈建 CIDR。當您執行本節中的命令時，`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所選擇的 `Locale` 選項相符。

```
aws ec2 create-public-ipv4-pool --region us-east-2 --profile member-account
```

您會在輸出結果中看到公有 IPv4 集區 ID。下一個步驟需要用到此 ID。

```
{
    "PoolId": "ipv4pool-ec2-09037ce61cf068f9a"
}
```

第 2 步：在公有 IPv4 集區佈建公有 IPv4 CIDR

在公有 IPv4 集區佈建公有 IPv4 CIDR。`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所選擇的 `Locale` 值相符。`--netmask-length` 是您要帶入公用集區的 IPAM 集區空間量。數值不能大於 IPAM 集區的網路遮罩長度。您可以定義的最不具體的 `--netmask-length` 是 24。

> **Note**
>
> - 如果您要將 /24 CIDR 範圍帶入 IPAM 以便跨 AWS Organization 共用，則可以將較小的字首佈建至多個 IPAM 集區，例如 /27 (使用 `-- netmask-length 27`)，而不用如本教學課程所示佈建整個 /24 CIDR (使用 `-- netmask-length 24`)。
> - 此步驟必須使用 AWS CLI，由該成員帳戶完成。

使用 建立公有 IPv4 集區 AWS CLI

1. 執行下列命令以佈建 CIDR。

```
aws ec2 provision-public-ipv4-pool-cidr --region us-east-2 --ipam-pool-id ipam-
pool-04d8e2d9670eeab21 --pool-id ipv4pool-ec2-09037ce61cf068f9a --netmask-length 24
 --profile member-account
```

輸出結果會顯示已佈建的 CIDR。

```
{
    "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. 執行下列命令以檢視公有 IPv4 集區中佈建的 CIDR。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --max-results 10 --
profile member-account
```

輸出結果會顯示已佈建的 CIDR。預設情況下不會公告 CIDR，亦即，不能透過網際網路公開存取它。透過本教學課程的最後一個步驟可設定此 CIDR，使其公告在網路上。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 255
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 255,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
```

```
        }
    ]
}
```

建立公有 IPv4 集區後，如要檢視配置於 IPAM 區域集區中的公有 IPv4 集區，請於 Allocations (分配) 或 Resources (資源)下，開啟 IPAM 主控台並檢視區域集區中分配。

第 3 步：在公有 IPv4 集區中配置彈性 IP 位址

完成《Amazon EC2 使用者指南》中配置彈性 IP 位址中的步驟，從公有 IPv4 集區建立 EIP。當您在 AWS 管理主控台中開啟 EC2 時，您在其中配置 EIP AWS 的區域必須符合您在建立將用於 BYOIP CIDR 的集區時選擇`Locale`的選項。

此步驟必須由該成員帳戶完成。如果您使用的是 AWS CLI，請使用 `--profile` **`member-account`**選項。

完成這三個步驟後，請返回 第 7 步：建立彈性 IP 位址與 EC2 執行個體的關聯 並繼續，直到您完成教學課程為止。

第 6 步清除的替代方案

請完成下列步驟，以清除使用第 9 步的替代方案建立的公有 IPv4 集區。您應該在 步驟 8：清除 中的標準清除程序期間釋出彈性 IP 位址之後，完成這些步驟。

第 1 步：從公有 IPv4 集區取消佈建公有 IPv4 CIDR

> **Important**
>
> 此步驟必須使用 AWS CLI，由該成員帳戶完成。

1. 檢視您的 BYOIP CIDR。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

輸出結果會顯示 BYOIP CIDR 中的 IP 地址。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
```

```
            "Description": "",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 256
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 256,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

2. 執行下列命令以釋出公有 IPv4 集區的 CIDR。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-2 --pool-id ipv4pool-
ec2-09037ce61cf068f9a --cidr 130.137.245.0/24 --profile member-account
```

3. 再次檢視您的 BYOIP CIDR，並確保其中不再有已佈建的地址。當您執行本節中的命令時，`--region` 的值必須與 IPAM 的區域相符。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

您會在輸出結果的公有 IPv4 集區中看到 IP 地址計數。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

> **Note**
>
> IPAM 可能需要一些時間才能發現公有 IPv4 集區分配已遭刪除。您無法繼續清除和解除佈建 IPAM 集區的 CIDR，直到您發現配置已從 IPAM 移除為止。

第 2 步：刪除公有 IPv4 集區

此步驟必須由該成員帳戶完成。

- 執行下列命令以刪除公有 IPv4 集區 CIDR。當您執行本節中的命令時，`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所選擇的 `Locale` 選項相符。在本教學課程中，集區為區域集區。此步驟必須使用 CLI AWS 完成。

  ```
  aws ec2 delete-public-ipv4-pool --region us-east-2 --pool-id ipv4pool-
  ec2-09037ce61cf068f9a --profile member-account
  ```

  在輸出中，您將會看到傳回值為 true。

  ```
  {
  "ReturnValue": true
  }
  ```

  刪除集區後，如要檢視未由 IPAM 管理的分配，請開啟 IPAM 主控台，然後檢視 Allocations (分配) 下的區域集區詳細資訊。

使用 AWS 管理主控台將您自己的 IPv6 CIDR 帶到 IPAM

遵循本教學課程中的步驟，將 IPv6 CIDR 帶到 IPAM，並使用 AWS 管理主控台和 配置具有 CIDR 的 VPC AWS CLI。

如果您不需要透過網際網路公告 IPv6 地址，則可以將私有 GUA IPv6 地址佈建至 IPAM。如需詳細資訊，請參閱啟用佈建私有 IPv6 GUA CIDR。

> **Important**
>
> - 此教學課程假設您已完成下列各節中的步驟：
>   - 將 IPAM 與 AWS Organizations 中的帳戶整合.

  - 建立 IPAM.
- 本教學課程的每個步驟必須由三個 AWS Organizations 帳戶的其中一個完成：
  - 管理帳戶。
  - 在 將 IPAM 與 AWS Organizations 中的帳戶整合 中設定為您 IPAM 管理員的成員帳戶。在本教學課程中，此帳戶將稱為 IPAM 帳戶。
  - 您組織中的成員帳戶將會從 IPAM 集區分配 CIDR。在本教學課程中，此帳戶將稱為成員帳戶。

目錄

步驟 1：建立最上層 IPAM 集區

由於您要建立內含區域集區的最上層 IPAM 集區，而且我們要從區域集區配置空間給資源，因此您必須在區域集區 (而不是最上層集區) 上設定地區設定。在稍後的步驟中建立區域集區時，您會新增區域集區的地區設定。IPAM 與 BYOIP 整合需要在 BYOIP CIDR 使用的任何集區上設定地區設定。

此步驟必須由 IPAM 帳戶完成。

建立集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。選擇公有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇建立集區。
5. (選用) 新增集區的 Name tag (名稱標籤) 和集區的 Description (說明)。
6. 在 Source (來源) 下，選擇 IPAM scope (IPAM 範圍)。

7. 在 Address family (地址系列) 下，選擇 IPv6。
8. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
9. 在 Locale (地區設定) 下，選擇 None (無)。您將設定區域集區上的地區設定。

   地區設定是您希望此 IPAM 集區可用於配置 AWS 的區域。例如，您只能從與 VPC 區域共用地區設定的 IPAM 集區為 VPC 配置 CIDR。請注意，當您為集區選擇地區時，您無法對其進行修改。如果 IPAM 的主區域因中斷而無法使用，且集區的地區設定與 IPAM 的主區域不同，則仍然可以使用集區來配置 IP 地址。

   > **Note**
   >
   > 如果您只建立單一集區，而不是在其中包含區域集區的頂層集區，則會想要為此區域選擇地區設定，以便集區可供配置使用。

10. 在公有 IP 來源下，預設會選取 BYOIP。
11. 在 要佈建的 CIDR 下，執行下列步驟：

    - 如果您使用 X.509 憑證驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 BYOIP 訊息和憑證簽章，以便我們能夠驗證您是否控制公有空間。
    - 如果您使用 DNS TXT 記錄驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 IPAM 驗證符記，以便我們能夠驗證您是否控制公有空間。

    請注意，在將 IPv6 CIDR 配置到頂層集區內的集區時，針對可公開公告的 CIDR，您可以使用的最特定 IPv6 地址範圍是 /48，而針對不可公開公告的 CIDR，則是 /60。

    > **Important**
    >
    > 大多數佈建會在兩個小時內完成，但公開可廣告範圍的佈建過程最多可能需要一週的時間。

12. 將調整此集區的分配規則設定保持在未選取的狀態。
13. (選用) 為集區選擇 Tags (標籤)。
14. 選擇建立集區。

請先確定此 CIDR 已佈建，然後再繼續。您可在集區詳細資訊頁面的 CIDRs (CIDR) 索引標籤中看到佈建狀態。

步驟 2. 在最上層集區內建立一個區域集區

在最上層集區內建立一個區域集區。集區上需有地區設定，且其必須是您在建立 IPAM 時設定的作業區域之一。

此步驟必須由 IPAM 帳戶完成。

在頂層集區內建立一個區域集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。如果不想使用預設的私有範圍，請從內容窗格最上方的下拉式選單中選擇您要使用的範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇建立集區。
5. (選用) 為集區新增 Name tag (名稱標籤) 以及集區的描述。
6. 在 Source (來源) 下，選擇您在上一節建立的頂層集區。
7. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。如需使用此選項規劃 VPC 內子網路 IP 空間的詳細資訊，請參閱 教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
8. 為集區選擇地區設定。選擇地區設定可確保您的集區和從中分配的資源之間沒有跨區域的依賴關係。可用選項來自您在建立 IPAM 時選擇的作業區域。在本教學課程中，我們將會使用 `us-east-2` 作為區域集區的地區設定。

   地區設定是您希望此 IPAM 集區可用於配置 AWS 的區域。例如，您只能從與 VPC 區域共用地區設定的 IPAM 集區為 VPC 配置 CIDR。請注意，當您為集區選擇地區時，您無法對其進行修改。如果 IPAM 的主區域因中斷而無法使用，且集區的地區設定與 IPAM 的主區域不同，則仍然可以使用集區來配置 IP 地址。
9. 在 Service (服務) 下，選擇 EC2 (EIP/VPC)。您選取的服務會決定 CIDR 可公告 AWS 的服務。目前，唯一的選項是 EC2 (EIP/VPC)，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務和 Amazon VPC 服務 (適用於與 VPC 關聯的 CIDR) 進行公告。
10. 在 CIDRs to provision (要佈建的 CIDR) 下，選擇一個要為集區佈建的 CIDR。請注意，在將 IPv6 CIDR 配置到頂層集區內的集區時，針對可公開公告的 CIDR，您可以使用的最特定 IPv6 地址範圍是 /48，而針對不可公開公告的 CIDR，則是 /60。

11. 啟用調整此集區的分配規則設定，並選擇此集區的選擇性分配規則：

    - Automatically import discovered resources (自動匯入探索的資源)：如果 Locale (地區設訂) 已設定為 None (無)，則此選項不可用。如果選取此選項，IPAM 會持續尋找此集區 CIDR 範圍內的資源，並自動將其作為配置匯入 IPAM。注意下列事項：
      - 為這些資源分配的 CIDR 必須尚未分配給其他資源，才能使匯入程序成功。
      - IPAM 會匯入 CIDR，不論其是否符合集區的配置規則，因此可能會匯入資源，隨後再將其標記為不合規。
      - 如果 IPAM 發現多個重疊的 CIDR，IPAM 只會匯入最大的 CIDR。
      - 如果 IPAM 發現多個 CIDR 具有相符的 CIDR，IPAM 將只會隨機匯入其中一個 CIDR。
    - Minimum netmask length (最小網路遮罩長度)：此 IPAM 集區中 CIDR 配置要符合所需的最小網路遮罩長度，以及可從集區配置的最大 CIDR 區塊。最小網路遮罩長度必須小於網路遮罩長度上限。IPv4 地址的可能網路遮罩長度為 `0` - `32`。IPv6 地址的可能網路遮罩長度為 `0` - `128`。
    - Default netmask length (預設網路遮罩長度)：新增至此集區的配置的預設網路遮罩長度。
    - Maximum netmask length (最大網路遮罩長度)：此集區中的 CIDR 配置所需的最大網路遮罩長度。此數值指定可以從集區配置的最小 CIDR 區塊。請確保此值為最小值 **`/48`**。
    - Tagging requirements (標記需求)：資源從集區配置空間所需的標籤。如果資源在配置空間之後變更了其標籤，或在集區上變更了配置標記規則，則資源可能會標示為不合規。
    - Locale (地區設定)：從此集區使用 CIDR 的資源所需的地區設定。沒有此地區設定的自動匯入資源會被標示為不合規。未自動匯入集區的資源將不允許從集區配置空間，除非其位於此地區設定。
12. (選用) 為集區選擇 Tags (標籤)。
13. 當您完成集區的設定後，請選擇 Create pool (建立集區)。

請先確定此 CIDR 已佈建，然後再繼續。您可在集區詳細資訊頁面的 CIDRs (CIDR) 索引標籤中看到佈建狀態。

步驟 3。共用區域集區

遵循本節中的步驟，使用 AWS Resource Access Manager (RAM) 共用 IPAM 集區。

在 中啟用資源共用 AWS RAM

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在您共用 IPAM 集區之前，請完成本節中的步驟，以啟用與 共用資源 AWS RAM。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`management-account`**選項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，在 https：//https://console.aws.amazon.com/ram/ 開啟 AWS RAM 主控台。
2. 在左側導覽窗格中，選擇設定，選擇啟用共用 AWS Organizations，然後選擇儲存設定。

您現在可以與組織的其他成員共用 IPAM 集區。

使用 共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共用區域集區。如需共用 IPAM 集區的完整說明 (包括所需 IAM 許可的相關資訊)，請參閱 透過 AWS RAM 共用 IPAM 集區。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`ipam-account`**選項。

使用 共用 IPAM 集區 AWS RAM

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍，選擇 IPAM 集區，然後選擇 動作 > 檢視詳細資料。
4. 在 Resource sharing (資源共用) 底下，選擇 Create resource share (建立資源共用)。 AWS RAM 主控台隨即開啟。您可以使用 共用集區 AWS RAM。
5. 選擇 Create a resource share (建立資源共用)。
6. 在 AWS RAM 主控台中，再次選擇建立資源共享。
7. 新增共用集區的名稱。
8. 在 選取資源類型 下，選擇 IPAM 集區，然後選擇您要共用的集區 ARN。
9. 選擇下一步。
10. 選擇 AWSRAMPermissionIpamPoolByoipCidrImport 許可。許可選項的詳細資料未涵蓋在本教學課程的範圍，但您可以在 透過 AWS RAM 共用 IPAM 集區 中了解有關這些選項的詳細資訊。
11. 選擇下一步。
12. 在主體 > 選取主體類型下，選擇 AWS 帳戶並輸入要將 IP 地址範圍帶入 IPAM 之帳戶的帳戶 ID，然後選擇新增。
13. 選擇下一步。
14. 檢閱資源共用選項，以及您要與其共用的主體，然後選擇建立。
15. 若要允許 **`member-account`** 帳戶從 IPAM 集區配置 IP 位址 CIDRS，請使用 `AWSRAMDefaultPermissionsIpamPool` 建立第二個資源共用。`--resource-arns` 值為您

在上一節建立之 IPAM 集區的 ARN。`--principals` 的值是 **`member-account`** 的帳戶 ID。`--permission-arns` 值為 `AWSRAMDefaultPermissionsIpamPool` 許可的 ARN。

步驟 4：建立 VPC

完成 Amazon VPC User Guide 的 Create a VPC 中的步驟。

此步驟必須由該成員帳戶完成。

> **Note**
>
> - 當您在 AWS 管理主控台中開啟 VPC 時，您在其中建立 VPC AWS 的區域必須符合您在建立將用於 BYOIP CIDR 的集區時選擇`Locale`的選項。
> - 當您到達為 VPC 選擇 CIDR 的步驟時，您可以選擇從 IPAM 集區使用 CIDR。選擇您在本教學課程中建立的區域集區。

當您建立 VPC 時， 會將 IPAM 集區中的 CIDR AWS 配置到 VPC。您可於 IPAM 主控台的內容窗格中選擇集區，然後檢視集區的 Allocations (分配) 索引標籤，以檢視 IPAM 中的分配。

步驟 5：公告 CIDR

本節中的步驟必須由 IPAM 帳戶完成。建立 VPC 之後，您就可以開始在已設定服務 EC2 (EIP/VPC) 的集區中，公告您帶到 AWS 的 CIDR。在本教學課程中是指您的區域集區。預設情況下不會公告 CIDR，亦即，不能透過網際網路公開存取它。

此步驟必須由 IPAM 帳戶完成。

如要公告 CIDR

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。選擇公有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇您在本教學課程中建立的區域集區。
5. 選擇 CIDRs 索引標籤。
6. 選取 BYOIP CIDR，然後選擇 Actions (動作) > Advertise (公告)。
7. 選擇 Advertise CIDR (公告 CIDR)。

因此，BYOIP CIDR 會進行公告，並將 Advertising (公告) 欄位中的值從 Withdrawn (已撤回) 變更為 Advertised (已公告)。

步驟 6：清除

請依照本節中的步驟清除您在本教學課程中佈建和建立的資源。

步驟 1：從公告中撤回 CIDR

此步驟必須由 IPAM 帳戶完成。

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 根據預設，建立集區時，系統會選取私有範圍。選擇公有範圍。
4. 選擇您在本教學課程中建立的區域集區。
5. 選擇 CIDRs 索引標籤。
6. 選取 BYOIP CIDR，然後選擇 Actions (動作) > Withdraw from advertising (從公告中撤回)。
7. 選擇 Withdraw CIDR (撤回 CIDR)。

因此，BYOIP CIDR 不再進行公告，並將 Advertising (公告) 欄位中的值從 Advertised (已公告) 變更為 Withdrawn (已撤回)。

步驟 2：刪除 VPC

此步驟必須由該成員帳戶完成。

- 完成 Amazon VPC User Guide 的 Delete a VPC 中的步驟，刪除 VPC。當您在 AWS 管理主控台中開啟 VPC 時， AWS 區域從 刪除 VPC 必須符合您在建立將用於 BYOIP CIDR 的集區時選擇`Locale`的選項。在本教學課程中，集區為區域集區。

  刪除 VPC 時，IPAM 需要時間才會發現資源已遭刪除，並將配置給 VPC 的 CIDR 解除分配。在您尚未看到從集區詳細資訊 Allocations (分配) 索引標籤中的集區移除 IPAM 之前，您無法繼續進行清理中的下一步。

步驟 3：刪除 RAM 共用並停用與 AWS Organizations 的 RAM 整合

此步驟必須各自由 IPAM 帳戶和管理帳戶完成。

- 完成 RAM AWS 使用者指南中的刪除 RAM 中的資源共用和停用與 AWS Organizations 的資源共用中的步驟，以刪除 RAM 共用並停用與 AWS Organizations 的 RAM 整合。 AWS

步驟 4：從區域集區和最上層集區解除佈建 CIDR

此步驟必須由 IPAM 帳戶完成。

- 完成 從集區解除佈建 CIDR 中的步驟，依順序從區域集區和最上層集區解除佈建 CIDR。

步驟 5：刪除區域集區和最上層集區

此步驟必須由 IPAM 帳戶完成。

- 完成 刪除集區 中的步驟，依順序刪除區域集區和最上層集區。

僅使用 AWS CLI，自攜 IP CIDR 至 IPAM

將自備 IP (BYOIP) 帶至 IPAM 可讓您在 AWS 中使用組織的現有 IPv4 和 IPv6 地址範圍。這可讓您在您自己的 IP 位址空間下整合內部部署和雲端環境，從而維持一致的品牌、提升網路效能、增強安全性並簡化管理。

請依照下列步驟，僅使用AWS CLI，將 IPv4 或 IPv6 CIDR 帶至 IPAM。

> **Note**
>
> 開始之前，您必須先驗證網域控制。

將 IPv4 地址範圍帶至 AWS 後，您可以使用範圍內的所有 IP 位址，包括第一個地址 (網路地址) 和最後一個地址 (廣播地址)。

目錄

僅使用 CLI 將您自己的公有 IPv4 CIDR AWS 帶到 IPAM

請依照下列步驟，僅使用 AWS CLI，自攜 IPv4 CIDR 至 IPAM，並以 CIDR 分配彈性 IP 地址 (EIP)。

Important

- 此教學課程假設您已完成下列各節中的步驟：
  - 將 IPAM 與 AWS Organizations 中的帳戶整合.
  - 建立 IPAM.
- 本教學課程的每個步驟必須由三個 AWS Organizations 帳戶的其中一個完成：
  - 管理帳戶。
  - 在 將 IPAM 與 AWS Organizations 中的帳戶整合 中設定為您 IPAM 管理員的成員帳戶。在本教學課程中，此帳戶將稱為 IPAM 帳戶。
  - 您組織中的成員帳戶將會從 IPAM 集區分配 CIDR。在本教學課程中，此帳戶將稱為成員帳戶。

目錄

步驟 1：建立 AWS CLI 具名設定檔和 IAM 角色

若要以單一 AWS 使用者身分完成本教學課程，您可以使用 AWS CLI 具名設定檔從一個 IAM 角色切換到另一個角色。具名設定檔是您在搭配 AWS CLI使用 `--profile` 選項時所參考的設定和憑證的集合。如需如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱《》中的使用 IAM 角色 AWS CLI。

為您將在本教學課程中使用的三個 AWS 帳戶各建立一個角色和一個具名設定檔：

- `management-account` 為 AWS Organizations 管理帳戶呼叫的設定檔。
- `ipam-account` 為 AWS Organizations 成員帳戶呼叫的設定檔，設定為您的 IPAM 管理員。
- 您組織中 `member-account` AWS Organizations 成員帳戶的 設定檔，將從 IPAM 集區配置 CIDRs。

建立 IAM 角色和具名設定檔後，請返回此頁面並繼續下一個步驟。在本教學課程的其餘部分，您會注意到範例 AWS CLI 命令使用 `--profile`選項搭配其中一個具名設定檔，以指出哪個帳戶必須執行 命令。

步驟 2：建立 IPAM

此為選擇性步驟。如果已建立 IPAM，其作業區域為 `us-east-1` 和 `us-west-2`，則可略過此步驟。建立 IPAM 並指定作業區域為 `us-east-1` 和 `us-west-2`。必須選取作業區域，才能在建立 IPAM 集區時使用地區設定選項。IPAM 與 BYOIP 整合需要在 BYOIP CIDR 使用的任何集區上設定地區設定。

此步驟必須由 IPAM 帳戶完成。

執行以下命令：

```
aws ec2 create-ipam --description my-ipam --region us-east-1 --operating-
regions RegionName=us-west-2 --profile ipam-account
```

您會在輸出結果中看到您已建立的 IPAM。請記下 `PublicDefaultScopeId` 的值。下一個步驟需使用您的公有範圍 ID。您要使用公有範圍是因為 BYOIP CIDR 是公有 IP 地址，這也是公有範圍的用途。

```
{
 "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-090e48e75758de279",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",
        "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",
        "ScopeCount": 2,
        "Description": "my-ipam",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            },
```

```
            {
                "RegionName": "us-west-2"
            }
        ],
        "Tags": []
    }
}
```

步驟 3：建立最上層 IPAM 集區

完成本節中的步驟來建立最上層 IPAM 集區。

此步驟必須由 IPAM 帳戶完成。

使用 為所有 AWS 資源建立 IPv4 地址集區 AWS CLI

1. 執行下列命令以建立 IPAM 集區。使用您在上一個步驟中建立的 IPAM 公有範圍 ID。

   此步驟必須由 IPAM 帳戶完成。

   ```
   aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-
   scope-0087d83896280b594 --description "top-level-IPv4-pool" --address-family ipv4
    --profile ipam-account
   ```

   您會在輸出結果中看到 create-in-progress，表示正在建立集區。

   ```
   {
       "IpamPool": {
           "OwnerId": "123456789012",
           "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
           "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
   pool-0a03d430ca3f5c035",
           "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
   scope-0087d83896280b594",
           "IpamScopeType": "public",
           "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
           "Locale": "None",
           "PoolDepth": 1,
           "State": "create-in-progress",
           "Description": "top-level-pool",
           "AutoImport": false,
           "AddressFamily": "ipv4",
           "Tags": []
   ```

```
    }
}
```

2. 執行下列命令，直到輸出結果顯示 `create-complete` 的狀態為止。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

下例的輸出結果顯示集區的狀態：

```
{
    "IpamPools": [
        {
            "OwnerId": "123456789012",
            "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
            "IpamScopeType": "public",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
            "Locale": "None",
            "PoolDepth": 1,
            "State": "create-complete",
            "Description": "top-level-IPV4-pool",
            "AutoImport": false,
            "AddressFamily": "ipv4",
            "Tags": []
        }
    ]
}
```

步驟 4：在最上層集區佈建 CIDR

在最上層集區佈建 CIDR 區塊。請注意，在最上層集區內的某集區佈建 IPv4 CIDR 時，您可佈建的最小 IPv4 CIDR 為 /24；不得佈建更明確的 CIDR (例如 /25)。

> **Note**
>
> - 如果您使用 X.509 憑證驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 BYOIP 訊息和憑證簽章，以便我們能夠驗證您是否控制公有空間。

- 如果您使用 DNS TXT 記錄驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 IPAM 驗證符記，以便我們能夠驗證您是否控制公有空間。

只有在最上層集區中佈建 BYOIP CIDR 時才需驗證網域控制。最上層集區內的區域集區可省略網域控制擁有權選項。

此步驟必須由 IPAM 帳戶完成。

> **Important**
>
> 只有在最上層集區中佈建 BYOIP CIDR 時才需驗證網域控制。最上層集區內的區域集區可省略網域控制選項。將 BYOIP 加入至 IPAM 後，如果要將 BYOIP 分割給多個區域與帳戶，就無需再驗證擁有權。

使用 將 CIDR 區塊佈建至集區 AWS CLI

1. 若要使用憑證資訊佈建 CIDR，請使用下列命令範例。除了視需要在範例中替換這些值之外，請確保將 `Message` 和 `Signature` 值替換為您在 使用 X.509 憑證驗證網域 中獲得的 `text_message` 和 `signed_message` 值。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-
pool-id ipam-pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --
verification-method remarks-x509 --cidr-authorization-context
 Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsMaU0P7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRYOdRaNx8yt-uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

   若要使用驗證符記資訊佈建 CIDR，請使用下列命令範例。除了視需要在範例中替換這些值之外，請確保將 `ipam-ext-res-ver-token-0309ce7f67a768cf0` 替換為您在 使用 DNS TXT 記錄驗證網域 中獲得的 `IpamExternalResourceVerificationTokenId` 符記 ID。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --verification-method dns-
```

```
token --ipam-external-resource-verification-token-id ipam-ext-res-ver-
token-0309ce7f67a768cf0 --profile ipam-account
```

輸出結果會顯示 CIDR 的佈建處於待定狀態。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. 請先確定此 CIDR 已佈建，然後再繼續。

> **Important**
>
> 大多數佈建會在兩個小時內完成，但公開可廣告範圍的佈建過程最多可能需要一週的時間。

執行下列命令，直到輸出結果顯示 `provisioned` 的狀態為止。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

下例的輸出結果即顯示狀態。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

步驟 5：在最上層集區內建立一個區域集區。

在最上層集區內建立一個區域集區。

集區的地區設定應是下列其中一項：

- 您希望此 IPAM 集區可用於配置 AWS 的區域。
- 您希望此 IPAM 集區可用於配置的 AWS Local Zone 的網路邊界群組 (支援的 Local Zones)。此選項僅適用於公有範圍內的 IPAM IPv4 集區。
- AWS 專用本地區域。若要在 AWS 專用本機區域中建立集區，請在選取器輸入中輸入 AWS 專用本機區域。
- `Global` 當您想要在所有 AWS 區域全域使用 IP 地址時，例如 CloudFront 位置。`Global` 地區設定僅適用於公有 IPv4 集區。

例如，您只能從與 VPC 區域共用地區設定的 IPAM 集區為 VPC 配置 CIDR。請注意，當您為集區選擇地區時，您無法對其進行修改。如果 IPAM 的主區域因中斷而無法使用，且集區的地區設定與 IPAM 的主區域不同，則仍然可以使用集區來配置 IP 位址。

當您執行本節中的命令時，`--region` 的值必須包含您在建立 BYOIP CIDR 即將使用的集區時所輸入的 `--locale` 選項。例如，如果您使用 us-east-1 作為地區設定建立了 BYOIP 集區，則 `--region` 應為 us-east-1。如果您使用 us-east-1-scl-1 作為地區設定建立了 BYOIP 集區 (該地區為本地區域的網路邊界群組)，則 `--region` 應為 us-east-1，因為該區域會管理 us-east-1-scl-1 這一地區設定。

此步驟必須由 IPAM 帳戶完成。

選擇地區設定可確保您的集區和從中分配的資源之間沒有跨區域的依賴關係。可用選項來自您在建立 IPAM 時選擇的作業區域。在本教學課程中，我們將會使用 `us-west-2` 作為區域集區的地區設定。

> **Important**
>
> 建立集區時，必須包含 `--aws-service ec2`。您選取的服務會決定 CIDR 可公告 AWS 的服務。目前，唯一的選項是 `ec2`，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務 (適用於彈性 IP 地址) 和 Amazon VPC 服務 (適用於與 VPC 關聯的 CIDR) 進行公告。

使用 建立區域集區 AWS CLI

1. 執行下列命令以建立集區。

```
aws ec2 create-ipam-pool --description "Regional-IPv4-pool" --region us-east-1
 --ipam-scope-id ipam-scope-0087d83896280b594 --source-ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --locale us-west-2 --address-family ipv4 --aws-service ec2
 --profile ipam-account
```

您會在輸出結果中看到 IPAM 建立了集區。

```
{
     "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
        "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0d8f3646b61ca5987",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-west-2",
        "PoolDepth": 2,
        "State": "create-in-progress",
        "Description": "Regional--pool",
        "AutoImport": false,
        "AddressFamily": "ipv4",
        "Tags": [],
        "ServiceType": "ec2"
    }
}
```

2. 執行下列命令，直到輸出結果顯示 `create-complete` 的狀態為止。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

您會在輸出結果中看到 IPAM 內的集區。在本教學課程中，我們建立了最上層和區域集區，所以這兩種集區您都會看到。

步驟 6：在區域集區中佈建 CIDR

在區域集區中佈建 CIDR 區塊。

> **Note**
>
> 在最上層集區內的某集區佈建 CIDR 時，您可佈建的最具體的 IPv4 CIDR 為 /24；不得佈建更具體的 CIDR (例如 /25)。建立區域集區後，您可以在同一區域集區內建立更小的集區 (例如 /25)。請注意，如果您共用區域集區或其中的集區，這些集區只能在相同區域集區的區域設定中使用。

此步驟必須由 IPAM 帳戶完成。

使用 將 CIDR 區塊指派給區域集區 AWS CLI

1. 執行下列命令以佈建 CIDR。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --cidr 130.137.245.0/24 --profile ipam-account
```

   輸出結果會顯示 CIDR 的佈建處於待定狀態。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. 執行下列命令，直到輸出結果顯示 provisioned 的狀態為止。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   下例的輸出結果顯示正確狀態。

```
{
    "IpamPoolCidrs": [
        {
```

```
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

步驟 7：公告 CIDR

本節中的步驟必須由 IPAM 帳戶完成。將彈性 IP 地址 (EIP) 與執行個體或 Elastic Load Balancer 建立關聯後，您就可以開始公告您帶到 AWS 已定義集區中的 CIDR。在本教學課程中是指您的區域集區。預設情況下不會公告 CIDR，亦即，不能透過網際網路公開存取它。當您執行本節中的命令時，`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所輸入的 `--locale` 選項相符。`--aws-service ec2`

此步驟必須由 IPAM 帳戶完成。

> **Note**
>
> 廣告狀態不會限制您配置彈性 IP 位址的能力。即使您的 BYOIPv4 CIDR 沒有公告，您仍然可以從 IPAM 集區建立 EIP。

使用 開始公告 CIDR AWS CLI

- 執行下列命令以公告 CIDR。

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
profile ipam-account
```

您會在輸出結果中看到 CIDR 已公告。

```
{
    "ByoipCidr": {
        "Cidr": "130.137.245.0/24",
        "State": "advertised"
    }
}
```

第 8 步：共用區域集區

遵循本節中的步驟，使用 AWS Resource Access Manager (RAM) 共用 IPAM 集區。

在 中啟用資源共用 AWS RAM

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在您共用 IPAM 集區之前，請完成本節中的步驟，以啟用與 共用資源 AWS RAM。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`management-account`**選項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，在 https：//https://console.aws.amazon.com/ram/ 開啟 AWS RAM 主控台。
2. 在左側導覽窗格中，選擇設定，選擇啟用共用 AWS Organizations，然後選擇儲存設定。

您現在可以與組織的其他成員共用 IPAM 集區。

使用 共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共用區域集區。如需共用 IPAM 集區的完整說明 (包括所需 IAM 許可的相關資訊)，請參閱 透過 AWS RAM 共用 IPAM 集區。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`ipam-account`**選項。

使用 共用 IPAM 集區 AWS RAM

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍，選擇 IPAM 集區，然後選擇 動作 > 檢視詳細資料。
4. 在 Resource sharing (資源共用) 底下，選擇 Create resource share (建立資源共用)。 AWS RAM 主控台隨即開啟。您可以使用 共用集區 AWS RAM。
5. 選擇 Create a resource share (建立資源共用)。
6. 在 AWS RAM 主控台中，再次選擇建立資源共享。
7. 新增共用集區的名稱。
8. 在 選取資源類型 下，選擇 IPAM 集區，然後選擇您要共用的集區 ARN。
9. 選擇下一步。
10. 選擇 AWSRAMPermissionIpamPoolByoipCidrImport 許可。許可選項的詳細資料未涵蓋在本教學課程的範圍，但您可以在 透過 AWS RAM 共用 IPAM 集區 中了解有關這些選項的詳細資訊。

11. 選擇下一步。
12. 在主體 > 選取主體類型下，選擇 AWS 帳戶並輸入要將 IP 地址範圍帶入 IPAM 之帳戶的帳戶 ID，然後選擇新增。
13. 選擇下一步。
14. 檢閱資源共用選項，以及您要與其共用的主體，然後選擇建立。
15. 若要允許 **member-account** 帳戶從 IPAM 集區配置 IP 位址 CIDRS，請使用 `AWSRAMDefaultPermissionsIpamPool` 建立第二個資源共用。`--resource-arns` 值為您在上一節建立之 IPAM 集區的 ARN。`--principals` 的值是 **member-account** 的帳戶 ID。`--permission-arns` 值為 `AWSRAMDefaultPermissionsIpamPool` 許可的 ARN。

第 9 步：從集區配置彈性 IP 位址

按照本節中的步驟，從集區配置彈性 IP 位址。請注意，如果您使用公有 IPv4 集區來配置彈性 IP 位址，您可以使用 第 9 步的替代方案 中的替代步驟，而非本節中的步驟。

> **Important**
>
> 如果您看到與沒有呼叫 ec2：AllocateAddress 相關的錯誤，則需要更新目前指派給與您共用的 IPAM 集區的受管許可。聯絡建立資源共用的人員，並要求他們將受管許可 `AWSRAMPermissionIpamResourceDiscovery` 更新為預設版本。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的更新資源共用。

AWS Management Console

請依照《Amazon EC2 使用者指南》中的配置彈性 IP 位址中的步驟配置地址，但請注意下列事項：

- 此步驟必須由該成員帳戶完成。
- 請確定您在 EC2 主控台中的 AWS 區域與您在建立區域集區時選擇的區域設定選項相符。
- 選擇地址集區時，請選擇使用 IPv4 IPAM 集區配置的選項，然後選擇您建立的區域集區。

Command line

使用 allocate-address 命令從集區配置地址。您使用的 `--region` 必須與您在步驟 2 中建立集區時所選擇的 `-locale` 選項相符。在 `--ipam-pool-id` 中包含您在第 2 步中建立的 IPAM 集區的 ID。您也可以選擇 IPAM 集區中的特定 `/32`，方法是使用 `--address` 選項。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

回應範例：

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的配置彈性 IP 位址。

第 10 步：建立彈性 IP 位址與 EC2 執行個體的關聯

完成本節中的步驟，建立彈性 IP 位址與 EC2 執行個體的關聯。

AWS Management Console

請遵循《Amazon EC2 使用者指南》中的關聯彈性 IP 地址的步驟，從 IPAM 集區配置彈性 IP 地址，但請注意下列事項：當您使用 AWS 管理主控台選項時，您在 中關聯彈性 IP 地址 AWS 的區域必須符合您在建立區域集區時選擇的區域設定選項。

此步驟必須由該成員帳戶完成。

Command line

此步驟必須由該成員帳戶完成。設定 `--profile` **`member-account`** 選項。

使用 associate-address 命令，建立彈性 IP 位址與 Outpost 執行個體的關聯。您在 `--region` 中關聯彈性 IP 位址的 `--locale` 選項必須與您創建區域集區時選擇的選項相符。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

回應範例：

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
```

```
}
```

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的將彈性 IP 位址與執行中的執行個體或網路介面建立關聯。

步驟 11：清除

請依照本節中的步驟清除您在本教學課程中佈建和建立的資源。當您執行本節中的命令時，`--region` 的值必須包含您在建立 BYOIP CIDR 即將使用的集區時所輸入的 `--locale` 選項。

使用 清除 AWS CLI

1. 檢視管理於 IPAM 中的 EIP 分配。

   此步驟必須由 IPAM 帳戶完成。

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   該輸出結果會顯示 IPAM 中的分配情況。

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "130.137.245.0/24",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
               "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
               "ResourceType": "ec2-public-ipv4-pool",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

2. 停止公告 IPv4 CIDR。

   此步驟必須由 IPAM 帳戶完成。

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
   profile ipam-account
   ```

您會在輸出結果中看到 CIDR 狀態從 advertised (已公告) 變成 provisioned (已佈建)。

```
{
    "ByoipCidr": {
        "Cidr": "130.137.245.0/24",
        "State": "provisioned"
    }
}
```

3. 釋出彈性 IP 地址。

   此步驟必須由該成員帳戶完成。

   ```
   aws ec2 release-address --region us-west-2 --allocation-
   id eipalloc-0db3405026756dbf6 --profile member-account
   ```

   當您執行此命令時，將不會看到任何輸出結果。

4. 檢視不再以 IPAM 進行管理的 EIP 分配。IPAM 可能需要一段時間才能發現彈性 IP 地址已遭移除。您無法繼續清除和解除佈建 IPAM 集區的 CIDR，直到您發現配置已從 IPAM 移除為止。當您執行本節中的命令時，`--region` 的值必須包含您在建立 BYOIP CIDR 即將使用的集區時所輸入的 `--locale` 選項。

   此步驟必須由 IPAM 帳戶完成。

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   該輸出結果會顯示 IPAM 中的分配情況。

   ```
   {
       "IpamPoolAllocations": []
   }
   ```

5. 解除佈建區域集區 CIDR。當您執行本步驟中的命令時，`--region` 的值必須與 IPAM 的區域相符。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --cidr 130.137.245.0/24 --profile ipam-account
```

輸出結果會顯示 CIDR 的解除佈建處於待定狀態。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }

}
```

解除佈建需要一段時間才能完成。檢查解除佈建狀態。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

請等到狀態變成 deprovisioned (已解除佈建) 後，再繼續進行下一個步驟。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

6. 刪除 RAM 共用並停用與 AWS Organizations 整合的 RAM。完成 RAM AWS 使用者指南中的刪除 RAM 中的資源共用和停用與 AWS Organizations 的資源共用中的步驟，以刪除 RAM 共用並停用與 AWS Organizations 的 RAM 整合。 AWS

   此步驟必須各自由 IPAM 帳戶和管理帳戶完成。如果您使用 AWS CLI 刪除 RAM 共用並停用 RAM 整合，請使用 `--profile ipam-account`和 `--profile management-account`選項。

7. 刪除區域集區。當您執行本步驟中的命令時，--region 的值必須與 IPAM 的區域相符。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   您可在輸出結果中看到刪除狀態。

```
{
   "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
        "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0d8f3646b61ca5987",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "reg-ipv4-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

8. 解除佈建最上層集區 CIDR。當您執行本步驟中的命令時，--region 的值必須與 IPAM 的區域相符。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --profile ipam-account
```

   輸出結果會顯示 CIDR 的解除佈建處於待定狀態。

```
{
```

```
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }

}
```

解除佈建需要一段時間才能完成。執行下列命令以檢查解除佈建的狀態。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

請等到狀態變成 deprovisioned (已解除佈建) 後，再繼續進行下一個步驟。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. 刪除上層集區。當您執行本步驟中的命令時，--region 的值必須與 IPAM 的區域相符。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

您可在輸出結果中看到刪除狀態。

```
{
  "IpamPool": {
        "OwnerId": "123456789012",
```

```
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

10. 刪除 IPAM。當您執行本步驟中的命令時，`--region` 的值必須與 IPAM 的區域相符。

    此步驟必須由 IPAM 帳戶完成。

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    您會在輸出結果中看到 IPAM 回應。這表示 IPAM 已刪除。

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-090e48e75758de279",

        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",

        "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",

        "ScopeCount": 2,

        "OperatingRegions": [

            {
```

```
                "RegionName": "us-east-1"

            },
            {
                "RegionName": "us-west-2"
            }
        ],
    }
}
```

第 9 步的替代方案

如果您使用公有 IPv4 集區來配置彈性 IP 位址，您可以使用本節中的步驟，而非 第 9 步：從集區配置彈性 IP 位址 中的步驟。

目錄

第 1 步：建立公有 IPv4 集區

此步驟通常由想要佈建彈性 IP 地址的不同 AWS 帳戶完成，例如成員帳戶。

> **Important**
>
> 公有 IPv4 集區和 IPAM 集區由 中的不同資源管理 AWS。公有 IPv4 集區是單一帳戶資源，可讓您將公有的 CIDR 轉換為彈性 IP 地址。使用 IPAM 集區可將公有空間配置給公有 IPv4 集區。

使用 建立公有 IPv4 集區 AWS CLI

- 執行下列命令以佈建 CIDR。當您執行本節中的命令時，`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所輸入的 `--locale` 選項相符。

```
aws ec2 create-public-ipv4-pool --region us-west-2 --profile member-account
```

您會在輸出結果中看到公有 IPv4 集區 ID。下一個步驟需要用到此 ID。

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2"
}
```

第 2 步：在公有 IPv4 集區佈建公有 IPv4 CIDR

在公有 IPv4 集區中佈建公有 IPv4 CIDR。`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所輸入的 `--locale` 值相符。您可以定義的最不具體的 `--netmask-length` 是 24。

此步驟必須由該成員帳戶完成。

使用 建立公有 IPv4 集區 AWS CLI

1. 執行下列命令以佈建 CIDR。

```
aws ec2 provision-public-ipv4-pool-cidr --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --netmask-length 24
 --profile member-account
```

輸出結果會顯示已佈建的 CIDR。

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. 執行下列命令以檢視公有 IPv4 集區中佈建的 CIDR。

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-
account
```

輸出結果會顯示已佈建的 CIDR。預設情況下不會公告 CIDR，亦即，不能透過網際網路公開存取它。透過本教學課程的最後一個步驟可設定此 CIDR，使其公告在網路上。

```
{
    "ByoipCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "StatusMessage": "Cidr successfully provisioned",
            "State": "provisioned"
        }
    ]
}
```

第 3 步：在公有 IPv4 集區中建立彈性 IP 位址

在公有 IPv4 集區中建立彈性 IP 地址 (EIP)。當您執行本節中的命令時，`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所輸入的 `--locale` 選項相符。

此步驟必須由該成員帳戶完成。

使用 從公有 IPv4 集區建立 EIP AWS CLI

1. 執行下列命令以建立 EIP。

```
aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
ec2-0019eed22a684e0b2 --profile member-account
```

您會在輸出結果中看到配置。

```
{
    "PublicIp": "130.137.245.100",
    "AllocationId": "eipalloc-0db3405026756dbf6",
    "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

2. 執行下列命令以檢視透過 IPAM 進行管理的 EIP 配置。

此步驟必須由 IPAM 帳戶完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

該輸出結果會顯示 IPAM 中的分配情況。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

第 9 步清除的替代方案

請完成下列步驟，以清除使用第 9 步的替代方案建立的公有 IPv4 集區。您應該在 步驟 10：清除 中的標準清除程序期間釋出彈性 IP 位址之後，完成這些步驟。

1. 檢視您的 BYOIP CIDR。

   此步驟必須由該成員帳戶完成。

```
aws ec2 describe-public-ipv4-pools --region us-west-2 --profile member-account
```

   輸出結果會顯示 BYOIP CIDR 中的 IP 地址。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
            "Description": "",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
```

```
                    "AddressCount": 256,
                    "AvailableAddressCount": 256
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 256,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

2. 釋出公有 IPv4 集區的 CIDR。當您執行本節中的命令時，`--region` 的值必須與 IPAM 的區域相符。

   此步驟必須由該成員帳戶完成。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.0/24 --profile member-account
```

3. 再次檢視您的 BYOIP CIDR，並確保其中不再有已佈建的地址。當您執行本節中的命令時，`--region` 的值必須與 IPAM 的區域相符。

   此步驟必須由該成員帳戶完成。

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
```

   您會在輸出結果的公有 IPv4 集區中看到 IP 地址計數。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

僅使用 CLI 將您自己的 IPv6 CIDR AWS 帶到 IPAM

請依照下列步驟，僅使用 AWS CLI，自攜 IPv6 CIDR 至 IPAM，並分配 VPC。

如果您不需要透過網際網路公告 IPv6 地址，則可以將私有 GUA IPv6 地址佈建至 IPAM。如需詳細資訊，請參閱啟用佈建私有 IPv6 GUA CIDR。

Important

- 此教學課程假設您已完成下列各節中的步驟：
  - 將 IPAM 與 AWS Organizations 中的帳戶整合.
  - 建立 IPAM.
- 本教學課程的每個步驟必須由三個 AWS Organizations 帳戶的其中一個完成：
  - 管理帳戶。
  - 在 將 IPAM 與 AWS Organizations 中的帳戶整合 中設定為您 IPAM 管理員的成員帳戶。在本教學課程中，此帳戶將稱為 IPAM 帳戶。
  - 您組織中的成員帳戶將會從 IPAM 集區分配 CIDR。在本教學課程中，此帳戶將稱為成員帳戶。

目錄

步驟 1：建立 AWS CLI 具名設定檔和 IAM 角色

若要以單一 AWS 使用者身分完成本教學課程，您可以使用 AWS CLI 具名設定檔從一個 IAM 角色切換到另一個角色。具名設定檔是您在搭配 AWS CLI使用 `--profile` 選項時所參考的設定和憑證的集合。如需如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱《》中的使用 IAM 角色 AWS CLI。

為您將在本教學課程中使用的三個 AWS 帳戶各建立一個角色和一個具名設定檔：

- `management-account` 為 AWS Organizations 管理帳戶呼叫的設定檔。
- `ipam-account` 為 AWS Organizations 成員帳戶呼叫的設定檔，設定為您的 IPAM 管理員。
- 您組織中 `member-account` AWS Organizations 成員帳戶的 設定檔，將從 IPAM 集區配置 CIDRs。

建立 IAM 角色和具名設定檔後，請返回此頁面並繼續下一個步驟。在本教學課程的其餘部分，您會注意到範例 AWS CLI 命令使用 `--profile`選項搭配其中一個具名設定檔，以指出哪個帳戶必須執行 命令。

步驟 2：建立 IPAM

此為選擇性步驟。如果已建立 IPAM，其作業區域為 `us-east-1` 和 `us-west-2`，則可略過此步驟。建立 IPAM 並指定作業區域為 `us-east-1` 和 `us-west-2`。必須選取作業區域，才能在建立 IPAM 集區時使用地區設定選項。IPAM 與 BYOIP 整合需要在 BYOIP CIDR 使用的任何集區上設定地區設定。

此步驟必須由 IPAM 帳戶完成。

執行以下命令：

```
aws ec2 create-ipam --description my-ipam --region us-east-1 --operating-
regions RegionName=us-west-2 --profile ipam-account
```

您會在輸出結果中看到您已建立的 IPAM。請記下 `PublicDefaultScopeId` 的值。下一個步驟需使用您的公有範圍 ID。

```
{
 "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-090e48e75758de279",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",
```

```
        "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",
        "ScopeCount": 2,
        "Description": "my-ipam",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            },
            {
                "RegionName": "us-west-2"
            }
        ],
        "Tags": []
    }
}
```

步驟 3：建立 IPAM 集區

由於您要建立內含區域集區的最上層 IPAM 集區，而且我們要從區域集區配置空間給資源 (VPC)，因此您必須在區域集區 (而不是最上層集區) 上設定地區設定。在稍後的步驟中建立區域集區時，您會新增區域集區的地區設定。IPAM 與 BYOIP 整合需要在 BYOIP CIDR 使用的任何集區上設定地區設定。

此步驟必須由 IPAM 帳戶完成。

如果您希望 AWS 透過公有網際網路 (`--publicly-advertisable` 或) 公告此 IPAM 集區 CIDR，請選擇 `--no-publicly-advertisable`。

> **Note**
>
> 請注意，範圍 ID 需為公有範圍的 ID，且地址系列需為 `ipv6`。

使用 為所有 AWS 資源建立 IPv6 地址集區 AWS CLI

1. 執行下列命令以建立 IPAM 集區。使用您在上一個步驟中建立的 IPAM 公有範圍 ID。

   ```
   aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-
   scope-0087d83896280b594 --description "top-level-IPv6-pool" --address-
   family ipv6 --publicly-advertisable --profile ipam-account
   ```

   您會在輸出結果中看到 `create-in-progress`，表示正在建立集區。

   ```
   {
   ```

```
    "IpamPool": {

        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-07f2466c7158b50c4",

        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-07f2466c7158b50c4",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",

        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",

        "Locale": "None",

        "PoolDepth": 1,

        "State": "create-in-progress",

        "Description": "top-level-Ipv6-pool",

        "AutoImport": false,

        "Advertisable": true,

        "AddressFamily": "ipv6",

        "Tags": []

    }

}
```

2. 執行下列命令，直到輸出結果顯示 `create-complete` 的狀態為止。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

下例的輸出結果顯示集區的狀態：

```
{
    "IpamPool": {

        "OwnerId": "123456789012",
```

```
        "IpamPoolId": "ipam-pool-07f2466c7158b50c4",

        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-07f2466c7158b50c4",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",

        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",

        "Locale": "None",

        "PoolDepth": 1,

        "State": "create-complete",

        "Description": "top-level-Ipv6-pool",

        "AutoImport": false,

        "Advertisable": true,

        "AddressFamily": "ipv6",

        "Tags": []

    }

}
```

步驟 4：在最上層集區佈建 CIDR

在最上層集區佈建 CIDR 區塊。請注意，在將 IPv6 CIDR 配置到頂層集區內的集區時，針對可公開公告的 CIDR，您可以使用的最特定 IPv6 地址範圍是 /48，而針對不可公開公告的 CIDR，則是 /60。

> **Note**
>
> - 如果您使用 X.509 憑證驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 BYOIP 訊息和憑證簽章，以便我們能夠驗證您是否控制公有空間。

- 如果您使用 DNS TXT 記錄驗證網域控制，則必須包含在該步驟中建立的 CIDR 和 IPAM 驗證符記，以便我們能夠驗證您是否控制公有空間。

只有在最上層集區中佈建 BYOIP CIDR 時才需驗證網域控制。最上層集區內的區域集區可省略網域控制擁有權選項。

此步驟必須由 IPAM 帳戶完成。

使用 將 CIDR 區塊佈建至集區 AWS CLI

1. 若要使用憑證資訊佈建 CIDR，請使用下列命令範例。除了視需要在範例中替換這些值之外，請確保將 `Message` 和 `Signature` 值替換為您在 使用 X.509 憑證驗證網域 中獲得的 `text_message` 和 `signed_message` 值。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-
x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|
20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

若要使用驗證符記資訊佈建 CIDR，請使用下列命令範例。除了視需要在範例中替換這些值之外，請確保將 `ipam-ext-res-ver-token-0309ce7f67a768cf0` 替換為您在 使用 DNS TXT 記錄驗證網域 中獲得的 `IpamExternalResourceVerificationTokenId` 符記 ID。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method
 dns-token --ipam-external-resource-verification-token-id ipam-ext-res-ver-
token-0309ce7f67a768cf0 --profile ipam-account
```

輸出結果會顯示 CIDR 的佈建處於待定狀態。

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",
```

```
        "State": "pending-provision"

    }

}
```

2. 請先確定此 CIDR 已佈建，然後再繼續。

> **Important**
>
> 大多數佈建會在兩個小時內完成，但公開可廣告範圍的佈建過程最多可能需要一週的時間。

執行下列命令，直到輸出結果顯示 `provisioned` 的狀態為止。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

下例的輸出結果即顯示狀態。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

步驟 5：在最上層集區內建立一個區域集區。

在最上層集區內建立一個區域集區。集區上需有 `--locale`，且其必須是您在建立 IPAM 時設定的作業區域之一。

此步驟必須由 IPAM 帳戶完成。

> **Important**
>
> 建立集區時，必須包含 `--aws-service ec2`。您選取的服務會決定 CIDR 可公告 AWS 的服務。目前，唯一的選項是 `ec2`，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務和 Amazon VPC 服務 (適用於與 VPC 關聯的 CIDR) 進行公告。

使用 建立區域集區 AWS CLI

1. 執行下列命令以建立集區。

```
aws ec2 create-ipam-pool --description "Regional-IPv6-pool" --region us-east-1
 --ipam-scope-id ipam-scope-0087d83896280b594 --source-ipam-pool-id ipam-
pool-07f2466c7158b50c4 --locale us-west-2 --address-family ipv6 --aws-service ec2
 --profile ipam-account
```

   您會在輸出結果中看到 IPAM 建立了集區。

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0053b7d2b4fc3f730",
        "SourceIpamPoolId": "ipam-pool-07f2466c7158b50c4",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0053b7d2b4fc3f730",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-west-2",
        "PoolDepth": 2,
        "State": "create-in-progress",
        "Description": "reg-ipv6-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv6",
        "Tags": [],
        "ServiceType": "ec2"
    }
}
```

2. 執行下列命令，直到輸出結果顯示 create-complete 的狀態為止。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

您會在輸出結果中看到 IPAM 內的集區。在本教學課程中，我們建立了最上層和區域集區，所以這兩種集區您都會看到。

步驟 6：在區域集區中佈建 CIDR

在區域集區中佈建 CIDR 區塊。請注意，在將 CIDR 配置到頂層集區內的集區時，針對可公開公告的 CIDR，您可以使用的最特定 IPv6 地址範圍是 /48，而針對不可公開公告的 CIDR，則是 /60。

此步驟必須由 IPAM 帳戶完成。

使用 將 CIDR 區塊指派給區域集區 AWS CLI

1. 執行下列命令以佈建 CIDR。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

輸出結果會顯示 CIDR 的佈建處於待定狀態。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
}
```

2. 執行下列命令，直到輸出結果顯示 provisioned 的狀態為止。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

下例的輸出結果顯示正確狀態。

```
{
    "IpamPoolCidrs": [
        {
```

```
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

步驟 7. 共用區域集區

遵循本節中的步驟，使用 AWS Resource Access Manager (RAM) 共用 IPAM 集區。

在 中啟用資源共用 AWS RAM

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在您共用 IPAM 集區之前，請完成本節中的步驟，以啟用與 共用資源 AWS RAM。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`management-account`**選項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，在 https：//https://console.aws.amazon.com/ram/ 開啟 AWS RAM 主控台。
2. 在左側導覽窗格中，選擇設定，選擇啟用共用 AWS Organizations，然後選擇儲存設定。

您現在可以與組織的其他成員共用 IPAM 集區。

使用 共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共用區域集區。如需共用 IPAM 集區的完整說明 (包括所需 IAM 許可的相關資訊)，請參閱 透過 AWS RAM 共用 IPAM 集區。如果您使用 AWS CLI 來啟用資源共用，請使用 `--profile` **`ipam-account`**選項。

使用 共用 IPAM 集區 AWS RAM

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍，選擇 IPAM 集區，然後選擇 動作 > 檢視詳細資料。
4. 在 Resource sharing (資源共用) 底下，選擇 Create resource share (建立資源共用)。 AWS RAM 主控台隨即開啟。您可以使用 共用集區 AWS RAM。
5. 選擇 Create a resource share (建立資源共用)。
6. 在 AWS RAM 主控台中，再次選擇建立資源共享。

7. 新增共用集區的名稱。
8. 在 選取資源類型 下，選擇 IPAM 集區，然後選擇您要共用的集區 ARN。
9. 選擇下一步。
10. 選擇 AWSRAMPermissionIpamPoolByoipCidrImport 許可。許可選項的詳細資料未涵蓋在本教學課程的範圍，但您可以在 透過 AWS RAM 共用 IPAM 集區 中了解有關這些選項的詳細資訊。
11. 選擇下一步。
12. 在主體 > 選取主體類型下，選擇 AWS 帳戶並輸入要將 IP 地址範圍帶入 IPAM 之帳戶的帳戶 ID，然後選擇新增。
13. 選擇下一步。
14. 檢閱資源共用選項，以及您要與其共用的主體，然後選擇建立。
15. 若要允許 **member-account** 帳戶從 IPAM 集區配置 IP 位址 CIDRS，請使用 AWSRAMDefaultPermissionsIpamPool 建立第二個資源共用。--resource-arns 值為您在上一節建立之 IPAM 集區的 ARN。--principals 的值是 **member-account** 的帳戶 ID。--permission-arns 值為 AWSRAMDefaultPermissionsIpamPool 許可的 ARN。

步驟 8：使用 IPv6 CIDR 建立 VPC

使用 IPAM 集區 ID 建立 VPC。同時還必須使用 --cidr-block 選項使 IPv4 CIDR 區塊與 VPC 產生關聯，否則請求會失敗。當您執行本節中的命令時，--region 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所輸入的 --locale 選項相符。

此步驟必須由該成員帳戶完成。

使用 建立具有 IPv6 CIDR 的 VPC AWS CLI

1. 執行下列命令以佈建 CIDR。

```
aws ec2 create-vpc --region us-west-2 --ipv6-ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr-block 10.0.0.0/16 --ipv6-netmask-length 56 --
profile member-account
```

您會在輸出結果中看到建立的 VPC。

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-2afccf50",
```

```
        "State": "pending",
        "VpcId": "vpc-00b5573ffc3b31a29",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-01b5703d6cc695b5b",
                "Ipv6CidrBlock": "2605:9cc0:409::/56",
                "Ipv6CidrBlockState": {
                    "State": "associating"
                },
                "NetworkBorderGroup": "us-east-1",
                "Ipv6Pool": "ipam-pool-0053b7d2b4fc3f730"
            }
        ],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-09cccb07d4e9a0e0e",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false
    }
}
```

2. 檢視 IPAM 中的 VPC 配置。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

您會在輸出結果中看到 IPAM 內的配置。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
```

```
            "ResourceOwner": "123456789012"
        }
    ]
}
```

步驟 9：公告 CIDR

使用 IPAM 中配置的 CIDR 建立 VPC 之後，您就可以開始公告您帶到的 CIDR AWS ，該 CIDR 位於已--aws-service ec2定義的集區中。在本教學課程中是指您的區域集區。預設情況下不會公告 CIDR，亦即，不能透過網際網路公開存取它。當您執行本節中的命令時，--region 的值必須與您在建立 BYOIP CIDR 即將使用的區域集區時所輸入的 --locale 選項相符。

此步驟必須由 IPAM 帳戶完成。

使用 開始公告 CIDR AWS CLI

- 執行下列命令以公告 CIDR。

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

您會在輸出結果中看到 CIDR 已公告。

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "advertised"
    }
}
```

步驟 10：清除

請依照本節中的步驟清除您在本教學課程中佈建和建立的資源。當您執行本節中的命令時，--region 的值必須與您在建立 BYOIP CIDR 即將使用的區域集區時所輸入的 --locale 選項相符。

使用 清除 AWS CLI

1. 執行下列命令以檢視透過 IPAM 進行管理的 VPC 配置。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

該輸出結果會顯示 IPAM 中的分配情況。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

2. 執行下列命令以停止公告 CIDR。當您執行本步驟中的命令時，--region 的值必須與您在建立 BYOIP CIDR 即將使用的區域集區時所輸入的 --locale 選項相符。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

   您會在輸出結果中看到 CIDR 狀態從 advertised (已公告) 變成 provisioned (已佈建)。

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "provisioned"
    }
}
```

3. 執行下列命令以刪除 VPC。當您執行本節中的命令時，--region 的值必須與您在建立 BYOIP CIDR 即將使用的區域集區時所輸入的 --locale 選項相符。

   此步驟必須由該成員帳戶完成。

```
aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
profile member-account
```

當您執行此命令時，將不會看到任何輸出結果。

4. 執行下列命令以檢視透過 IPAM 中的 VPC 配置。IPAM 可能需要一段時間才會發現 VPC 已遭刪除並移除此配置。當您執行本節中的命令時，`--region` 的值必須與您在建立 BYOIP CIDR 即將使用的區域集區時所輸入的 `--locale` 選項相符。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   該輸出結果會顯示 IPAM 中的分配情況。

```
{
   "IpamPoolAllocations": [

        {

            "Cidr": "2605:9cc0:409::/56",

            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",

            "ResourceType": "vpc",

            "ResourceOwner": "123456789012"

        }

    ]

}
```

   重新執行命令並尋找要移除的配置。您無法繼續清除和解除佈建 IPAM 集區的 CIDR，直到您發現配置已從 IPAM 移除為止。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

輸出結果會顯示該配置已從 IPAM 中刪除。

```
{
    "IpamPoolAllocations": []
}
```

5. 刪除 RAM 共用並停用與 AWS Organizations 整合的 RAM。完成 RAM AWS 使用者指南中的刪除 RAM 中的資源共用和停用與 AWS Organizations 的資源共用中的步驟，以刪除 RAM 共用並停用與 AWS Organizations 的 RAM 整合。 AWS

   此步驟必須各自由 IPAM 帳戶和管理帳戶完成。如果您使用 AWS CLI 刪除 RAM 共用並停用 RAM 整合，請使用 `--profile ipam-account`和 `--profile management-account`選項。

6. 執行下列命令以解除佈建區域集區的 CIDR。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   輸出結果會顯示 CIDR 的解除佈建處於待定狀態。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   解除佈建需要一段時間才能完成。繼續執行命令，直到 CIDR 狀態變成 deprovisioned (已解除佈建) 為止。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   輸出結果會顯示 CIDR 的解除佈建處於待定狀態。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "deprovisioned"
    }
}
```

7. 執行下列命令以刪除區域集區。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   您可在輸出結果中看到刪除狀態。

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0053b7d2b4fc3f730",
        "SourceIpamPoolId": "ipam-pool-07f2466c7158b50c4",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0053b7d2b4fc3f730",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "reg-ipv6-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv6"
    }
}
```

8. 執行下列命令以解除佈建最上層集區的 CIDR。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

輸出結果會顯示 CIDR 的解除佈建處於待定狀態。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

解除佈建需要一段時間才能完成。執行下列命令以檢查解除佈建的狀態。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

請等到狀態變成 deprovisioned (已解除佈建) 後，再繼續進行下一個步驟。

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. 執行下列命令以刪除最上層集區。

   此步驟必須由 IPAM 帳戶完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

   您可在輸出結果中看到刪除狀態。

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0053b7d2b4fc3f730",
        "SourceIpamPoolId": "ipam-pool-07f2466c7158b50c4",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0053b7d2b4fc3f730",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "reg-ipv6-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv6"
    }
}
```

10. 執行下列命令以刪除 IPAM。

    此步驟必須由 IPAM 帳戶完成。

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    您會在輸出結果中看到 IPAM 回應。這表示 IPAM 已刪除。

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-090e48e75758de279",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",
        "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
```

```
                "RegionName": "us-east-1"

            },
            {
                "RegionName": "us-west-2"
            }
        ]
    }
}
```

使用 IPAM 將您自己的 IP 帶到 CloudFront （ 支援 IPv4 和 IPv6)

IPAM 的 BYOIP for 全域服務可讓您將自己的 IPv4 和 IPv6 地址與 CloudFront 等 AWS 全域服務搭配使用。與區域 BYOIP 不同，您的 IP 地址會透過任何傳送路由同時從多個節點公告。

本教學課程涵蓋：

- 為 IPv4 (/24) 和/或 IPv6 (/48) 地址範圍建立全域 IPAM 集區
- 使用您自己的 IP 地址佈建 Anycast 靜態 IP 清單
- 透過 CloudFront 節點在全球公告您的 CIDRs
- 使用個別 IPv4 和 IPv6 IPAM 集區的雙堆疊組態

為什麼要使用此功能？

- 維護 IP 允許清單 – 使用現有的已核准 IP 地址，而不是更新防火牆組態
- 簡化遷移 – 從其他 CDNs 遷移而不變更 IP 基礎設施
- 一致的品牌 – 移至 時保留現有的 IP 地址空間 AWS
- IPv6 整備 – 支援具有 IPv4 和 IPv6 的現代雙堆疊架構

誰應該使用此功能？

需要具有全域內容交付之自有 IP 地址的組織：

- 具有 IP 允許清單要求的大型企業
- 使用現有 IP 地址從其他 CDNs 遷移的公司
- 具有要求特定 IP 範圍之嚴格安全政策的組織

- 需要雙堆疊 (IPv4/IPv6) 組態以實現全域覆蓋的企業

何時使用此功能？

當您需要下列項目時，請將 BYOIP 用於全域服務：

- 與合作夥伴/用戶端維護現有的 IP 允許清單
- 使用您的 IP 地址從另一個 CDN 遷移
- 符合特定 IP 範圍的合規要求
- 部署支援 IPv4 和 IPv6 用戶端的雙堆疊架構

> **Note**
>
> 需要 IPv4 的 IPv4 CIDR 區塊。雙堆疊 (IPv4 和 IPv6) 需要 /24 IPv4 和 /48 IPv6 CIDR 區塊。目前僅適用於 CloudFront。

先決條件

請先完成下列步驟，再開始：

- IPAM 設定 – 將 IPAM 與 AWS Organizations 中的帳戶整合和 建立 IPAM
- 網域驗證 – 驗證網域控制
- 建立頂層集區 – 遵循將您自己的 IPv4 CIDR 帶到 IPAM 和/或將您自己的 IPv6 CIDR 帶到 IPAM 中的步驟 1-2 (IPv4 IPv6
- ROA （路由來源授權） – 如果部署雙堆疊，請確保同時為 IPv4 (/24) 和 IPv6 (/48) 字首設定 ROAs

全域服務組態步驟

下列步驟與標準區域 BYOIP 程序不同，並建立全域服務的模式。對於雙堆疊部署，您將為 IPv4 和 IPv6 建立單獨的集區，然後將兩者佈建至 CloudFront。

步驟 1：為任何廣播服務建立全域集區 (s)

不是建立區域集區，而是為任何廣播服務建立全域集區：

主控台

若要使用主控台建立全域集區：

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇集區
3. 選擇建立集區
4. 來源：選擇最上層 BYOIP 集區
5. 地區設定：選擇全域
6. 服務：選擇全域服務（選取全域時出現）
7. 公有 IP 來源：選擇 BYOIP
8. 要佈建CIDRs：指定您的 /24 CIDR 範圍（適用於 IPv4) 或 /48 CIDR 範圍（適用於 IPv6)
9. 選擇建立集區

CLI

對於 IPv4：

```
aws ec2 create-ipam-pool \
  --ipam-scope-id scope-id \
  --locale None \
  --address-family ipv4 \
  --source-ipam-pool-id top-level-pool-id

aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id global-pool-id \
  --cidr your-ipv4-/24
```

對於 IPv6：

```
aws ec2 create-ipam-pool \
  --ipam-scope-id scope-id \
  --locale None \
  --address-family ipv6 \
  --source-ipam-pool-id top-level-pool-id

aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id global-pool-id \
```

```
--cidr your-ipv6-/48
```

Important

- 對於 IPv4：您必須將完整的 /24 區塊配置到此集區。您可以在此區塊中為不同用途佈建更具體的範圍。
- 對於 IPv6：您必須將完整的 /48 區塊配置到此集區。您可以在此區塊中為不同用途佈建更具體的範圍。

步驟 2：建立服務特定的資源

針對 CloudFront，建立使用您的 IPAM 集區的任何廣播 IP 清單。如需詳細說明，請參閱《Amazon CloudFront 開發人員指南》中的使用 IPAM 將您自己的 IP 帶到 CloudFront。 Amazon CloudFront

IPAM 整合的關鍵參數：

- IP 地址類型 – 選擇 BYOIP
- IPAM 集區 – 從步驟 1 選取您的全域集區 (IPv4 或 IPv6)
- IP 計數 – 輸入 3 (CloudFront 需要)

步驟 3：與服務資源建立關聯

將您的 Anycast 靜態 IP 清單與 CloudFront 分佈建立關聯。如需詳細說明，請參閱《Amazon CloudFront 開發人員指南》中的使用 IPAM 將您自己的 IP 帶到 CloudFront。 Amazon CloudFront

金鑰組態：

- 在分佈設定中，從步驟 2 選取您的 Anycast IP 清單

步驟 4：準備遷移

- 降低 DNS TTL – 將記錄的 DNS TTL 設定為 60 秒或更短
- 等待傳播 – 允許新的 TTL 在網際網路上生效

步驟 5：全域公告 CIDR

使用 IPAM 全域公告命令：

主控台

若要使用主控台公告 CIDR：

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中，選擇集區
3. 選取您的全域集區
4. 選擇 CIDRs索引標籤
5. 選取您的 CIDR，然後選擇動作 > 公告 CIDR
6. 確認廣告

CLI

對於 IPv4：

```
aws ec2 advertise-byoip-cidr \
  --cidr your-ipv4-/24
```

對於 IPv6：

```
aws ec2 advertise-byoip-cidr \
  --cidr your-ipv6-/48
```

> **Important**
>
> - 在執行此命令之前，從先前的供應商中撤回公告
> - 更新 DNS 記錄以指向 CloudFront 以完成遷移 (IPv4 的記錄、IPv6 的 AAAA 記錄)

清除

若要清除本教學課程中建立的資源：

- 刪除 CloudFront 資源 – 遵循《Amazon CloudFront 開發人員指南》中的使用 IPAM 將您自己的 IP 帶到 CloudFront 中的清除說明 Amazon CloudFront
- 撤銷 CIDR 並刪除 IPAM 集區 – 遵循 中的標準清除程序 步驟 8：清除

> **Important**
>
> 首先刪除 CloudFront 資源，然後繼續 IPAM 清除，以避免服務中斷。

教學課程：將 BYOIP IPv4 CIDR 傳輸至 IPAM

請依照下列步驟將現有的 IPv4 CIDR 傳輸至 IPAM。如果您已使用 IPv4 BYOIP CIDR AWS，您可以從公有 IPv4 集區將 CIDR 移至 IPAM。您無法將 IPv6 CIDR 移動至 IPAM。

本教學課程假設您已 AWS 使用 Amazon EC2 中自有 IP 地址 (BYOIP) 所述的程序，成功將 IP 地址範圍帶到 ，現在您想要將該 IP 地址範圍轉移到 IPAM。如果您是 AWS 第一次將新的 IP 地址帶到 ，請完成 中的步驟教學課程：將 IP 地址帶入 IPAM。

如果您是將公用 IPv4 集區轉移至 IPAM，則對現有配置不會有影響。將公用 IPv4 集區轉移至 IPAM 後，視資源類型而定，您或許能監視現有的配置。如需詳細資訊，請參閱依資源監控 CIDR 使用情況。

> **Note**
>
> - 本教學課程假設您已完成 建立 IPAM 中的步驟。
> - 本教學課程的每個步驟必須由兩個 AWS 帳戶之一完成：
>   - IPAM 管理員的帳戶。在本教學課程中，此帳戶將稱為 IPAM 帳戶。
>   - 您組織中擁有 BYOIP CIDR 的帳戶。在本教學課程中，此帳戶將稱為 BYOIP CIDR 擁有者帳戶。

目錄

步驟 1：建立 AWS CLI 具名設定檔和 IAM 角色

若要以單一 AWS 使用者身分完成本教學課程，您可以使用 AWS CLI 具名設定檔從一個 IAM 角色切換到另一個角色。具名設定檔是您在搭配 AWS CLI使用 `--profile` 選項時所參考的設定和憑證的集合。如需如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱《》中的使用 IAM 角色 AWS CLI。

為您將在本教學課程中使用的三個 AWS 帳戶各建立一個角色和一個具名設定檔：

- `ipam-account` 為 IPAM 管理員 AWS 帳戶呼叫的設定檔。
- 您組織中擁有 BYOIP CIDR `byoip-owner-account` 之 AWS 帳戶的 設定檔。

建立 IAM 角色和具名設定檔後，請返回此頁面並繼續下一個步驟。在本教學課程的其餘部分，您會注意到範例 AWS CLI 命令使用 `--profile`選項搭配其中一個具名設定檔，以指出哪個帳戶必須執行 命令。

步驟 2：取得您 IPAM 的公有範圍 ID

請依照本節中的步驟取得 IPAM 的公有範圍 ID。此步驟應由 **`ipam-account`** 帳戶執行。

執行以下命令以取得公有範圍 ID。

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

您會在輸出結果中看到您的公有範圍 ID。請記下 `PublicDefaultScopeId` 的值。下一個步驟將需要此值。

```
{
 "Ipams": [
        {
            "OwnerId": "123456789012",
            "IpamId": "ipam-090e48e75758de279",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
            "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",
            "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",
            "ScopeCount": 2,
            "Description": "my-ipam",
            "OperatingRegions": [
                {
```

```
                    "RegionName": "us-east-1"
                },
                {
                    "RegionName": "us-west-2"
                }
            ],
            "Tags": []
        }
    ]
}
```

步驟 3：建立 IPAM 集區

請依照本節中的步驟來建立 IPAM 集區。此步驟應由 **ipam-account** 帳戶執行。您建立的 IPAM 集區需為最上層集區，其 `--locale` 選項需與 BYOIP CIDR AWS 區域相符。只能將 BYOIP 傳輸至最上層 IPAM 集區。

> **Important**
>
> 建立集區時，必須包含 `--aws-service ec2`。您選取的服務會決定 CIDR 可公告 AWS 的服務。目前，唯一的選項是 `ec2`，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務 (適用於彈性 IP 地址) 和 Amazon VPC 服務 (適用於與 VPC 關聯的 CIDR) 進行公告。

使用 為傳輸的 BYOIP CIDR 建立 IPv4 地址集區 AWS CLI

1. 執行下列命令以建立 IPAM 集區。使用您在上一個步驟中取得的 IPAM 公有範圍 ID。

```
aws ec2 create-ipam-pool --region us-east-1 --profile ipam-account --ipam-scope-
id ipam-scope-0087d83896280b594 --description "top-level-pool" --locale us-west-2
 --aws-service ec2 --address-family ipv4
```

   您會在輸出結果中看到 `create-in-progress`，表示正在建立集區。

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
```

```
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-west-2",
        "PoolDepth": 1,
        "State": "create-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "AddressFamily": "ipv4",
        "Tags": [],
        "AwsService": "ec2"
    }
}
```

2. 執行下列命令，直到輸出結果顯示 `create-complete` 的狀態為止。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

下例的輸出結果顯示集區的狀態。您在下個步驟中將會需要 OwnerId。

```
{
    "IpamPools": [
        {
            "OwnerId": "123456789012",
            "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
            "IpamScopeType": "public",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
            "Locale": "us-west-2",
            "PoolDepth": 1,
            "State": "create-complete",
            "Description": "top-level-pool",
            "AutoImport": false,
            "AddressFamily": "ipv4",
            "Tags": [],
            "AwsService": "ec2"
        }
    ]
```

```
}
```

步驟 4：使用 共用 IPAM 集區 AWS RAM

請依照本節中的步驟使用 共用 IPAM 集區， AWS RAM 讓另一個 AWS 帳戶可以將現有的 BYOIP IPV4 CIDR 轉移到 IPAM 集區，並使用 IPAM 集區。此步驟應由 **ipam-account** 帳戶執行。

使用 共用 IPv4 地址集區 AWS CLI

1. 檢視 IPAM 集區的可用 AWS RAM 許可。您需要使用兩個 ARN，才能完成本節中的步驟。

```
aws ram list-permissions --region us-east-1 --profile ipam-account --resource-type
 ec2:IpamPool
```

```
{
    "permissions": [
        {
           "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool",
           "version": "1",
           "defaultVersion": true,
           "name": "AWSRAMDefaultPermissionsIpamPool",
           "resourceType": "ec2:IpamPool",
           "status": "ATTACHABLE",
           "creationTime": "2022-06-30T13:04:29.335000-07:00",
           "lastUpdatedTime": "2022-06-30T13:04:29.335000-07:00",
           "isResourceTypeDefault": true
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionIpamPoolByoipCidrImport",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMPermissionIpamPoolByoipCidrImport",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:55.032000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:55.032000-07:00",
            "isResourceTypeDefault": false
        }
    ]
}
```

2. 建立資源共用，以讓 **byoip-owner-account** 帳戶將 BYOIP CIDR 匯入 IPAM。--resource-arns 值為您在上一節建立之 IPAM 集區的 ARN。--principals 值為 BYOIP CIDR 擁有者帳戶的帳戶 ID。--permission-arns 值為 AWSRAMPermissionIpamPoolByoipCidrImport 許可的 ARN。

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare2 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMPermissionIpamPoolByoipCidrImport
```

```
{

    "resourceShare": {

        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7993758c-a4ea-43ad-be12-b3abaffe361a",
        "name": "PoolShare2",

        "owningAccountId": "123456789012",

        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:32:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:32:25.536000-07:00"

        }

}
```

3. (選用) 如果您要允許 **byoip-owner-account** 帳戶在傳輸完成後，將 IPAM 集區的 IP 地址 CIDRS 配置給公有 IPv4 集區，請複製 AWSRAMDefaultPermissionsIpamPool 的 ARN，並建立第二個資源共用。--resource-arns 值為您在上一節建立之 IPAM 集區的 ARN。--principals 值為 BYOIP CIDR 擁有者帳戶的帳戶 ID。--permission-arns 值為 AWSRAMDefaultPermissionsIpamPool 許可的 ARN。

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare1 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
```

```
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool
```

```
{

    "resourceShare": {

        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f",
        "name": "PoolShare1",

        "owningAccountId": "123456789012",

        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:31:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:31:25.536000-07:00"

        }

}
```

由於您已在 RAM 中建立資源共用，因此 byoip-owner-account 帳戶現在可將 CIDR 移動至 IPAM。

步驟 5：將現有的 BYOIP IPV4 CIDR 傳輸至 IPAM

請依照本節中的步驟將現有的 BYOIP IPV4 CIDR 傳輸至 IPAM。此步驟應由 **byoip-owner-account** 帳戶執行。

> **Important**
>
> 將 IPv4 地址範圍帶入其中後 AWS，您可以使用範圍內的所有 IP 地址，包括第一個地址（網路地址）和最後一個地址（廣播地址）。

若要將 BYOIP CIDR 傳輸至 IPAM，BYOIP CIDR 擁有者的 IAM 政策需具有下列許可：

- `ec2:MoveByoipCidrToIpam`

- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> 您可以 AWS CLI 針對此步驟使用 AWS 管理主控台 或 。

AWS Management Console

若要將 BYOIP CIDR 傳輸至 IPAM 集區：

1. 請以 **`byoip-owner-account`** 帳戶的身分在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇此教學課程中所建立的最上層集區並共用之。
4. 選擇動作 >傳輸 BYOIP CIDR。
5. 選擇傳輸 BYOIP CIDR。
6. 選擇您的 BYOIP CIDR。
7. 選擇 Provision (佈建)。

Command line

使用下列 AWS CLI 命令，使用 將 BYOIP CIDR 傳輸至 IPAM 集區 AWS CLI：

1. 執行下列命令以傳輸 CIDR。請確定該`--region`值是 BYOIP CIDR AWS 的區域。

```
aws ec2 move-byoip-cidr-to-ipam --region us-west-2 --profile byoip-owner-account
 --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --ipam-pool-owner 123456789012 --
cidr 130.137.249.0/24
```

輸出結果會顯示 CIDR 的佈建處於待定狀態。

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",
```

```
        "State": "pending-transfer"

    }

}
```

2. 確保 CIDR 已傳輸。執行下列命令，直到輸出結果顯示 complete-transfer 的狀態為止。

```
aws ec2 move-byoip-cidr-to-ipam --region us-west-2  --profile byoip-
owner-account --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --ipam-pool-
owner 123456789012 --cidr 130.137.249.0/24
```

下例的輸出結果即顯示狀態。

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

步驟 6：檢視 IPAM 中的 CIDR

請依照本節中的步驟檢視 IPAM 中的 CIDR。此步驟應由 **ipam-account** 帳戶執行。

使用 在 IPAM 集區中檢視傳輸的 BYOIP CIDR AWS CLI

- 執行下列命令以檢視透過 IPAM 進行管理的配置。請確定該--region值是 BYOIP CIDR AWS 的區域。

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

該輸出結果會顯示 IPAM 中的分配情況。

```
{
```

```
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

步驟 7：清除

請依照本節中的步驟移除您在本教學課程中建立的資源。此步驟應由 **ipam-account** 帳戶執行。

使用 清除本教學課程中建立的資源 AWS CLI

1. 若要刪除 IPAM 集區共用資源，請執行下列命令，以取得第一個資源共用 ARN：

```
aws ram get-resource-shares --region us-east-1 --profile ipam-account --
name PoolShare1 --resource-owner SELF
```

```
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f",
            "name": "PoolShare1",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2023-04-28T07:31:25.536000-07:00",
            "lastUpdatedTime": "2023-04-28T07:31:25.536000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

2. 複製資源共用 ARN，並使用其刪除 IPAM 集區資源共用。

```
aws ram delete-resource-share --region us-east-1 --profile ipam-account
 --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f
```

```
{
    "returnValue": true
}
```

3. 如果您在 步驟 4：使用 共用 IPAM 集區 AWS RAM 中已建立其他資源共用，請重複前兩個步驟，以取得 PoolShare2 的第二個資源共用 ARN，並刪除第二個資源共用。
4. 執行下列命令以取得 BYOIP CIDR 的配置 ID。確保 `--region`值符合 BYOIP CIDR AWS 的區域。

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

該輸出結果會顯示 IPAM 中的分配情況。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

5. 釋出公有 IPv4 集區的 CIDR。當您執行本節中的命令時，`--region` 的值必須與 IPAM 的區域相符。

此步驟必須由 **byoip-owner-account** 帳戶完成。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1  --profile byoip-
owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.0/24
```

6. 再次檢視您的 BYOIP CIDR，並確保其中不再有已佈建的地址。當您執行本節中的命令時，--region 的值必須與 IPAM 的區域相符。

   此步驟必須由 **byoip-owner-account** 帳戶完成。

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
```

   您會在輸出結果的公有 IPv4 集區中看到 IP 地址計數。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

7. 執行下列命令以刪除最上層集區。

```
aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
id ipam-pool-0a03d430ca3f5c035
```

   您可在輸出結果中看到刪除狀態。

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
```

```
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4",
        "AwsService": "ec2"
    }
}
```

教學課程：為子網路 IP 配置規劃 VPC IP 地址空間

完成此教學課程，即可規劃 VPC IP 地址空間，以便將 IP 地址配置給 VPC 子網路，並在子網路和 VPC 層級監控 IP 地址相關指標。

> **Note**
>
> 本教學課程涵蓋將私有 IPAM 範圍中的私有 IPv4 地址空間配置給 VPC 和子網路。亦可透過在 VPC 主控台上使用 Amazon 提供的 IPv6 CIDR 區塊選項來建立 VPC，使用 IPv6 CIDR 範圍完成本教學課程。

可透過為子網路規劃 VPC IP 地址空間執行下列動作：

- 規劃和組織待配置給子網路的 VPC IP 地址：您可以將 VPC IP 地址空間劃分為較小的 CIDR 區塊，並將這些 CIDR 區塊佈建至具有不同業務需求的子網路，例如在開發或生產子網路中執行工作負載。
- 簡化 VPC 子網路的 IP 地址配置：規劃和組織 VPC 的地址空間後，可以選擇網路遮罩長度，而不必手動輸入 CIDR。例如，如果開發人員正在建立用於託管開發工作負載的子網路，他們需要為子網路選擇集區和網路遮罩長度，IPAM 就會自動將 CIDR 區塊配置給子網路。

以下範例顯示依照本教學課程建立之集區和資源結構的階層：

- 私有範圍
  - 資源規劃集區 (10.0.0.0/20)
    - 開發子網路集區 (10.0.0.0/24)
      - 開發子網路 (10.0.0.0/28)
    - 生產子網路集區 (10.0.0.1/24)

- 生產子網路 (10.0.0.16/28)

Important

- 資源規劃集區可用來將 CIDR 配置給子網路，也可以用作可在其中建立其他集區的來源集區。本教學課程將資源規劃集區用作子網路集區的來源集區。
- 如果已為 VPC 佈建一個以上的 CIDR，則您可以使用相同的 VPC 建立多個資源規劃集區；例如，如果已為 VPC 指派兩個 CIDR，您可以建立兩個資源規劃集區，每個 CIDR 各一個。每個 CIRD 一次可指派至一個集區。

步驟 1：建立 VPC

完成本節中的步驟，建立用於子網路 IP 地址規劃的 VPC。如需建立 VPC 所需的 IAM 許可的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 政策範例。

Note

您可以使用現有 VPC 而不是建立新 VPC，但本教學課程著重於使用手動配置的 CIDR 區塊 (而不是自動配置 IPAM 的 CIDR 區塊) 來設定 VPC 的案例。

建立 VPC

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/vpc/ 中開啟 IPAM 主控台。
2. 選擇建立 VPC。
3. 輸入 VPC 的名稱，例如 tutorial-vpc。
4. 選擇 IPv4 CIDR manual input (IPv4 CIDR 手動輸入)，然後輸入 IPv4 CIDR 區塊。本教學課程中使用 10.0.0.0/20。
5. 略過新增 IPv6 CIDR 區塊的選項。
6. 選擇建立 VPC。
7. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
8. 在左側導覽窗格中選擇 Resource (資源)。
9. 等待顯示建立的 VPC。該動作需要一些時間，並且可能需要重新整理視窗才能看到。IPAM 必須探索到 VPC，然後才能繼續下一步。

步驟 2：建立資源規劃集區

完成本節中的步驟來建立資源規劃集區。

建立資源規劃集區

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍。
4. 選擇建立集區。
5. 在 IPAM 範圍下，保持選取的私有範圍。
6. (可選) 新增集區的 Name tag (名稱標籤)，例如 "Resource-planning-pool"。
7. 在 Source (來源) 下，選擇 IPAM scope (IPAM 範圍)。
8. 在 Resource planning (資源規劃) 下，選擇 Plan IP space within a VPC (規劃 VPC 內的 IP 空間)，然後選擇在上一步中建立的 VPC。VPC 是用來將 CIDR 佈建至資源規劃集區的資源。
9. 在 CIDRs to provision (要佈建的 CIDR) 下，選擇要為集區佈建的 CIDR。佈建至資源規劃集區的 CIDR 必須與佈建至 VPC 的 CIDR 相符。本教學課程中使用 10.0.0.0/20。
10. 選擇建立集區。
11. 建立集區後，選擇 CIDR tab (CIDR 索引標籤)，查看已佈建 CIDR 的狀態。重新整理頁面並等待 CIDR 狀態從 Pending-provision (待佈建) 變更為 Provisioned (已佈建)，然後再進行下一步。

步驟 3：建立子網路集區

完成本節中的步驟，建立兩個將 IP 空間配置給子網路的子網路集區。

建立子網路集區

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍。
4. 選擇建立集區。
5. 在 IPAM 範圍下，保持選取的私有範圍。
6. (可選) 新增集區的 Name tag (名稱標籤)，例如 "dev-subnet-pool"。
7. 在 Source (來源) 下，選擇 IPAM pool (IPAM 集區)，然後選取在步驟 3 中建立的資源規劃集區。會自動從來源集區繼承地址系列、資源規劃組態及地區設定。

8. 在 CIDRs to provision (要佈建的 CIDR) 下，選擇要為子網路集區佈建的 CIDR。本教學課程中使用 10.0.0.0/24。
9. 選擇建立集區。
10. 建立集區後，選擇 CIDR tab (CIDR 索引標籤)，查看已佈建 CIDR 的狀態。重新整理頁面並等待 CIDR 狀態從 Pending-provision (待佈建) 變更為 Provisioned (已佈建)，然後再進行下一步。
11. 重複此程序，建立另一個名為 "prod-subnet-pool" 的子網路。

此時，如果您想要將此子網路集區提供給其他 AWS 帳戶，您可以共用子網路集區。如需如何執行該作業的說明，請參閱 透過 AWS RAM 共用 IPAM 集區。然後回到此處以完成教學課程。

步驟 4：建立子網路

完成這些步驟，建立兩個子網路。

建立子網路

1. 使用適當的帳戶，在 https://console.aws.amazon.com/vpc/ 中開啟 VPC 主控台。
2. 選擇 Subnets (子網路) > Create subnet (建立子網路)。
3. 選擇在本教學課程開始時建立的 VPC。
4. 輸入子網路的名稱，例如 "tutorial-subnet"。
5. (可選) 選擇 Availability Zone (可用區域)。
6. 在 IPv4 CIDR block (IPv4 CIDR 區塊) 下，選擇 IPAM-allocated IPV4 CIDR block (IPAM 配置的 IPV4 CIDR 區塊)，然後選擇開發子網路集區和 /28 網路遮罩。
7. 選擇 Create subnet (建立子網路)。
8. 重複此程序，建立其他子網路。這次選擇生產子網路集區和 /28 網路遮罩。
9. 回到 IPAM 主控台，然後在左側導覽窗格中選擇 Resources (資源)。
10. 尋找已建立的子網路集區，然後等待建立的子網路顯示在其下方。該動作需要一些時間，並且可能需要重新整理視窗才能看到。

此教學課程完成。可視需要建立其他子網路集區，亦可在 EC2 執行個體中啟動到其中一個子網路中。

IPAM 會在子網路中發佈與 IP 地址使用狀況相關的指標。您可以針對 SubnetIPUsage 指標設定 CloudWatch 警示，以便在違反 IP 使用率閾值時採取行動。例如，如果已將 /24 CIDR (256 個 IP 地址) 指派給子網路，而您希望在使用 80% 的 IP 時收到通知，則可以設定在達到此閾值時提醒您的 CloudWatch 警示。如需為子網路 IP 使用情況建立警示的詳細資訊，請參閱 建立警示的快速提示。

步驟 5：清除

完成以下步驟，刪除在本教學課程中建立的資源。

清除資源

1. 使用 IPAM 管理員帳戶，在 https://console.aws.amazon.com/ipam/ 中開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇私有範圍。
4. 選擇資源規劃集區，然後選擇 Action (動作) > Delete (刪除)。
5. 選取 Cascade delete (串聯刪除)。將刪除資源規劃集區和子網路集區。該動作不會刪除子網路本身。它們會保留在佈建的 CIDR 內，但是 CIDR 不再來自 IPAM 集區。
6. 選擇 刪除。
7. 刪除子網路。
8. 刪除 VPC。

清理完成。

從 IPAM 集區配置循序彈性 IP 位址

IPAM 可讓您將 Amazon 擁有的公有 IPv4 區塊佈建至 IPAM 集區，並將這些集區的循序彈性 IP 地址配置至 AWS 資源。

連續配置的彈性 IP 位址是依序配置的公有 IPv4 地址。例如，如果 Amazon 為您提供 `192.0.2.0/30` 的公有 IPv4 CIDR 區塊，且您從該 CIDR 區塊配置四個可用的公有 IPv4 地址，則四個循序彈性 IP 位址的範例為 `192.0.2.0`、`192.0.2.1`、`192.0.2.2` 和 `192.0.2.3`。

配置一致性的彈性 IP 位址可讓您以下列方式簡化您的安全和聯網規則：

- 安全管理：使用循序 IPv4 地址可降低防火牆管理開銷。您可以使用單一規則新增整個字首，並將 IP 與擴展時相同的字首建立關聯，以節省時間和精力。
- 企業存取：您可以使用整個 CIDR 區塊來簡化與用戶端共用的位址空間，而不是個別公有 IPv4 地址的長清單。這樣可避免隨著應用程式在 AWS上擴展，而需要持續傳達 IP 變更。
- 簡化的 IP 管理：使用循序 IPv4 地址可簡化中央聯網團隊的公有 IP 管理，因為它可減少追蹤個別公有 IP 的需求，並讓團隊專注於有限數量的 IP 字首。

在本教學課程中，您將完成從 IPAM 集區配置循序彈性 IP 位址的必要步驟。您將使用 Amazon 提供的連續公有 IPv4 CIDR 區塊建立 IPAM 集區，從集區配置彈性 IP 位址，並了解如何監控 IPAM 集區配置。

> **Note**
>
> - 佈建 Amazon 擁有的公有 IPv4 CIDR 區塊會產生相關費用。如需詳細資訊，請參閱 Amazon VPC 定價頁面上的 Amazon 提供的連續 IPv4 區塊索引標籤。
> - 本教學假設您想要使用 IPAM 搭配單一帳戶來建立 IPAM。如果您想要跨帳戶共用 Amazon 擁有的連續公有 IPv4 區塊，請先將 IPAM 與 AWS Organizations 中的帳戶整合，然後透過 AWS RAM 共用 IPAM 集區。如果您與 AWS Organizations 整合，您可以選擇建立服務控制政策，以防止取消佈建指派給集區的爭用 IPv4 區塊。
> - 您無法將配置的循序彈性 IP 位址從 IPAM 集區轉移到其他 AWS 帳戶。相反地，IPAM 可讓您透過整合 IPAM 與 AWS Organizations （如上所述） 來跨 AWS 帳戶共用 IPAM 集區。
> - 您可以佈建的 Amazon 擁有公有 IPv4 CIDR 區塊數量及其大小有所限制。如需詳細資訊，請參閱IPAM 的配額。

目錄

步驟 1：建立 IPAM

完成本節中的步驟來建立 IPAM。

AWS Management Console

建立 IPAM

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。

2. 在 AWS 管理主控台中，選擇您要在其中建立 IPAM AWS 的區域。在您的主要作業區域中建立 IPAM。
3. 在服務首頁選擇 Create IPAM (建立 IPAM)。
4. 選擇 Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (允許 Amazon VPC IP 地址管理員將來源帳戶的資料複寫到 IPAM 委託帳戶)。若未選取此選項，即無法建立 IPAM。
5. 選擇 IPAM tier (IPAM 方案)。如需每個方案中的可用功能以及方案關聯成本的詳細資訊，請參閱 Amazon VPC 定價頁面中的 IPAM 索引標籤。
6. 在 Operating regions (作業區域) 下，選取此 IPAM 可管理及探索資源的 AWS 區域。您建立 IPAM AWS 的區域預設會選取為其中一個操作區域。例如，如果您要在 AWS 區域中建立此 IPAM，`us-east-1`但稍後想要建立區域 IPAM 集區，以提供 CIDRs給 中的 VPC`us-west-2`，請選取`us-west-2`這裡。如果您忘記作業區域，稍後可以返回並編輯 IPAM 設定。

   > **Note**
   >
   > 如果要在免費方案中建立 IPAM，可以為 IPAM 選取多個作業區域，但唯一可在各個作業區域使用的 IPAM 功能是公共 IP 洞察功能。無法在 IPAM 的作業區域中使用免費方案中的其他功能，例如 BYOIP。只能在 IPAM 的主區域中使用。若要跨作業區域使用所有 IPAM 功能，請在進階方案中建立 IPAM。

7. 選擇 Create IPAM (建立 IPAM)。

Command line

本節中的命令連結至 CLI AWS 參考文件。本文件旨在詳細說明執行命令時可使用的選項。

使用 create-ipam 命令建立 IPAM：

```
aws ec2 create-ipam --region us-east-1
```

回應範例：

```
{
    "Ipam": {
        "OwnerId": "320805250157",
        "IpamId": "ipam-0755477df834ea06b",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
```

```
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-01bc7290e4a9202f9",
        "PrivateDefaultScopeId": "ipam-scope-0a50983b97a7a583a",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "State": "create-in-progress",
        "Tags": [],
        "DefaultResourceDiscoveryId": "ipam-res-disco-02cc5b34cc3f04f09",
        "DefaultResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-06b3a4dccfc81f7c1",
        "ResourceDiscoveryAssociationCount": 1,
        "Tier": "advanced"
    }
}
```

您將需要在下一步使用公有範圍 ID。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。

第 2 步：建立 IPAM 集區並佈建 CIDR

完成本節中的步驟，以建立您要從中配置彈性 IP 位址的 IPAM 集區。

AWS Management Console

建立集區

1. 請在 https://console.aws.amazon.com/ipam/ 開啟 IPAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇公有範圍。如需有關範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇建立集區。
5. (選用) 新增集區的 Name tag (名稱標籤) 和集區的 Description (說明)。
6. 在 Source (來源) 下，選擇 IPAM scope (IPAM 範圍)。
7. 在 Address family (地址系列) 下，選擇 IPv4。
8. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。

9. 在 Locale (區域設定) 下，選擇該集區的區域設定。地區設定是您希望此 IPAM 集區可用於配置 AWS 的區域。可用選項來自您在建立 IPAM 時選擇的作業區域。
10. 在 Service (服務) 下，選擇 EC2 (EIP/VPC)。您選取的服務決定 CIDR 將公告 AWS 的服務。目前，唯一的選項是 EC2 (EIP/VPC)，這意味著從此集區配置的 CIDR 可針對 Amazon EC2 服務 (適用於彈性 IP 位址) 進行公告。
11. 在 公有 IP 來源 下，選擇 Amazon 擁有。
12. 在 要佈建的 CIDR 下，選擇 新增 Amazon 擁有的公有 CIDR。選擇介於 /29 (8 個 IP 位址) 和 /30 (4 個 IP 位址) 之間的 網路遮罩 長度。根據預設，您最多可以新增 2 個 CIDR。如需提高 Amazon 提供的連續公有 IPv4 CIDR 限制的相關資訊，請參閱 IPAM 的配額。
13. 將調整此集區的分配規則設定保持在未選取的狀態。
14. (選用) 為集區選擇 Tags (標籤)。
15. 選擇建立集區。

請先確定此 CIDR 已佈建，然後再繼續。您可在集區詳細資訊頁面的 CIDRs (CIDR) 索引標籤中看到佈建狀態。

Command line

建立集區

1. 使用 create-ipam-pool 命令建立 IPAM 集區。地區設定為您希望此 IPAM 集區可供配置使用的 AWS 區域。可用選項來自您在建立 IPAM 時選擇的作業區域。

```
aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-
scope-01bc7290e4a9202f9 --address-family ipv4 --locale us-east-1 --aws-service
 ec2 --public-ip-source amazon
```

狀態為 create-in-progress 的回應範例：

```
{

    "IpamPool": {

        "OwnerId": "320805250157",

        "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",
```

```
        "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-07ccc86aa41bef7ce",
        "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-01bc7290e4a9202f9",
        "IpamScopeType": "public",

        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",

        "IpamRegion": "us-east-1",

        "Locale": "us-east-1",

        "PoolDepth": 1,

        "State": "create-in-progress",

        "AutoImport": false,

        "AddressFamily": "ipv4",

        "Tags": [],

        "AwsService": "ec2",

        "PublicIpSource": "amazon"

    }

}
```

2. 使用 describe-ipam-pools 命令檢查集區是否已成功建立。

```
aws ec2 describe-ipam-pools --region us-east-1 --ipam-pool-ids ipam-
pool-07ccc86aa41bef7ce
```

狀態為 create-complete 的回應範例：

```
{

    "IpamPools": [
        {
            "OwnerId": "320805250157",
            "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",
```

```
            "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-07ccc86aa41bef7ce",
            "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-01bc7290e4a9202f9",
            "IpamScopeType": "public",
            "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
            "IpamRegion": "us-east-1",
            "Locale": "us-east-1",
            "PoolDepth": 1,
            "State": "create-complete",
            "AutoImport": false,
            "AddressFamily": "ipv4",
            "Tags": [],
            "AwsService": "ec2",
            "PublicIpSource": "amazon"
        }
    ]
}
```

3. 使用 provision-ipam-pool-cidr 命令位集群佈建 CIDR。選擇介於 /29 (8 個 IP 位址) 和 /30 (4 個 IP 位址) 之間的 --netmask-length。根據預設，您最多可以新增 2 個 CIDR。如需提高 Amazon 提供的連續公有 IPv4 CIDR 限制的相關資訊，請參閱 IPAM 的配額。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce --netmask-length 29
```

狀態為 pending-provision 的回應範例：

```
{

    "IpamPoolCidr": {
        "State": "pending-provision",
        "IpamPoolCidrId": "ipam-pool-cidr-01856e43994df4913b7bc6aac47adf983",
        "NetmaskLength": 29
    }
}
```

4. 請先確定此 CIDR 已佈建，然後再繼續。您可以使用 get-ipam-pool-cidrs 命令檢視佈建狀態。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

狀態為 provisioned 的回應範例：

```
{

    "IpamPoolCidrs": [
        {
            "Cidr": "18.97.0.40/29",
            "State": "provisioned",
            "IpamPoolCidrId": "ipam-pool-
cidr-01856e43994df4913b7bc6aac47adf983",
            "NetmaskLength": 29
        }
    ]
}
```

第 3 步：從集區配置彈性 IP 位址

按照本節中的步驟，從集區配置彈性 IP 位址。

AWS Management Console

請依照《Amazon EC2 使用者指南》中的配置彈性 IP 位址中的步驟配置地址，但請注意下列事項：

- 請確定您在 EC2 主控台中的 AWS 區域符合您在步驟 2 中建立集區時所選擇的地區設定選項。
- 選擇位址集區時，請選擇使用 IPv4 IPAM 集區配置的選項，然後選擇您在第 1 步中建立的集區。

Command line

使用 allocate-address 命令從集區配置地址。您使用的 --region 必須與您在步驟 2 中建立集區時所選擇的 -locale 選項相符。在 --ipam-pool-id 中包含您在第 2 步中建立的 IPAM 集區的 ID。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

回應範例：

```
{
```

```
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

您也可以選擇 IPAM 集區中的特定 /32，方法是使用 --address 選項。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce --address 18.97.0.41
```

回應範例：

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的配置彈性 IP 位址。

第 4 步：建立彈性 IP 位址與 EC2 執行個體的關聯

完成本節中的步驟，建立彈性 IP 位址與 EC2 執行個體的關聯。

AWS Management Console

請遵循《Amazon EC2 使用者指南》中的關聯彈性 IP 地址的步驟，從 IPAM 集區配置彈性 IP 地址，但請注意下列事項：當您使用 AWS 管理主控台選項時，您在 中關聯彈性 IP 地址 AWS 的區域必須符合您在步驟 2 中建立集區時所選擇的地區設定選項。

Command line

使用 associate-address 命令，建立彈性 IP 位址與 Outpost 執行個體的關聯。您在 --region 中關聯彈性 IP 位址的 --locale 選項必須與您在第 2 步中建立集區時選擇的選項相符。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

回應範例：

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的將彈性 IP 位址與執行中的執行個體或網路介面建立關聯。

第 5 步：追蹤和監控集區用量

從 IPAM 集區配置彈性 IP 位址後，您就可以追蹤和監控 IPAM 集區配置。

AWS Management Console

- 在 IPAM 主控台中檢視 IPAM 集區詳細資訊的 配置 索引標籤。從 IPAM 集區配置的任何彈性 IP 位址都具有 EIP 的 資源類型。
- 使用公共 IP 洞察功能：
  - 在公有 IP 類型下，依 Amazon 擁有的 EIP 進行篩選。這會顯示配置給 Amazon 擁有彈性 IP 位址的公有 IPv4 地址總數。如果您依此量值篩選並捲動至頁面底部的 公有 IP 位址，您會看到已配置的彈性 IP 位址。
  - 在 EIP 用量下，依關聯的 Amazon 擁有的 EIP 或未關聯的 Amazon 擁有的 EIP 進行篩選。這會顯示您在 AWS 帳戶中配置的彈性 IP 地址總數，且您已或尚未與 EC2 執行個體、網路介面或 AWS 資源建立關聯。如果您依此量值篩選並捲動至頁面底部的 公有 IP 位址，您會看到已篩選資源的詳細資訊。
  - 在 Amazon 擁有的 IPv4 連續 IP 用量下，監控一段時間內的循序公有 IPv4 地址用量，以及相關的 Amazon 擁有的 IPv4 IPAM 集區。
- 使用 Amazon CloudWatch 來追蹤和監控與已佈建至 IPAM 集區的 Amazon 提供的連續公有 IPv4 區塊相關的指標。如需針對連續 IPv4 區塊的可用指標，請參閱 IPAM 指標 下的公有 IP 指標。除了檢視指標之外，您還可以在 Amazon CloudWatch 中建立警示，以便在達到閾值時通知您。使用 Amazon CloudWatch 建立警示和設定通知不在本教學課程的範圍內。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示。

Command line

- 使用 get-ipam-pool-allocations 命令檢視 IPAM 集區配置。從 IPAM 集區配置的任何彈性 IP 位址都具有 eip 的 資源類型。

```
aws ec2 get-ipam-pool-allocations --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

回應範例：

```
{
     "IpamPoolAllocations": [
        {
            "Cidr": "18.97.0.40/32",
            "IpamPoolAllocationId": "ipam-pool-
alloc-0bd07df786e8148aba2763e2b6c1c44bd",
            "ResourceId": "eipalloc-0c9decaa541d89aa9",
            "ResourceType": "eip",
            "ResourceRegion": "us-east-1",
            "ResourceOwner": "320805250157"
        }
    ]
}
```

- 使用 Amazon CloudWatch 來追蹤和監控與已佈建至 IPAM 集區的 Amazon 提供的連續公有 IPv4 區塊相關的指標。如需針對連續 IPv4 區塊的可用指標，請參閱 IPAM 指標 下的公有 IP 指標。除了檢視指標之外，您還可以在 Amazon CloudWatch 中建立警示，以便在達到閾值時通知您。使用 Amazon CloudWatch 建立警示和設定通知不在本教學課程的範圍內。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示。

此教學課程現已完成。您已使用 Amazon 提供的連續公有 IPv4 CIDR 區塊建立 IPAM 集區、從集區配置彈性 IP 位址，並了解如何監控 IPAM 集區配置。繼續前往下一節，刪除您在本教學課程中建立的資源。

清除

請按照本節中的步驟，清除您在本教學課程中已建立的資源。

第 1 步：取消與彈性 IP 位址的關聯

完成《Amazon EC2 使用者指南》中取消彈性 IP 位址的關聯中的步驟，以取消彈性 IP 位址的關聯。

第 2 步：釋出彈性 IP 位址

完成《Amazon EC2 使用者指南》中釋出彈性 IP 位址中的步驟，從公有 IPv4 集區釋出彈性 IP 位址。

第 3 步：從 IPAM 集區取消佈建 CIDR

完成 從集區解除佈建 CIDR 中的步驟，從 IPAM 集區取消佈建 Amazon 擁有的公有 CIDR。您需要完成此步驟才能刪除集區。直到此步驟完成為止，您將需要支付 Amazon 提供的連續 IPv4 區塊的費用。

第 4 步：刪除 IPAM 集區

完成 刪除集區 中的步驟以刪除 IPAM 集區。

第 5 步：刪除 IPAM

完成 刪除 IPAM 中的步驟以刪除 IPAM。

此教學課程清除完成。

IPAM 中的 Identity and Access Management

AWS 使用安全登入資料來識別您的身分，並授予您存取 資源 AWS 的權限。您可以使用 AWS Identity and Access Management (IAM) 的功能，允許其他使用者、服務和應用程式完整或有限地使用您的 AWS 資源，而無需共用您的安全登入資料。

本節說明專為 IPAM 建立 AWS 的服務連結角色，以及連接到 IPAM 服務連結角色的受管政策。如需有關 AWS IAM 角色和政策的詳細資訊，請參閱《IAM 使用者指南》中的角色術語和概念。

如需有關 VPC 身分與存取管理的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 的身分和存取管理。

目錄

IPAM 的服務連結角色

IPAM 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是一種特殊的 IAM 角色類型。服務連結角色由 IPAM 預先定義，且內含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 IPAM 更為簡單，因為您不必手動新增必要的許可。IPAM 定義其服務連結角色的許可，除非另有定義，否則僅有 IPAM 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

服務連結角色許可

IPAM 使用 AWSServiceRoleForIPAM 服務連結角色來呼叫附加 AWSIPAMServiceRolePolicy 受管政策中的動作。如需有關該政策中允許之動作的詳細資訊，請參閱 AWS IPAM 的 受管政策。

服務連結角色亦會連接 IAM 信任政策，以允許 `ipam.amazonaws.com` 服務擔任服務連結角色。

建立服務連結角色

IPAM 會擔任帳戶中的服務連結角色、探索資源及其 CIDR，並將資源與 IPAM 整合，以監控一或多個帳戶中的 IP 地址使用情況。

有兩種建立服務連結角色的方式：

- 當您與 AWS Organizations 整合時

  如果您使用 IPAM 主控台或使用 `enable-ipam-organization-admin-account` AWS CLI 命令將 IPAM 與 AWS Organizations 中的帳戶整合，則會自動在您的每個 AWS Organizations 成員帳戶中建立 AWSServiceRoleForIPAM 服務連結角色。因此，IPAM 可以探索所有成員帳戶內的資源。

  > **Important**
  >
  > 若要讓 IPAM 代表您建立服務連結角色：
  >
  > - 啟用 IPAM 與 AWS Organizations 整合的 AWS Organizations 管理帳戶必須連接允許以下動作的 IAM 政策：
  >   - `ec2:EnableIpamOrganizationAdminAccount`
  >   - `organizations:EnableAwsServiceAccess`
  >   - `organizations:RegisterDelegatedAdministrator`
  >   - `iam:CreateServiceLinkedRole`
  > - IPAM 帳戶必須連接允許 `iam:CreateServiceLinkedRole` 動作的 IAM 政策。

- 當您使用單一 AWS 帳戶建立 IPAM 時

  如果您與單一帳戶共用 IPAM，當您建立 IPAM 作為該帳戶時，會自動建立 AWSServiceRoleForIPAM 服務連結角色。

  > **Important**
  >
  > 在您建立 IPAM 之前，如果您以單一 AWS 帳戶使用 IPAM，則必須確保您使用的 AWS 帳戶連接有允許 `iam:CreateServiceLinkedRole` 動作的 IAM 政策。當您建立 IPAM 時，您將自動建立 AWSServiceRoleForIPAM 服務連結角色。如需有關管理 IAM 政策的詳細資訊，請參閱 IAM User Guide 中的 Editing a service-linked role description。

編輯服務連結角色

您無法編輯 AWSServiceRoleForIPAM 服務連結角色。

刪除服務連結角色

如果您不再需要使用 IPAM，建議您刪除 AWSServiceRoleForIPAM 服務連結角色。

> **Note**
>
> 只有在刪除您的 AWS 帳戶中的所有 IPAM 資源之後，您才可以刪除服務連結角色。這可確保您不會無意中移除 IPAM 的監控功能。

請依照下列步驟，使用 AWS CLI 刪除服務連結角色：

1. 使用 deprovision-ipam-pool-cidr 和 delete-ipam 刪除 IPAM 資源。如需詳細資訊，請參閱從集區解除佈建 CIDR及 刪除 IPAM。
2. 使用 disable-ipam-organization-admin-account 停用 IPAM 帳戶。
3. 使用 disable-aws-service-access 和 `--service-principal ipam.amazonaws.com` 選項停用 IPAM 服務。
4. 刪除服務連結角色：delete-service-linked-role。刪除服務連結角色時，也會一併刪除 IPAM 受管政策。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS IPAM 的 受管政策

如果您使用 IPAM 搭配單一 AWS 帳戶並建立 IPAM，則 AWSIPAMServiceRolePolicy 受管政策會自動在您的 IAM 帳戶中建立，並連接到 AWSServiceRoleForIPAM 服務連結角色。

如果您啟用 IPAM 與 AWS Organizations 整合，AWSIPAMServiceRolePolicy 受管政策會自動在您的 IAM 帳戶和每個 AWS Organizations 成員帳戶中建立，且受管政策會連接至 AWSServiceRoleForIPAM 服務連結角色。

此受管政策可讓 IPAM 執行以下操作：

- 監控 AWS 組織所有成員之間與聯網資源相關聯的 CIDRs。
- 將與 IPAM 相關的指標 (例如 IPAM 集區中可用的 IP 地址空間以及符合配置規則的資源 CIDR 數目等) 存放在 Amazon CloudWatch 中。
- 修改與讀取受管字首清單。

下例顯示建立之受管政策的詳細資訊。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "IPAMDiscoveryDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:ListByoipCidrs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsPublishActions",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

上述範例中的第一個陳述式可讓 IPAM 監控單一 AWS 帳戶或 AWS 組織成員所使用的 CIDRs。

上例中的第二個陳述式使用 `cloudwatch:PutMetricData` 條件金鑰允許 IPAM 將 IPAM 指標存放在 `AWS/IPAM` Amazon CloudWatch 命名空間中。這些指標由 用來 AWS 管理主控台 顯示 IPAM 集區和範圍中配置的資料。如需詳細資訊，請參閱使用 IPAM 儀表板監控 CIDR 使用情況。

AWS 受管政策的更新

檢視自此服務開始追蹤這些變更以來 IPAM AWS 受管政策更新的詳細資訊。

變更	描述	Date
AWSIPAMServiceRolePolicy	新增至 AWSIPAMServiceRolePolicy 受管政策 (ec2:ModifyManagedPrefixList、ec2:DescribeManagedPrefixLists 和 ec2:GetManagedPrefixListEntries) 的動作讓 IPAM 能夠修改與讀取受管字首清單。	2025 年 10 月 31 日
AWSIPAMServiceRolePolicy	新增至 AWSIPAMServiceRolePolicy 受管政策 (`organizations:ListChildren` `organizations:ListParents` 、和 `organizations:DescribeOrganizationalUnit`) 的動作，可讓 IPAM	2024 年 11 月 21 日

變更	描述	Date
	取得 AWS Organizations 中組織單位 (OUs) 的詳細資訊，讓客戶可以在 OU 層級使用 IPAM。	
AWSIPAMServiceRolePolicy	動作已新增至 AWSIPAMServiceRolePolicy 受管政策 (`ec2:GetIpamDiscoveredPublicAddresses`)，可讓 IPAM 在資源探索期間取得公有 IP 地址。	2023 年 11 月 13 日
AWSIPAMServiceRolePolicy	動作已新增至 AWSIPAMServiceRolePolicy 受管政策 (`ec2:DescribeAccountAttributes` 、`ec2:DescribeNetworkInterfaces` 、`ec2:DescribeSecurityGroups` 、`ec2:DescribeSecurityGroupRules` 、`ec2:DescribeVpnConnections` 、`globalaccelerator:ListAccelerators` 及 `globalaccelerator:ListByoipCidrs`)，可讓 IPAM 在資源探索期間取得公有 IP 地址。	2023 年 11 月 1 日

變更	描述	Date
AWSIPAMServiceRolePolicy	新增至 AWSIPAMServiceRolePolicy 受管政策 (`ec2:GetIpamDiscoveredAccounts` 和 `ec2:GetIpamDiscoveredResourceCidrs`) 的兩個動作，可讓 IPAM 在資源探索期間取得受監控 AWS 的帳戶和資源 CIDRs。	2023 年 1 月 25 日
IPAM 開始追蹤變更	IPAM 開始追蹤其 AWS 受管政策的變更。	2021 年 12 月 2 日

範例 政策

本節中的範例政策包含完整 IPAM 用量的所有相關 AWS Identity and Access Management (IAM) 動作。視您使用 IPAM 的方式而定，您可能不需要包含所有 IAM 動作。如需使用 IPAM 主控台的完整體驗，您可能需要為 服務包含其他 IAM 動作 AWS Organizations，例如 AWS Resource Access Manager (AWS RAM) 和 Amazon CloudWatch。

JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIpamByoasn",
                "ec2:DeprovisionIpamByoasn",
                "ec2:DescribeIpamByoasn",
                "ec2:DisassociateIpamByoasn",
                "ec2:ProvisionIpamByoasn",
                "ec2:CreateIpam",
                "ec2:DescribeIpams",
                "ec2:ModifyIpam",
```

```
                "ec2:DeleteIpam",
                "ec2:CreateIpamScope",
                "ec2:DescribeIpamScopes",
                "ec2:ModifyIpamScope",
                "ec2:DeleteIpamScope",
                "ec2:CreateIpamPool",
                "ec2:DescribeIpamPools",
                "ec2:ModifyIpamPool",
                "ec2:DeleteIpamPool",
                "ec2:ProvisionIpamPoolCidr",
                "ec2:GetIpamPoolCidrs",
                "ec2:DeprovisionIpamPoolCidr",
                "ec2:AllocateIpamPoolCidr",
                "ec2:GetIpamPoolAllocations",
                "ec2:ReleaseIpamPoolAllocation",
                "ec2:CreateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveries",
                "ec2:ModifyIpamResourceDiscovery",
                "ec2:DeleteIpamResourceDiscovery",
                "ec2:AssociateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveryAssociations",
                "ec2:DisassociateIpamResourceDiscovery",
                "ec2:GetIpamResourceCidrs",
                "ec2:ModifyIpamResourceCidr",
                "ec2:GetIpamAddressHistory",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ipam.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

IPAM 的配額

本節列出 IPAM 的相關配額。Service Quotas 主控台亦載明有關 IPAM 配額的資訊。您可以使用 Service Quotas 主控台來檢視預設配額，並對可調整的配額請求提高配額。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的請求提高配額。

Name	預設	可調整
Amazon 提供的連續公有 IPv4 CIDR 區塊	2	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
Amazon 提供的連續公有 IPv4 CIDR 區塊	/29	可接受的大小介於 /29 和 /30 之間。若要請求增加，請聯絡 AWS Support Center，如中的AWS 服務配額中所述AWS 一般參考。
Amazon 提供的 IPv6 CIDR 區塊網路遮罩長度	/52	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
每個區域集區的 Amazon 提供的 IPv6 CIDR 區塊	1	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
可帶入 IPAM 的自治系統編號 (ASN)	5	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
每個集區的 CIDR 數目	50	是

Name	預設	可調整
每個 IPAM 政策啟用的目標數	100	是。若要請求調整配額，請聯絡 AWS Support Center，如中的AWS 服務配額中所述AWS 一般參考。
每個組織的 IPAM 管理員	1	否
每個區域的 IPAM	1	否
每個 IPAM 的 IPAM 政策	10	是。若要請求調整配額，請聯絡 AWS Support Center，如中的AWS 服務配額中所述AWS 一般參考。
每個資源區域配對的 IPAM 政策配置規則*	10	是。若要請求調整配額，請聯絡 AWS Support Center，如中的AWS 服務配額中所述AWS 一般參考。
每個資源探索的組織單位排除	10	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
集區深度 (集區層數)	10	是
每個範圍的集區數目	50	是
每個 IPAM 的字首清單解析程式數量	10	是
每個字首清單解析程式的字首清單解析程式目標數量	50	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。

Name	預設	可調整
每個字首清單解析程式的規則數量	100	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
每個字首清單解析程式版本的 CIDR 項目數量	1000	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
每個 IPAM 的資源探索關聯	5	是
每個區域的資源探索	1	否
資源使用率指標	50	是。如 中的AWS 服務配額所述，聯絡 AWS 支援中心AWS 一般參考。
每個 IPAM 的範圍	5	是。建立 IPAM 時，會為您建立一個私有和一個公有預設範圍。如果要建立其他範圍，它們將是私有範圍。您無法建立其他的公有範圍。

* 資源-地區設定對：設定配置規則時，您必須同時指定資源類型 (EIPs、ALBs 或 RDS 叢集等 AWS 資源） 和地區設定 （套用規則的區域 AWS 或本機區域）。配置規則的範圍限定於此資源類型和地區設定組合。例如，如果您要在 us-east-1 中為 EIPs 設定政策，您可以為該特定資源區域設定最多 10 個規則*。

IPAM 定價

Amazon VPC IP Address Manager (IPAM) 是一項服務，可協助您跨 AWS 資源和內部部署網路管理 IP 地址空間。IPAM 提供集中式方法來規劃、監控和控制 AWS 和內部部署資源所使用的 IP 地址。

本節描述如何檢視與定價相關的資訊和您目前的 IPAM 成本。

目錄

檢視定價資訊

IPAM 提供兩種方案：免費和進階方案。如需每個方案中的可用功能以及方案關聯成本的詳細資訊，請參閱 Amazon VPC 定價頁面中的 IPAM 索引標籤。

使用 檢視您目前的成本和用量 AWS Cost Explorer

使用 IPAM 進階方案時，您會依照 IPAM 管理的作用中 IP 地址來支付每小時費率。如果您要檢視和分析 IPAM 成本與用量，可以使用 AWS Cost Explorer。

1. 在 https：//https://console.aws.amazon.com/cost-management/home 開啟 AWS Cost Management 主控台。
2. 選擇 Cost Explorer。
3. 選擇用量型態並輸入 **`IPAddressManager`**，藉此篩選 IPAM 用量。
4. 選取一或多個核取方塊。每個區域都代表不同的 AWS 區域。
5. 按一下 Apply (套用)。

舉例來說，如果您選取 USE1-IPAddressManager-IP-Hours(Hrs) 並且 us-east-1 是您的 IPAM 主區域，您會看見依照所有區域中的 IPAM 計費的作用中 IP 時數和成本。例如，假設以小時為單位的用量為 18，則表示您可以擁有 1 個作用中 IP 位址 18 個小時、3 個 IP 位址，每個在 3 個不同區域中可作用 6 個小時，或者這些 IP 位址的任何組合，只要其總計達 18 個小時即可。

如需 的詳細資訊 AWS Cost Explorer，請參閱AWS Cost Management 《 使用者指南》中的使用 分析您的成本 AWS Cost Explorer。

相關資訊

雖然 AWS 技術文件網站是全方位的資源，但還有許多地方可以尋找 AWS 服務的相關資訊。AWS 部落格、白皮書、案例研究和社群論壇可以提供重要的洞見、實際範例，以及官方技術詳細資訊以外的替代觀點。探索這些多樣化來源可讓您更全面地了解 AWS 產品。

以下相關資源可協助您使用 Amazon VPC IP Address Manager:

- Amazon VPC IP Address Manager Best Practices (Amazon VPC IP 地址管理員最佳實務)：有關透過 Amazon VPC IP 地址管理員規劃和建立可擴展地址配置的最佳實務的 AWS 部落格。
- Network Address Management and Auditing at Scale with Amazon VPC IP Address Manager (透過 Amazon VPC IP 地址管理員進行大規模的網路位址管理和稽核)：介紹 Amazon VPC IP 地址管理員以及如何在 AWS 主控台中使用該服務的 AWS 部落格。
- 對使用 AWS Resource Access Manager 共用的資源設定精細存取：一個 AWS 部落格，它說明了如何與 AWS Organizations 組織單位中的帳戶共用 IPAM 集區。
- 使用 CIDR 映射視覺化企業 IP 位址管理和規劃：AWS 部落格，介紹如何使用 IPAM 主控台中的 IPAM CIDR 映射視覺化整個 IPv4 和 IPv6 環境。

IPAM 的文件歷史紀錄

下表說明 IPAM 的各個版本。

功能	Description	版本日期
使用 IPAM 將您自己的 IP 帶到 CloudFront	使用 IPAM 來管理 AWS 全球服務的 BYOIP CIDRs，從 CloudFront anycast 服務開始。	2025 年 11 月 21 日
使用 IPAM 政策定義公有 IPv4 配置策略	您現在可以使用 IPAM 政策來定義將 AWS 服務映射至特定 IPAM 集區的規則，協助定義公有 IPv4 配置策略。	2025 年 11 月 19 日
整合 IPAM 與 Infoblox 基礎設施	您現在可以將 IPAM 與 Infoblox 基礎設施整合，讓您能夠透過現有的 Infoblox 工作流程管理 AWS IP 地址，同時獲得雲端原生 AWS 功能。此整合適用於私有範圍，且需要 IPAM 進階層。	2025 年 11 月 7 日
自動更新字首清單	您現在可以使用 IPAM 字首清單解析程式，根據 IPAM 集區 CIDR 自動更新字首清單。	2025 年 10 月 31 日
在 IPAM 主控台中管理警示	您現在可以直接在 IPAM 主控台中建立和管理 Amazon CloudWatch 警示。IPAM 相關警示會在處於 INSUFFICIENT_DATA 或 ALARM 狀態時顯示為警告列和視覺化指示器。	2025 年 8 月 21 日
啟用成本分配	啟用成本分配後，作用中 IP 位址的費用將分配給使用這些 IP 位址的帳戶，而不是 IPAM 擁有者。這對於委派 IPAM 管理員使用 IPAM 集中管理 IP 位址的大型組織很有用，每個帳戶都負責自己的使用量，因此不需要手動計算帳單費用。	2025 年 5 月 1 日
從 IPAM 排除組織單位	如果您的 IPAM 已與 AWS Organizations 整合，您現在可以從 IPAM 中排除組織單位。IPAM 不會管理組織單位排除中帳戶的 IP 位址。	2024 年 11 月 21 日
AWS 受管政策更新 - 更新現有政策	現有 AWSIPAMServiceRolePolicy 已更新。	2024 年 11 月 21 日

功能	Description	版本日期
從 IPAM 集區配置循序彈性 IP 位址	IPAM 現在可讓您將 Amazon 擁有的公有 IPv4 區塊佈建至 IPAM 集區，並將這些集區的循序彈性 IP 地址配置至 AWS 資源。循序彈性 IP 位址可以幫助您簡化網路和安全白名單的需求。	2024 年 8 月 28 日
私有 IPv6 GUA 和 ULA	您現在可以將私有 IPv6 GUA 和 ULA 範圍佈建至私有範圍內的 IPAM 集區。私有 IPv6 地址僅適用於 IPAM。如需有關公有和私有 IPv6 定址的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 私有 IPv6 地址。	2024 年 8 月 8 日
IPAM 免費和進階方案	現在可以為 IPAM 選擇免費方案和進階方案。	2023 年 11 月 17 日
公有 IP 深入解析	以前，您只能在單一區域中檢視公共 IP 洞察功能。現在可以跨區域檢視公共 IP 洞察功能。此外，現在可以檢視 Amazon CloudWatch 中的公共 IP 地址洞察功能。	2023 年 11 月 17 日
為子網路 IP 配置規劃 VPC IP 地址空間	您現在可以使用 IPAM 規劃 VPC 內的子網路 IP 空間，並在子網路和 VPC 層級監控 IP 地址相關指標。	2023 年 11 月 17 日
使用自有 ASN (BYOASN)	您現在可以將自己的自治系統編號 (ASN) 帶入其中 AWS。	2023 年 11 月 17 日
AWS 受管政策更新 - 更新現有政策	現有 AWSIPAMServiceRolePolicy 已更新。	2023 年 11 月 17 日
AWS 受管政策更新 - 更新現有政策	現有 AWSIPAMServiceRolePolicy 已更新。	2023 年 11 月 1 日
資源使用率指標	IPAM 現在會將 IPAM 監控之資源的 IP 使用率指標發佈至 Amazon CloudWatch。	2023 年 8 月 2 日

功能	Description	版本日期
公有 IP 深入解析	公有 IP 深入解析會顯示您帳戶中此區域服務所使用的所有公有 IPv4 地址。您可以使用這些深入解析來識別公有 IPv4 地址使用情況，並檢視釋出未使用之彈性 IP 地址的建議。	2023 年 7 月 28 日
AWS 受管政策更新 - 更新現有政策	現有 AWSIPAMServiceRolePolicy 已更新。	2023 年 1 月 25 日
將 IPAM 與組織外的帳戶整合	您現在可以從單一 IPAM 帳戶管理組織外部的 IP 地址，並與其他 AWS Organizations 帳戶共用 IPAM 集區。	2023 年 1 月 25 日
Amazon 為 IPAM 集區提供的 IPv6 連續 CIDR 區塊	在公有範圍中建立 IPAM 集區時，現在可將 Amazon 提供的 IPv6 連續 CIDR 區塊佈建至集區。如需詳細資訊，請參閱在 IPAM 中建立 IPv6 地址集區。	2023 年 1 月 25 日
初始版本	此版本介紹了 Amazon VPC IP 地址管理員。	2021 年 12 月 2 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。