



IP 地址管理員

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: IP 地址管理員

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

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

Table of Contents

什麼是 IPAM？	1
IPAM 的運作方式	2
IPAM 入門	3
存取 IPAM	3
設定 IPAM 的許可	4
將 IPAM 與組 AWS 織中的帳戶整合	4
將 IPAM 與組織外的帳戶整合	7
與單一帳戶共用 IPAM	8
建立 IPAM	9
規劃 IP 地址佈建	11
IPAM 集區計畫範例	12
建立 IPv4 集區	14
建立 IPv6 集區	22
配置 CIDR	28
建立使用 IPAM 集區 CIDR 的 VPC	28
手動將 CIDR 配置給集區，以保留 IP 地址空間	29
管理 IPAM 中的 IP 地址空間	31
強制使用 IPAM 建立 VPC	31
強制使用 IPAM 建立 VPC	32
強制使用 IPAM 集區建立 VPC	32
針對指定 OU 清單以外的所有 OU 強制執行 IPAM	33
透過 AWS RAM 共用 IPAM 集區	34
佈建集區的 CIDR	36
從集區解除佈建 CIDR	37
編輯集區	38
刪除集區	39
使用資源探索	40
建立資源探索	40
檢視資源探索詳細資訊	41
共用資源探索	43
將資源探索與 IPAM 建立關聯	45
取消關聯資源探索	46
刪除資源探索	47
建立其他範圍	47

在各範圍之間移動 VPC CIDR	48
變更 VPC CIDR 的監控狀態	50
刪除範圍	51
釋出配置	52
修改 IPAM	54
修改 IPAM 方案	54
修改 IPAM 作業區域	55
刪除 IPAM	56
追蹤 IPAM 中的 IP 地址使用情況	58
使用 IPAM 儀表板監控 CIDR 使用情況	58
依資源監控 CIDR 使用情況	60
使用 Amazon CloudWatch 監控 IPAM	63
IPAM 集區和範圍指標	63
資源使用率指標	65
檢視 IP 地址歷程記錄	70
檢視公有 IP 深入解析	73
教學課程	77
使用主控台建立 IPAM 和集區	77
先決條件	78
AWS Organizations 如何與 IPAM 整合	78
步驟 1：委派 IPAM 管理員	79
步驟 2：建立 IPAM	80
步驟 3：建立最上層 IPAM 集區	83
步驟 4：建立區域 IPAM 集區	88
步驟 5：建立生產前開發集區	92
步驟 6：共用 IPAM 集區	96
步驟 7：使用從 IPAM 集區配置的 CIDR 建立 VPC	101
步驟 8：清除	105
使用 AWS CLI 建立 IPAM 和集區	106
步驟 1：在您的組織中啟用 IPAM	107
步驟 2：建立 IPAM	108
步驟 3：建立 IPv4 地址集區	110
步驟 4：在最上層集區佈建 CIDR	111
步驟 5. 利用最上層集區中的 CIDR 建立區域集區	112
步驟 6：在區域集區中佈建 CIDR	114
步驟 7. 建立 RAM 共用以啟用跨帳戶的 IP 指派	116

步驟 8. 建立 VPC	117
步驟 9. 清除	117
使用 AWS CLI 檢視 IP 地址歷程記錄	118
概要	118
案例	119
將 ASN 帶入 IPAM	126
ASN 加入先決條件	127
教學步驟	127
將 IP 地址帶入 IPAM	131
AWS 主控台和 CLI	132
AWS 僅限 CLI	154
將 BYOIP IPv4 CIDR 傳輸至 IPAM	195
步驟 1：建立 AWS CLI 命名的設定檔和 IAM 角色	195
步驟 2：取得您 IPAM 的公有範圍 ID	196
步驟 3：建立 IPAM 集區	197
步驟 4：使用分享 IPAM 集區 AWS RAM	198
步驟 5：將現有的 BYOIP IPV4 CIDR 傳輸至 IPAM	201
步驟 6：檢視 IPAM 中的 CIDR	203
步驟 7：清除	204
為子網路 IP 配置規劃 VPC IP 地址空間	207
步驟 1：建立 VPC	208
步驟 2：建立資源規劃集區	209
步驟 3：建立子網路集區	209
步驟 4：建立子網路	210
步驟 5：清除	211
IPAM 中的 Identity and Access Management	212
IPAM 的服務連結角色	212
授予服務連結角色的許可	212
建立服務連結角色	212
編輯服務連結角色	213
刪除服務連結角色	213
IPAM 的受管政策	214
AWS 受管政策更新	216
範例 政策	217
配額	219
定價	221

檢視定價資訊	221
以下列方式檢視目前的成本和用量 AWS Cost Explorer	221
相關資訊	222
文件進版記錄	223
.....	CCXXV

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

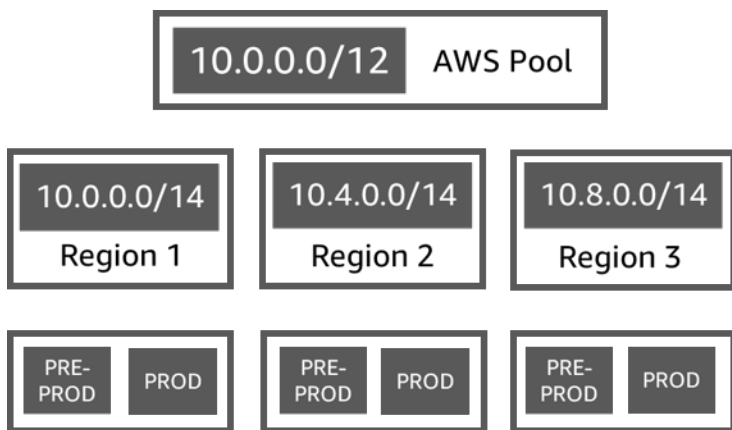
本指南涵蓋下列章節：

- [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。IPAM 包含兩個預設範圍。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。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 可以管理和監控您擁有的私有 IPv4 CIDR 和公有 IPv4/IPv6 CIDR 以及 Amazon 擁有的公有 IPv6 空間。

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。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。

內容

- [存取 IPAM](#)
- [設定 IPAM 的許可](#)
- [建立 IPAM](#)
- [規劃 IP 地址佈建](#)
- [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 命令列介面 (AWS CLI)：提供適用於各種 AWS 服務 (包含 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個描述中，我們都會包含指向 AWS CLI 文件的連結，該文件會介紹如何使用 AWS CLI 來完成相同的操作。

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 的許可](#) 中的指示。

設定 IPAM 的許可

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 與組 AWS 織中的帳戶整合](#)。
- 與整合之後 AWS Organizations，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)，但無法在儀表中看見指標，也無法監控資源的狀態。

目錄

- [將 IPAM 與組 AWS 織中的帳戶整合](#)
- [將 IPAM 與組織外的帳戶整合](#)
- [與單一帳戶共用 IPAM](#)

將 IPAM 與組 AWS 織中的帳戶整合

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 Organizations 整合並委派 IPAM 管理員具有 AWS 以下優點：

- 與您的組織共用 IPAM 集區：當您委派 IPAM 帳戶時，IPAM 可讓組 Organ AWS izations 中的其他組織成員帳戶從使用 AWS Resource Access Manager (RAM) 共用的 IPAM 集區配置 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 會自動將其他 Organizations 成員帳戶中現有 VPC 所使用的 CIDR 匯入 IP AWS AM。

如果您未將 Organ AWS izations 成員帳戶委派為 IPAM 帳戶，IPAM 只會監視您用來建立 IPAM 的 AWS 帳戶中的資源。

⚠ Important

- 您必須在 AWS 管理主控台中使用 IPAM 或 [enable-ipam-organization-admin-account](#) AWS CLI 命令來啟用與 Organizations AWS 織的整合。此可確保建立了 AWSServiceRoleForIPAM 服務連結角色。如果您使用 Organization 主控台或 [register-delegated-administrator](#) AWS CLI 命令啟用組 Organ AWS izations 的受信任存取，則不會建立 AWSServiceRoleForIPAM 服務連結角色，而且您無法管理或監視組織內的資源。
AWS

ℹ Note

與 Organizations 整合 AWS 時：

- 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「Organ AWS izations」中擁有帳戶，且管理帳戶必須設定一或多個成員帳戶。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 帳戶必須是組 Organ AWS izations 成員帳戶。您無法使用 AWS Organizations 管理帳戶作為 IPAM 帳戶。
- IPAM 帳戶使用的 IAM 角色所連接的 IAM 政策必須允許 iam:CreateServiceLinkedRole 動作。建立 IPAM 時，您會自動建立 AWSServiceRoleForIPAM 服務連結角色。
- 與 Organ AWS izations 管理帳戶關聯的使用者必須使用附加下列 IAM 政策動作的 IAM 角色：
 - 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 Organ AWS izations 管理帳戶關聯的使用者可以使用 IAM 角色，該角色附加了下列 IAM 政策動作，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 Organ AWS izations 管理帳戶，開啟 IPAM 主控台，網址為 <https://console.aws.amazon.com/ipam/>。
2. 在 AWS 管理主控台中，選擇您要使用 IPAM 的 AWS 區域。
3. 在導覽窗格中，選擇 Organization settings (組織設定)。
4. 只有當您 Organ AWS izations 管理帳戶的身分登入主控台時，才能使用 [委派] 選項。選擇委派。
5. 輸入 IPAM AWS 帳戶的帳戶識別碼。IPAM 管理員必須是組 Organ AWS izations 成員帳戶。
6. 選擇儲存變更。

Command line

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

- [若要使用委派 IPAM 管理員帳戶 AWS CLI，請使用下列命令：`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 AWS Organizations 管理員的管理帳戶角色現在已完成。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 與組織中的帳戶整合](#) 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。

內容

- [考量與限制](#)
- [程序概觀](#)

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 與組 AWS 織中的帳戶整合](#))。
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 與組 AWS 織中的帳戶整合](#))。
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](#) 和 [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 與組 AWS 織中的帳戶整合](#)，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 中為 Amazon VPC IPAM 服務建立服務連結角色。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 (從成員帳戶到委派的 IPAM 成員帳戶) 和跨 AWS 區域 (從作業區域到 IPAM 的主區域) 複寫資源和 IP 使用詳細資訊。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，請選擇允許 IPAM 管理 IP 地址 CIDR 的 AWS 區域。這些 AWS 區域稱為「作業區域」。IPAM 僅會在您選取作為作業區域的 AWS 區域中探索並監控資源。IPAM 不會在您選取的作業區域之外存放任何資料。

下列範例階層會顯示您在建立 IPAM 時指派的 AWS 區域將會影響稍後建立集區的可用區域。

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
 - 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，選擇欲建立 IPAM 的 AWS 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製到 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。依預設，您要在其中建立 IPAM 的 AWS 區域會被選為其中一個作業區域。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 Create IPAM (建立 IPAM)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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、修改和檢視與 IPAM 相關的詳細資訊：

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。集區建立程序對於公用和私有範圍中的集區而言是不同的。本節包括在私有範圍中建立地區集區的步驟。如需自攜 IP 和自攜自學課程，請參閱 [〈〉](#)。[教學課程](#)

Important

若要跨 AWS 帳戶使用 IPAM 集區，您必須將 IPAM 與 Organ AWS izations 整合，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 與組 AWS 織中的帳戶整合](#)。

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。您可以為 IPAM 區 AWS 域以外的區域建立集區。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 在 AWS 區域 1 和 AWS 區域 2 運作
 - 私有範圍

- 最上層集區
 - AWS 區域 1 的區域泳池
 - 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 [配置 CIDR](#)。

目錄

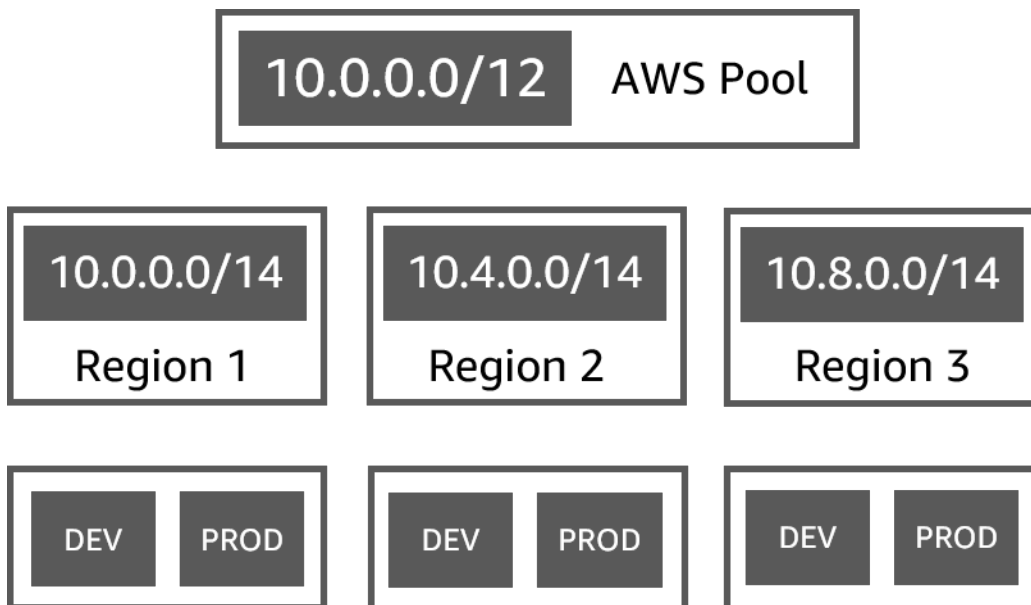
- [IPAM 集區計畫範例](#)
- [建立 IPv4 集區](#)
- [建立 IPv6 集區](#)

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。

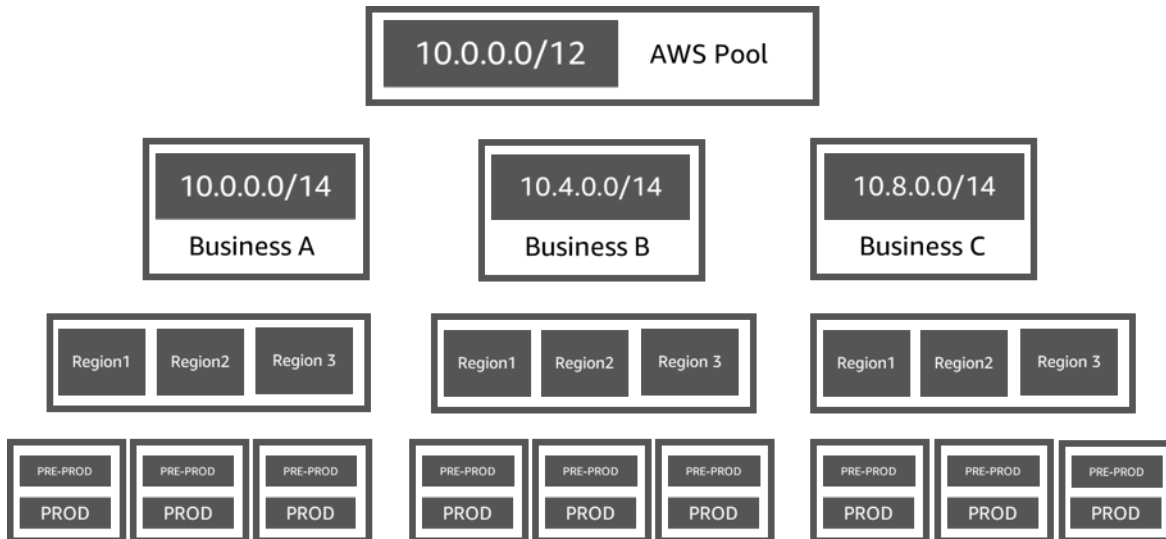
多個 AWS 區域中的 IPv4 集區

下例顯示的 IPAM 集區階層跨最上層集區內的多個 AWS 區域。每個 AWS 區域集區內都有兩個 IPAM 開發集區，一個是用於開發資源的集區，另一個是用於生產資源的集區。



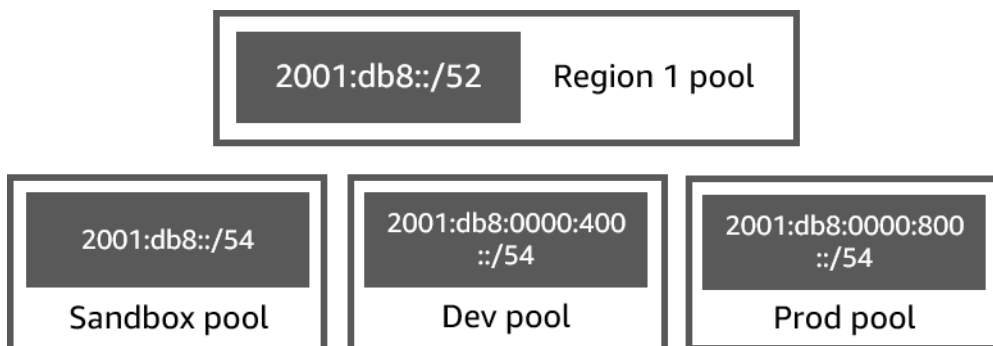
多個業務單位的 IPv4 集區

下例顯示的 IPAM 集區階層跨最上層集區內的多個業務單位。每個業務單位的各個集區都有三個 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。



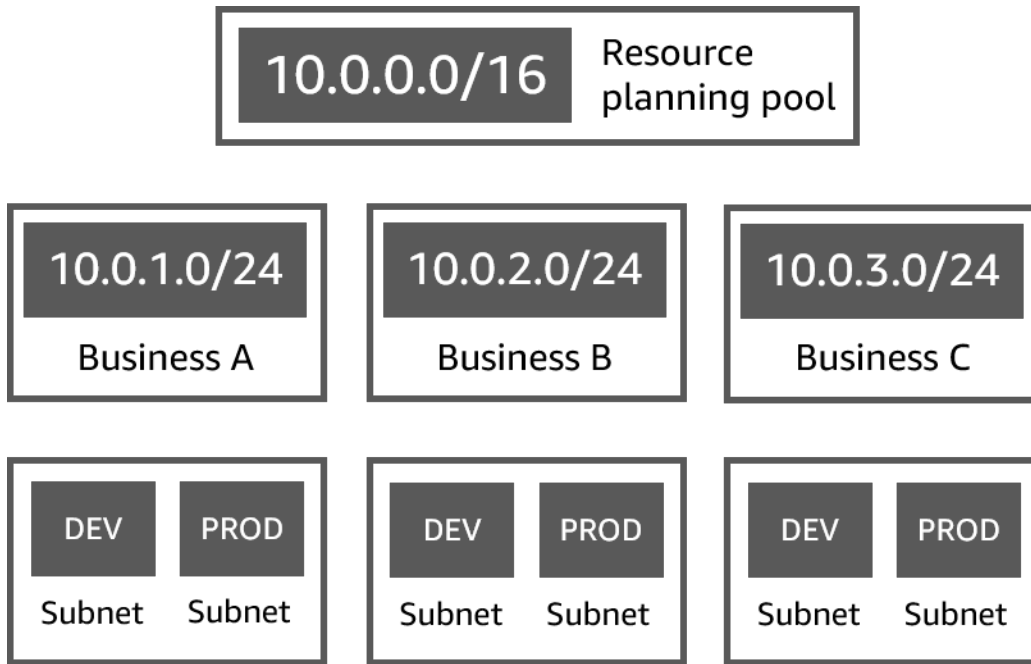
AWS 區域中的 IPv6 集區

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。

內容

- [建立頂層 IPv4 集區](#)
- [建立區域 IPv4 集區](#)
- [建立開發 IPv4 集區](#)

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：

- 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。

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。地區設定為 IPAM 集區可供配置使用的 AWS 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 IPAM 集區，且此集區為 AWS Resource Access Manager (RAM) 中的共享資源，則資源擁有者必須設定為 AWS RAM 中的委託人。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，如果空間可用，仍可使用大於 /24 的 CIDR 從此集區建立資源，但是因為這樣做會違反集區上的配置規則，IPAM 會將此資源標記為不合規。

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)，則有一些先決條件。如需更多詳細資訊，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 Create pool (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。

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，則有一些先決條件。如需更多詳細資訊，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 的資源所需的地区設定。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. 選擇 Create pool (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 參考文件連結。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[配置 CIDR](#)。

Note

集區建立程序對於公用和私有範圍中的集區而言是不同的。本節包括在私有範圍中建立地區集區的步驟。如需自攜 IP 和自攜自學課程，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 在 AWS 區域 1 和 AWS 區域 2 運作
 - 私有範圍
 - 最上層集區 (10.0.0.0/8)

- 在第一區域的 AWS 區域泳池 (10.0.0/16)
 - 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. 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。

AWS 地區設定是您希望此 IPAM 集區可供配置使用的區域。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](#)。

9. (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。

10. 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。
11. (選用) 為集區選擇 Tags (標籤)。
12. 當您完成集區的設定後，請選擇 Create pool (建立集區)。
13. 請參閱 [建立開發 IPv4 集區](#)。

Command line

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

使用下列 AWS CLI 命令在 IPAM 中建立地區集區：

1. 獲取要在其中創建池的範圍的 ID：[describe-ipam-scopes](#)
2. 獲取您要在其中創建池的池的 ID：[describe-ipam-pools](#)
3. 建立集區：[create-ipam-pool](#)
4. 檢視新儲存池：[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 [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 Create pool (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 [配置 CIDR](#)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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。

建立 IPv6 集區

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。

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
 - 公有範圍
 - 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)

內容

- [建立區域 IPv6 集區](#)
- [建立開發 IPv6 集區](#)

建立區域 IPv6 集區

請依照本節中的步驟來建立 IPv6 區域 IPAM 集區。將 Amazon 提供的 IPv6 CIDR 區塊佈建至集區時，必須將其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：

- IPAM 執行於 AWS 區域 1 和 AWS 區域 2
 - 公有範圍

- 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。地區設定為 IPAM 集區可供配置使用的 AWS 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 IPAM 集區，且此集區為 AWS Resource Access Manager (RAM) 中的共享資源，則資源擁有者必須設定為 AWS RAM 中的委託人。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。

Important

本主題說明如何使用 AWS 提供的 IP 地址範圍建立 IPv6 區域集區。如果您想要將自己的 IPv4 或 IPv6 IP 地址範圍帶到 AWS (BYOIP)，則有一些先決條件。如需更多詳細資訊，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 Create pool (建立集區)。
4. 在 IPAM 範圍下，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](#)。

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 AWS 可以或當前在網際網路上發佈廣告的所有空間。

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. 針對地址系列，選取 IPv6。則會顯示允許此集區中的 CIDR 可公開公告。依預設，此集區中的所有 CIDR 都將公開公告。無法啟用或停用此選項。
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。將 Amazon 提供的 IPv6 CIDR 區塊佈建至集區時，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. 在 Service (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. 在公有 IP 來源選項下，選擇 Amazon 擁有，可讓 AWS 為此集區提供 IPv6 地址範圍。如本頁面頂部所述，本主題說明如何使用 AWS 提供的 IP 地址範圍建立 IPv6 區域集區。如果您想要將自己的 IPv4 或 IPv6 地址範圍帶到 AWS (BYOIP)，則有一些先決條件。如需更多詳細資訊，請參閱 [教學課程：將 IP 地址帶入 IPAM](#)。
12. 對於公有範圍中使用公有 IP 來源 BYOIP 的集區，您可以控制 AWS 是否可以使用 Allow CIDRs in this pool to be publicly advertisable (允許此集區中的 CIDR 公開公告)，公開公告此集區中的 CIDR。此選項預設為啟用。如果您不想允許 AWS 公開公告此集區中的 CIDR，請停用此選項。
13. (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 Amazon 擁有的 CIDR，然後為 CIDR 選擇介於 /40 和 /52 之間的網路遮罩大小。

 Note

注意下列事項：

- 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](#)。
- 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。

14. 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。
15. (選用) 為集區選擇 Tags (標籤)。
 16. 選擇 Create pool (建立集區)。
 17. 請參閱[建立開發 IPv6 集區](#)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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 IPv6 區域集區：

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](#)。

建立開發 IPv6 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[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
 - 公有範圍
 - 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 Create pool (建立集區)。
4. 在 IPAM 範圍下，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](#)。

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 AWS 可以或當前在網際網路上發佈廣告的所有空間。

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 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 [建立區域 IPv6 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 [配置 CIDR](#)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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。

配置 CIDR

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 整合的 AWS 服務 (例如 Amazon VPC)，然後選取將 IPAM 集區用於 CIDR 的選項。IPAM 會自動在集區中為您建立配置。
- 在 IPAM 集區內手動配置 CIDR，將其保留以便日後和與 IPAM 整合的 AWS 服務一起使用，例如 Amazon VPC。

本節會逐步說明這兩個選項：如何使用與 IPAM 整合的 AWS 服務來佈建 IPAM 集區 CIDR，以及如何手動保留 IP 地址空間。

內容

- [建立使用 IPAM 集區 CIDR 的 VPC](#)
- [手動將 CIDR 配置給集區，以保留 IP 地址空間](#)

建立使用 IPAM 集區 CIDR 的 VPC

請依照《Amazon VPC 使用者指南》中[建立 VPC](#)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。

建立 VPC 時，如果您選擇使用 IPAM 集區的選項，則 AWS 會在 IPAM 集區中配置 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 AWS CLI (包括建立 VPC) 的完整說明，請參閱 [Amazon VPC IP 地址管理員教學課程](#) 章節。

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 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 參考文件連結。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 配置給集區：

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。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

- [強制使用 IPAM 建立 VPC](#)
- [透過 AWS RAM 共用 IPAM 集區](#)
- [佈建集區的 CIDR](#)
- [從集區解除佈建 CIDR](#)
- [編輯集區](#)
- [刪除集區](#)
- [使用資源探索](#)
- [建立其他範圍](#)
- [在各範圍之間移動 VPC CIDR](#)
- [變更 VPC CIDR 的監控狀態](#)
- [刪除範圍](#)
- [釋出配置](#)
- [修改 IPAM](#)
- [刪除 IPAM](#)

強制使用 IPAM 建立 VPC

Note

本節僅適用於已啟用 IPAM 且使其與 AWS Organizations 整合的情況下。如需更多詳細資訊，請參閱 [將 IPAM 與組 AWS 組織中的帳戶整合](#)。

本節說明如何在 AWS Organizations 中建立服務控制政策，該政策可要求您組織中的成員使用 IPAM 建立 VPC。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. 請依照《AWS Organizations 使用者指南》中[建立 SCP](#)的步驟進行操作，在 JSON 編輯器中輸入以下文字：

```
{
  "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[連接和分離服務控制政策](#)。

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. 請依照 AWS Organizations 使用者指南中[建立 SCP](#)的步驟進行操作，在 JSON 編輯器中輸入以下文字：

```
{
  "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[連接和分離服務控制政策](#)。

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。本節中說明的政策要求組織中的 OU (除了您在 aws:PrincipalOrgPaths 中指定的 OU 以外) 使用 IPAM 建立和擴充 VPC。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. 請依照《AWS Organizations 使用者指南》中[建立 SCP](#)的步驟進行操作，在 JSON 編輯器中輸入以下文字：

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
    "Resource": "arn:aws:ec2:*:*:vpc/*",
    "Condition": {
      "Null": {
        "ec2:Ipv4IpamPoolId": "true"
      },
      "ForAllValues: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/`)，並新增您想選擇 (但不需要) 使用 IPAM 之 OU 的 AWS Organizations 組織實體路徑。如需有關實體路徑的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的[了解 AWS 組織實體路徑](#)與 [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[連接和分離服務控制政策](#)。

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 與組 AWS 織中的帳戶整合](#)。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。

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權限：
 - AWSRAMDefaultPermissionsIpamPool：選擇此許可權限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：選擇此許可權限可允許委託人將 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，才需要此許可權限。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 參考文件連結。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](#)。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 使用者指南》中的 [建立 VPC](#)。

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. 輸入您要新增的 CIDR，然後選擇 Add new CIDR (新增 CIDR) 以新增其他 CIDR。

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 Request provisioning (請求佈建)。
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 參考文件連結。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 命令可佈建集區的 CIDR：

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](#)

從集區解除佈建 CIDR

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。

Important

如果集區中有配置，則無法取消佈建 CIDR。若要移除配置，請參閱 [釋出配置](#)。

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 參考文件連結。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 命令可取消佈建集區 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](#)。

編輯集區

請依照本節中的步驟來編輯 IPAM 集區。您可能想要編輯集區以變更集區中的配置規則。如需分配規則的詳細資訊，請參閱 [建立頂層 IPv4 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](#)

刪除集區

請依照本節中的步驟來刪除 IPAM 集區。

Important

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。

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 參考文件連結。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](#)。

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帳戶的資源。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。

目錄

- [建立資源探索](#)
- [檢視資源探索詳細資訊](#)
- [共用資源探索](#)
- [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

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 Create (建立)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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

本節描述如何檢視資源探索的詳細資訊。其中包括資源 CIDR 和在資源探索下監控的帳戶探索狀態。

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。
 - IP 使用率 – 使用中 IP 地址空間的百分比。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。

Command line

本節中的命令與 AWS CLI 參考文件連結。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-discovery](#)

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 Next (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 Next (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 參考文件連結。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 Associate (關聯)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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 Disassociate (取消關聯)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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

- 請在 <https://console.aws.amazon.com/ipam/> 開啟 IPAM 主控台。
- 在導覽窗格中，選擇尋找探索。
- 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 參考文件連結。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](#)

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 探索具有私有 IPv4 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 參考文件連結。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 命令來建立其他的私有範圍：

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](#)

在各範圍之間移動 VPC CIDR

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。
- 這兩個範圍必須歸同一 AWS 帳戶所有。
- 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](#)

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。如需更多詳細資訊，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。如需更多詳細資訊，請參閱 [檢視 IP 地址歷程記錄](#)。

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

使用下列的 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](#)

刪除範圍

請依照本節中的步驟來刪除 IPAM 範圍。

Important

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 參考文件連結。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](#)。

釋出配置

請依照本節中的步驟在 IPAM 集區中釋出 CIDR 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。

如果您打算刪除某個集區，則可能需要釋出集區配置。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。如需更多詳細資訊，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 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#) 中的清除或 [僅使用 CLI 將您自己的 IPv6 CIDR 帶到 IPAM AWS](#) 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。需要幾分鐘的時間 CIDR 才會變成可用於隨後分配。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。
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 參考文件連結。本文件旨在詳細說明執行命令時可使用的選項。

使用下列項目 AWS CLI 命令可釋出集區配置：

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 [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](#)。

修改 IPAM

請依照本節中的步驟來修改 IPAM。

目錄

- [修改 IPAM 方案](#)
- [修改 IPAM 作業區域](#)

修改 IPAM 方案

請依照本節中的步驟修改 IPAM 方案。IPAM 提供兩種方案：免費方案和進階方案。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。

Important

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

Command line

本節中的命令與 AWS CLI 參考文件連結。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 方案：

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

請依照本節中的步驟修改 IPAM 作業區域。作業區域是允許 IPAM 管理 IP 地址 CIDR 的 AWS 區域。IPAM 僅會在您選取作為作業區域的 AWS 區域中探索並監控資源。

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 Save changes (儲存變更)。

Command line

本節中的命令與 AWS CLI 參考文件連結。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 命令來檢視及修改 IPAM 作業區域：

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](#)

刪除 IPAM

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](#)。

Important

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. 執行下列任意一項：
 - 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。如需更多詳細資訊，請參閱 [從集區解除佈建 CIDR](#)。
- 刪除任何其他非預設範圍。如需更多詳細資訊，請參閱 [刪除範圍](#)。
- 刪除 IPAM 集區。如需更多詳細資訊，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 參考文件連結。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](#)。

追蹤 IPAM 中的 IP 地址使用情況

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。

請依照本節中的步驟來追蹤 IPAM 中的 IP 地址使用方式。

目錄

- [使用 IPAM 儀表板監控 CIDR 使用情況](#)
- [依資源監控 CIDR 使用情況](#)
- [使用 Amazon CloudWatch 監控 IPAM](#)
- [檢視 IP 地址歷程記錄](#)
- [檢視公有 IP 深入解析](#)

使用 IPAM 儀表板監控 CIDR 使用情況

依照本節中的步驟存取 IPAM 儀表板，並檢視特定 IPAM 範圍內所有 CIDR 的狀態。

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。如需詳細資訊，請參閱 [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。如需詳細資訊，請參閱 [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

在 IPAM 中，資源是指派 IP 地址或 CIDR 區塊的 AWS 服務實體。IPAM 會管理某些資源，但只會監控其他資源。

- 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：
 - VPC
 - 公有 IPv4 集區

⚠ Important

公有 IPv4 集區和 IPAM 集區會透過 AWS 的不同資源進行管理。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。

- **Monitored resource (監控資源)**：如果資源由 IPAM 監控，則 IPAM 已偵測到資源，且當您透過 AWS CLI 使用 `get-ipam-resource-cidrs` 或在導覽窗格中查看 Resources (資源) 時，您可以查看有關資源 CIDR 的詳細資訊。IPAM 支援監控下列資源：
 - VPC
 - 公有 IPv4 集區
 - VPC 子網路
 - 彈性 IP 地址

下列步驟示範如何依資源監控 CIDR 使用情況和是否符合配置規則。

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. 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 地址範圍會配置給 IPAM 管理的資源。
 - 已佔用：IP 地址範圍已配置給資源。
 - 重疊：IP 地址範圍已配置給多個資源且重疊。
 - 不相容：IP 地址範圍不相容。一個使用 IP 地址範圍的資源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 地址區塊，以檢視較小 CIDR 區塊中的資源。選擇對應頂部的 IP 地址區塊，以檢視較大 CIDR 區塊中的資源。

5. 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。
- Management state (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。
 - Ignored (已忽略)：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 可以管理的資源類型之一。
- 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。
 - Noncompliant (不合規)：資源 CIDR 不符合 IPAM 集區的一或多個配置規則。

Example

如果 VPC 的 CIDR 不符合 IPAM 集區的網路遮罩長度參數，或者如果資源不在同一個 AWS 區域內做為 IPAM 集區，則會被標記為不合規。

- 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。
- Ignored (已忽略)：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)：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 可以管理的資源類型之一。
 - IP usage (IP 使用情況) : 如果是 VPC 資源, 此為 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。
 - Region (區域) : 資源的 AWS 區域。
 - Owner ID (擁有者 ID) : 建立此資源之人員的 AWS 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。
 - Pool ID (集區 ID) : 資源所在 IPAM 集區的 ID。
6. 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 參考文件連結。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 命令來依資源監控 CIDR 使用情況 :

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。

目錄

- [IPAM 集區和範圍指標](#)
- [資源使用率指標](#)

IPAM 集區和範圍指標

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 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

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。

您可以用來篩選 IPAM 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。
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](#)。

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)。
OwnerID	子網路擁有者的 ID。

維度	說明
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	說明
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 地址歷程記錄

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 地址
- 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未受 IPAM 監控的 AWS 帳號，則不會顯示與該資源相關的任何新歷程記錄，且 IPAM 也不會監控該資源。但是，資源的 IP 地址仍然可以搜索。

- 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號擁有之所有資源 CIDR 的 IP 位址歷程記錄。

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 參考文件連結。本文件旨在詳細說明執行命令時可使用的選項。

- 檢視 CIDR 的歷史記錄：[get-ipam-address-history](#)

如要檢視如何使用 AWS CLI 分析和稽核 IP 地址使用情況的範例，請參閱[教學課程：使用 AWS CLI 來檢視 IP 地址歷程記錄](#)。

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。
 - Noncompliant (不合規)：資源 CIDR 不符合 IPAM 集區的一或多個配置規則。

Example

如果 VPC 的 CIDR 不符合 IPAM 集區的網路遮罩長度參數，或者如果資源不在同一個 AWS 區域內做為 IPAM 集區，則會被標記為不合規。

- 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。
- 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)。
- Region (區域) : 此資源的 AWS 區域。
- Owner ID (擁有者 ID) : 建立此資源之使用者的 AWS 帳戶 ID (如果適用)。

檢視公有 IP 深入解析

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 所有公用 IPv4 位址的費用，包括與執行中執行個體和彈性 IP 位址相關聯的公用 IPv4 位址。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 (EIP) : Amazon 提供的靜態公有 IPv4 地址，您可以與 EC2 執行個體、elastic network interface 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 位址 : [您使用自帶 IP 位址 \(BYOIP\) 所帶來](#) 的 IPv4 位址範圍內的公 AWS 用 IPv4 位址。
- 服務管理的 IPv4 位址 : 在 AWS 資源上自動佈建並由服務管理的公用 IPv4 位址。AWS 例如，Amazon ECS、Amazon RDS 或 Amazon 上的公共 IPv4 地址。WorkSpaces

您可以使用公共 IP 洞察功能來查看下列資訊：

- 如果您的 IPAM [與組織中的帳戶整合](#)，您可以檢視整個 [AWSAWS 組織](#) 中所有 AWS 區域的服務使用的所有公用 IPv4 位址。

- 如果您的 IPAM [與單一帳戶整合](#)，您可以檢視帳戶中所有 AWS 區域的服務使用的所有公用 IPv4 位址。

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。
 - 亞馬遜擁有的 EIP：您已佈建或指派給帳戶中資源的彈性 IP 位址。AWS
 - 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。
 - 自攜 IP：您使用自攜 IP 位址 (BYO IP) 所帶來的公 AWS 用 IPv4 位址。
 - 服務受管 IP：由服 AWS 務佈建和管理的公用 IPv4 位址。
- EIP 使用量：彈性 IP 地址的使用方式組織的數目。
 - 相關聯的 Amazon 擁有的 EIP：您在 AWS 帳戶中佈建且已與 EC2 執行個體、網路界面或資源相關聯的彈性 IP 地址。AWS
 - 關聯的 BYOIP：您使用與網路界面相關聯的 BYOIP 所帶來的公 AWS 用 IPv4 位址。
 - 無關聯的 Amazon 擁有的 EIP：您在 AWS 帳戶中佈建但尚未與網路界面相關聯的彈性 IP 位址。
 - 未關聯的 BYOIP：您使用 BYOIP 帶來的公 AWS 用 IPv4 位址，但您尚未與網路界面產生關聯。
- 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。
 - 關聯：地址是否與 EC2 執行個體、網路界面或 AWS 資源相關聯。
 - 關聯：公用 IPv4 地址與 EC2 執行個體、網路界面或 AWS 資源相關聯。
 - 未關聯：公共 IPv4 地址與任何資源沒有關聯，並且在您 AWS 的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。
 - 自備 IP：已將公用 IPv4 位址帶到使 AWS 用 BYOIP。
 - EC2 公有 IP：自動指派給 EC2 執行個體的公有 IPv4 地址。
 - 服務管理的 BYOIP：使用自攜 IP (BYOIP) 將公 AWS 用 IPv4 位址帶入。
 - 服務受管理 IP：已佈建公用 IPv4 位址，並由 AWS 服務管理。
 - 服務：與 IP 地址相關聯的服務。
 - ~~阿迦：安 AWS Global Accelerator。如果使用[自訂線路加速器](#)，則不會列出其公用 IP。若要檢視這些公用 IP，請參閱[檢視您的自訂路由加速器](#)。~~

- Database Migration Service : AWS Database Migration Service (DMS) 複製執行處理。
- 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 IP 位址已通告，這就是通告 IP 位址的來源地 AWS 區。
- 擁有者 ID : 資源擁有者的帳 AWS 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。如果您看到與沒有呼叫權限相關的錯誤 `GetIpamDiscoveredPublicAddresses`，則需要更新與您共用的資源探索附加的 Managed 權限。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：作為組織 AWS 資源的中繼資料的索引鍵和值配對。

Command line

[使用下列命令取得 IPAM 探索到的公用 IP 位址：get-ipam-discovered-public-位址](#)

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

- [教學課程：使用主控台建立 IPAM 和集區](#)
- [教學課程：使用 AWS CLI 建立 IPAM 和集區](#)
- [教學課程：使用 AWS CLI，檢視 IP 地址歷史記錄](#)
- [教學課程：將 ASN 帶入 IPAM](#)
- [教學課程：將 IP 地址帶入 IPAM](#)
- [教學課程：將 BYOIP IPv4 CIDR 傳輸至 IPAM](#)
- [教學課程：為子網路 IP 配置規劃 VPC IP 地址空間](#)

教學課程：使用主控台建立 IPAM 和集區

在本教學課程中，您將學習如何建立 IPAM、整合 AWS Organizations、建立 IP 地址集區，以及使用 IPAM 集區的 CIDR 建立 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 作為單一使用者，但整合 AWS Organizations 可讓您管理組織中各帳戶的 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](#)
- [AWS Organizations 如何與 IPAM 整合](#)
- [步驟 1：委派 IPAM 管理員](#)
- [步驟 2：建立 IPAM](#)
- [步驟 3：建立最上層 IPAM 集區](#)
- [步驟 4：建立區域 IPAM 集區](#)
- [步驟 5：建立生產前開發集區](#)
- [步驟 6：共用 IPAM 集區](#)
- [步驟 7：使用從 IPAM 集區配置的 CIDR 建立 VPC](#)
- [步驟 8：清除](#)

先決條件

開始之前，您必須先設定具有至少一個成員帳戶的 AWS Organizations 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](#)。

AWS Organizations 如何與 IPAM 整合

本節將提供您會在本教學課程中使用的 AWS Organizations 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。

The screenshot shows the AWS Organizations console interface. On the left is a navigation sidebar with 'AWS Organizations' and 'AWS accounts' selected. The main content area is titled 'AWS accounts' and includes an 'Add an AWS account' button. Below this is a search bar and a table of organizational units and accounts. The table has columns for 'Organizational structure' and 'Account created/joined date'. The structure shows a hierarchy: Root (r-fssg) -> Organizational-unit-1 (ou-fssg-ycy89843) -> Organizational-unit-1a (ou-fssg-q5brfv9c). Under Organizational-unit-1a, there are three accounts: 'example-member-account-1', 'example-member-account-2', and 'example-management-account' (management account). All accounts were joined on 2022/12/28.

Organizational structure	Account created/joined date
Root r-fssg	
Organizational-unit-1 ou-fssg-ycy89843	
Organizational-unit-1a ou-fssg-q5brfv9c	
example-member-account-1 848560618819 example-member-account-1@amazon.com	Joined 2022/12/28
example-member-account-2 848560618819 example-member-account-2@amazon.com	Joined 2022/12/28
example-management-account (management account) 855210303341 example-management-account@amazon.com	Joined 2022/12/28

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

如需有關管理和成員帳戶等 AWS Organizations 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 成員帳戶作為 IPAM 管理員。委派 IPAM 管理員時，系統會在每個 AWS Organizations 成員帳戶中自動建立 [服務連結角色](#)。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。

除非您擁有必要的 AWS Identity and Access Management (IAM) 許可，否則無法完成此步驟。如需更多詳細資訊，請參閱 [將 IPAM 與組 AWS 織中的帳戶整合](#)。

委派 IPAM 管理員帳戶

1. 使用 AWS Organizations 管理帳戶，在 <https://console.aws.amazon.com/iam/> 中開啟 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. 選擇委派。只有在您以 AWS Organizations 管理帳戶的身分登入主控台後，才能使用 Delegate (委派) 選項。
5. 輸入組織成員帳戶的 AWS 帳戶 ID。IPAM 管理員必須為 AWS Organizations 成員帳戶，而非管理帳戶。

The screenshot shows the 'Settings' page for Amazon VPC IP Address Manager. The breadcrumb navigation is 'Amazon VPC IP Address Manager > Settings > Edit'. The main heading is 'Settings' with an 'Info' icon. Below this is a section titled 'Delegated administrator'. Underneath, there is a sub-section 'Delegated administrator account' with a description: 'The account to be delegated as the IPAM administrator for your organization. To monitor resources across your organization, the IPAM must be created in the delegated administrator's account.' Below the description is a text input field with the placeholder text 'Enter an account ID for the IPAM administrator'. Further down is a sub-section 'Service access' with a description: 'When you delegate an IPAM administrator, you grant Amazon VPC IP Address Manager permission to describe resources on your behalf.' Below this is a 'View details' button. At the bottom right of the form are 'Cancel' and 'Save changes' buttons.

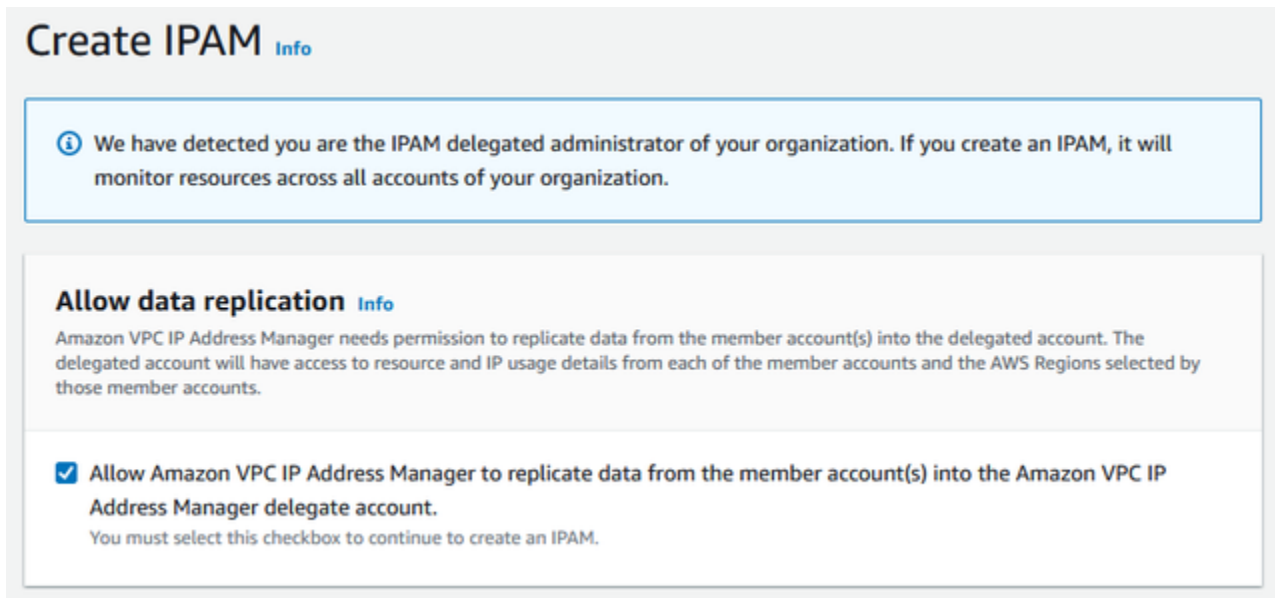
6. 選擇 Save changes (儲存變更)。委派的管理員資訊會填入與成員帳戶相關的詳細資料。

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。如需更多詳細資訊，請參閱 [IPAM 的運作方式](#)。

建立 IPAM

1. 使用在**前述步驟**中委派為 IPAM 管理員的 AWS Organizations 成員帳戶，在 <https://console.aws.amazon.com/ipam/> 中開啟 IPAM 主控台。
2. 在 AWS 管理主控台中，選擇欲建立 IPAM 的 AWS 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. 在作業區域下，選擇此 IPAM 可管理與探索資源的 AWS 區域。您會在其中建立 IPAM 的 AWS 區域，會自動獲選為其中一個作業區域。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。

IPAM settings [Info](#)

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

Description - *optional*

Write a brief description for the IPAM.

Operating Regions

Select Regions in which the IPAM will discover resources and manage IPs. The current region will always be set as an operating region.



Default resources will be created

On IPAM creation, the following IPAM resources will also be created:

- A default private scope. Resources using private IP space will be imported into the private scope.
- A default public scope. Resources using public IP space will be imported into the public scope.
- A default resource discovery, which controls the resources that IPAM will discover.

6. 選擇 Create IPAM (建立 IPAM)。

✔ Successfully created IPAM ipam-005f921c17ebd5107✕

Amazon VPC IP Address Manager > IPAMs > ipam-005f921c17ebd5107

DemoIPAM (ipam-005f921c17ebd5107) Info

Edit Delete

IPAM details

IPAM ID ipam-005f921c17ebd5107	Description -	Owner ID 320805250157	Region us-east-1
IPAM ARN arn:aws:ec2::320805250157:ipam/ipam-005f921c17ebd5107	Default public scope ipam-scope-0d3539a30b57dcdd1	Default private scope ipam-scope-0a158dde35c51107b	Scope count 2
State Create-complete	Default resource discovery ipam-res-disco-0f4ef577a9f37a162		

Operating Regions | Associated discoveries | Tags

Operating Regions (3) Info

Region
US East (N. Virginia) - us-east-1
US West (N. California) - us-west-1
US West (Oregon) - us-west-2

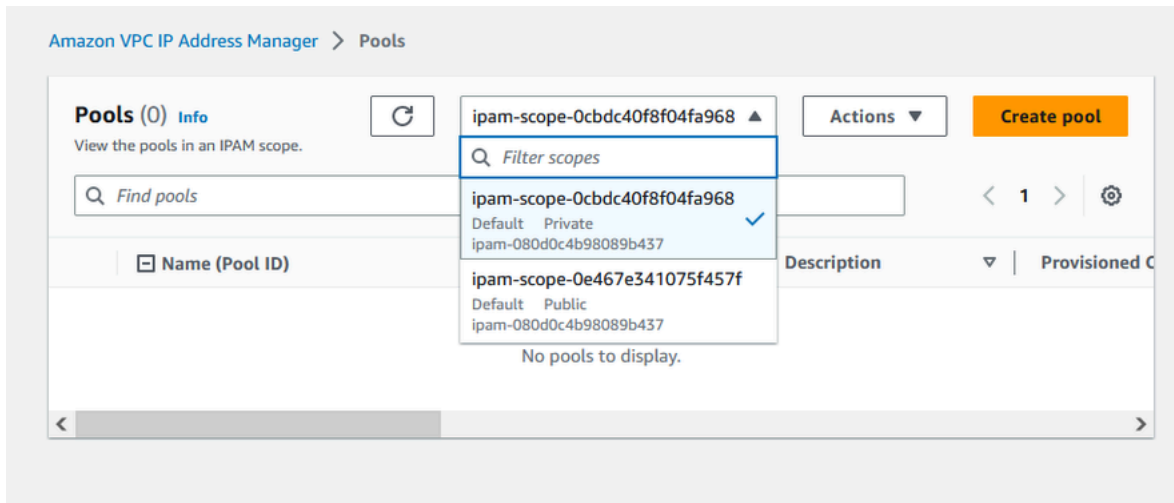
步驟 3：建立最上層 IPAM 集區

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 Create pool (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)。地區設定為您希望此 IPAM 集區可供配置使用的 AWS 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。

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

Name (IPAM ID) DemoIPAM (ipam-080d0c4b98089b437)	Name (Scope ID) ipam-scope-0cbdc40f8f04fa968
---	---

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify. Tags are not visible to other accounts even if a pool is shared.

Description - optional
Write a brief description for the pool.

Pool hierarchy [Info](#)

Source pool
To provision a CIDR into this pool, it must be available in the source pool. If no source pool is selected, then the space must be available in the scope.

Address family
Select the address family for this pool.

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

A locale can only be selected if there is no source pool, or if the source pool's locale is None.

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。

CIDRs to provision [Info](#)

CIDRs to be provisioned must either be available in the source pool's space, or in the scope's space if no source pool.

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/16	65K IPs	Remove
< > ^ v		

Add new CIDR

- 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。

Allocation rule settings - *optional* [Info](#)



AWS best practice

We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).

Configure this pool's allocation rule settings

- 選擇 Create pool (建立集區)。集區已建立，且 CIDR 處於待佈建狀態：

Sent request to provision 10.0.0.0/16

Amazon VPC IP Address Manager > Pools > ipam-pool-06fb4cace4bc1e551

Global pool (ipam-pool-06fb4cace4bc1e551)

Pool summary

Pool ID ipam-pool-06fb4cace4bc1e551	Description -	IPAM ID ipam-005f921c17ebd5107	Scope ID ipam-scope-0a158dde35c51107b
Pool ARN arn:aws:ec2::320805250157:ipam-pool-06fb4cace4bc1e551	Owner ID 320805250157	Compliance status -	Overlap status -

Pool details | Monitoring | IP space visualization | **CIDRs** | Allocations | Resources | Compliance | Reso

CIDRs (1) Info

Deprovision CIDRs | Provision CIDR

Filter CIDRs

CIDR	CIDR ID	State
10.0.0.0/16	ipam-pool-cidr-0657f970d119e40899e0e...	Pending-provision

14. 等待狀態變為已佈建後，即可前往下一個步驟。

✔ Sent request to provision 10.0.0.0/16 ✕

Amazon VPC IP Address Manager > Pools > ipam-pool-06fb4cace4bc1e551

Global pool (ipam-pool-06fb4cace4bc1e551) ↻ Actions ▾

Pool summary

Pool ID ipam-pool-06fb4cace4bc1e551	Description -	IPAM ID ipam-005f921c17ebd5107	Scope ID ipam-scope-0a158dde35c51107b
Pool ARN arn:aws:ec2::320805250157:ipam-pool-06fb4cace4bc1e551	Owner ID 320805250157	Compliance status -	Overlap status -

< Pool details | Monitoring | IP space visualization | CIDRs | Allocations | Resources | Compliance | Resc >

CIDRs (1) InfoDeprovision CIDRsProvision CIDR

<input type="checkbox"/>	CIDR	CIDR ID	State
<input type="checkbox"/>	10.0.0.0/16	ipam-pool-cidr-0657f970d119e40899...	✔ Provisioned

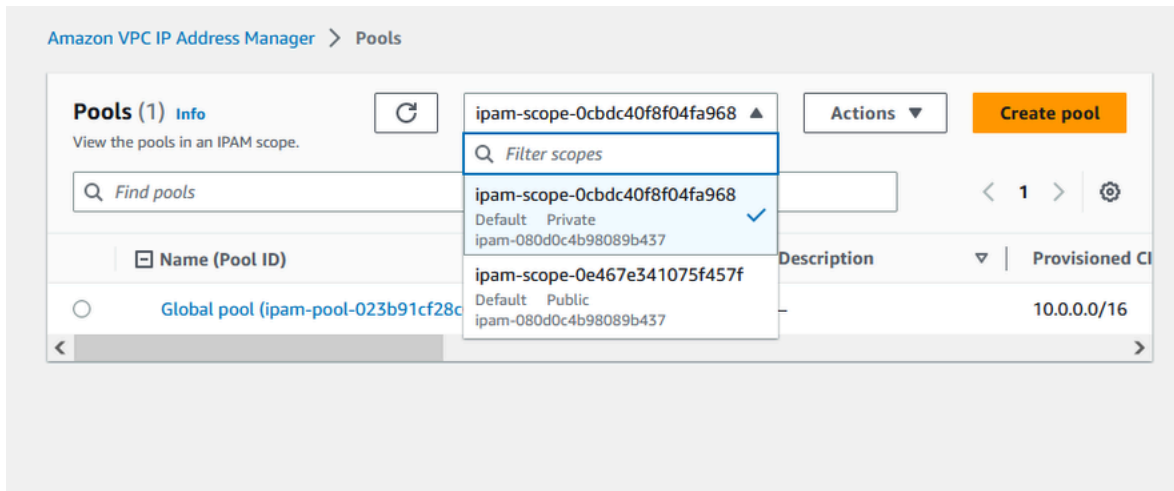
現在您已建立頂層集區，將可在 us-west-1 和 us-west-2 中建立區域集區。

步驟 4：建立區域 IPAM 集區

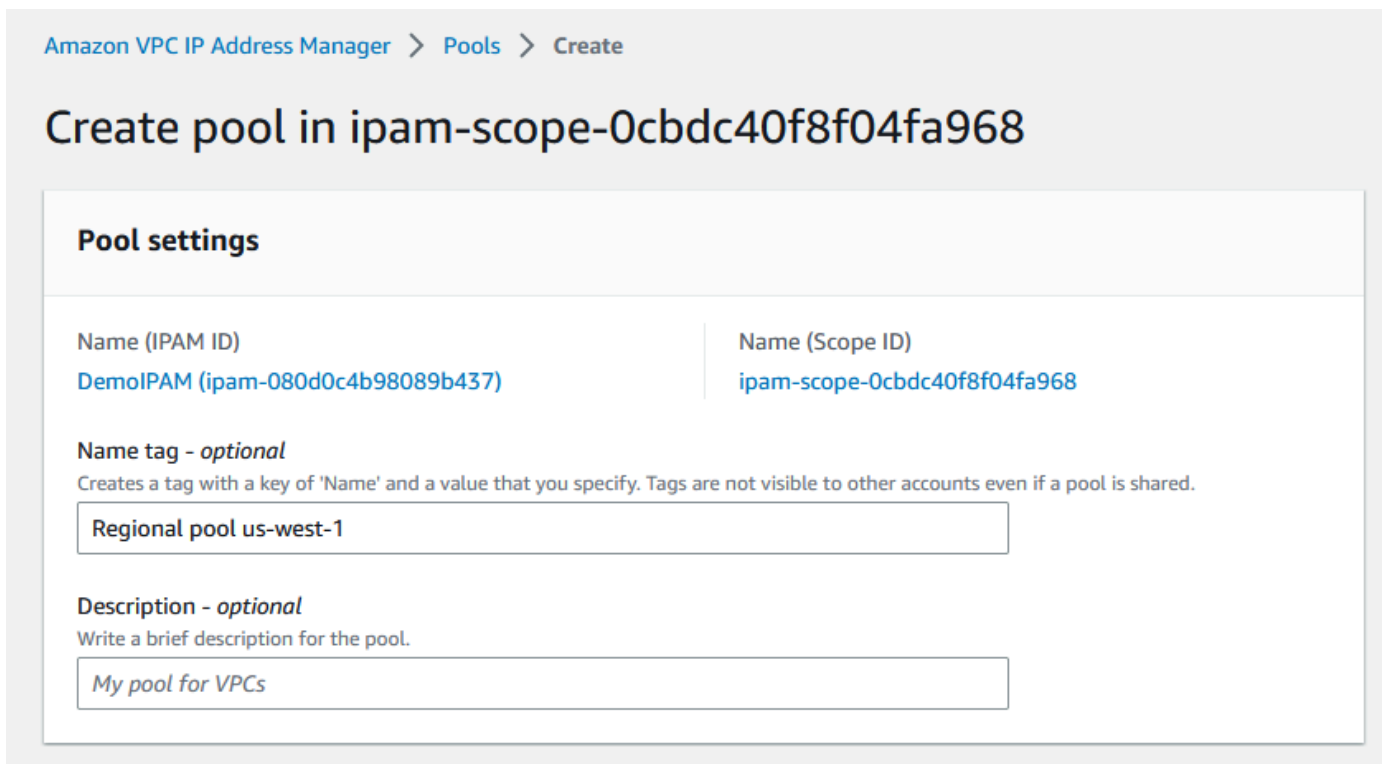
本節將會說明如何使用兩個區域集區來組織 IP 地址。在本教學課程中，我們將按照其中一個 [IPAM 集區計劃範例](#)，建立兩個區域集區 (這兩個區域集區可供組織中的成員帳戶使用，以將 CIDR 配置給其 VPC)。

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 Create pool (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。

Pool hierarchy [Info](#)

Source pool
To provision a CIDR into this pool, it must be available in the source pool. If no source pool is selected, then the space must be available in the scope.

Global pool (ipam-pool-023b91cf28c61a0fb) ▼

▼ **Source pool summary**

Name (Pool ID)	Provisioned CIDRs
Global pool (ipam-pool-023b91cf28c61a0fb)	10.0.0.0/16
Description	Locale
-	None

Address family (inherited)
Select the address family for this pool.

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

US West (N. California) - us-west-1 ▼

A locale can only be selected if there is no source pool, or if the source pool's locale is None.

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)。

CIDRs to provision [Info](#)

CIDRs to be provisioned must either be available in the source pool's space, or in the scope's space if no source pool.

IP space visualization (source pool)

Zoom Overlapping New allocation Allocated Available

10.0.0.0/16 (100% available → 75% available after allocations)

**CIDR**

Enter a CIDR to be provisioned.

10.0.0.0/18 16K IPs Remove

< > ^ v

Add specific CIDR

Add CIDR by size

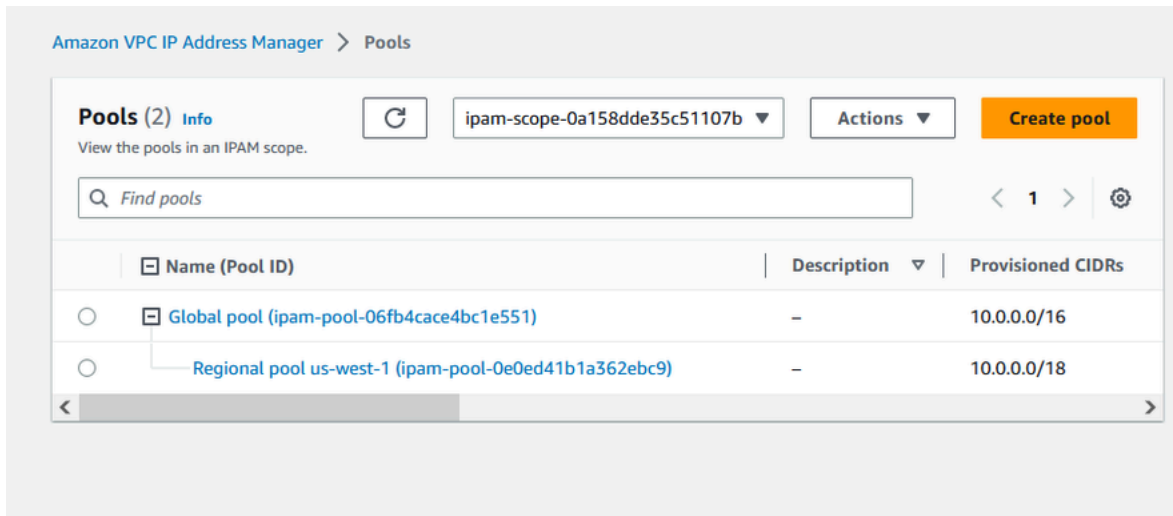
- 將設定此集區的配置規則設定保持停用。您將無法直接從此集區將 CIDR 配置到 VPC。相反地，您可能須從自己在此集區建立的子集區進行配置。

Allocation rule settings - optional [Info](#)**AWS best practice**

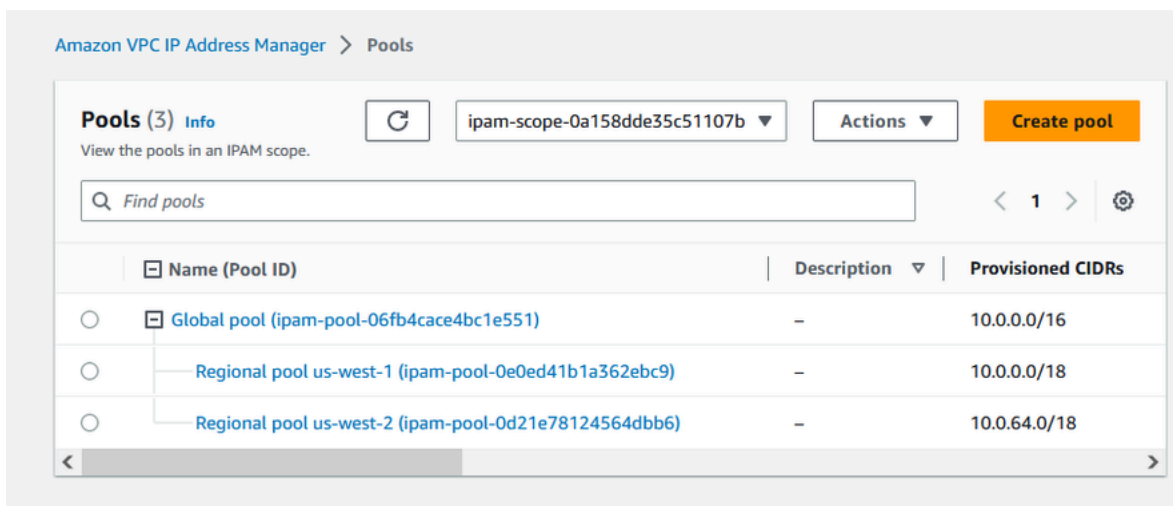
We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).

Configure this pool's allocation rule settings

- 選擇 Create pool (建立集區)。
- 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

- 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。

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

Name (IPAM ID)

DemoIPAM (ipam-080d0c4b98089b437)

Name (Scope ID)

ipam-scope-0cbdc40f8f04fa968

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify. Tags are not visible to other accounts even if a pool is shared.

Pre-prod pool

Description - *optional*

Write a brief description for the pool.

My pool for VPCs

Pool hierarchy [Info](#)

Source pool

To provision a CIDR into this pool, it must be available in the source pool. If no source pool is selected, then the space must be available in the scope.

Regional pool us-west-1 (ipam-pool-03b74e706bb0df4ab) ▼

▼ Source pool summary

Name (Pool ID)

Regional pool us-west-1 (ipam-pool-03b74e706bb0df4ab)

Description

-

Provisioned CIDRs

10.0.0.0/18

Locale

us-west-1

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)。

CIDRs to provision [Info](#)

CIDRs to be provisioned must either be available in the source pool's space, or in the scope's space if no source pool.

IP space visualization (source pool)

Zoom Overlapping New allocation Allocated Available

10.0.0.0/18 (100% available → 75% available after allocations)

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/20 4K IPs Remove

< > ^ v

Add specific CIDR Add CIDR by size

3. 切換設定此集區的配置規則設定選項。請執行下列動作：

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。

Allocation rule settings - *optional* [Info](#)



AWS best practice

We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).

Configure this pool's allocation rule settings

CIDR management

Automatically import discovered resources

It is recommended to allow automatic import if this pool will be used to allocate CIDRs to resources such as VPCs.

- Allow automatic import
- Don't allow

Netmask compliancy

Minimum netmask length

The minimum netmask length for allocating resources within the pool.

/24 (256 IPs)

Default netmask length

The default netmask length used when IPAM allocates a CIDR from this pool to a resource.

/24 (256 IPs)

Maximum netmask length

The maximum netmask length for allocating resources within the pool.

/24 (256 IPs)

Tag compliancy

Tagging requirements

Add tagging requirements for resources in this pool.

Key

environment



Value - *optional*

pre-prod



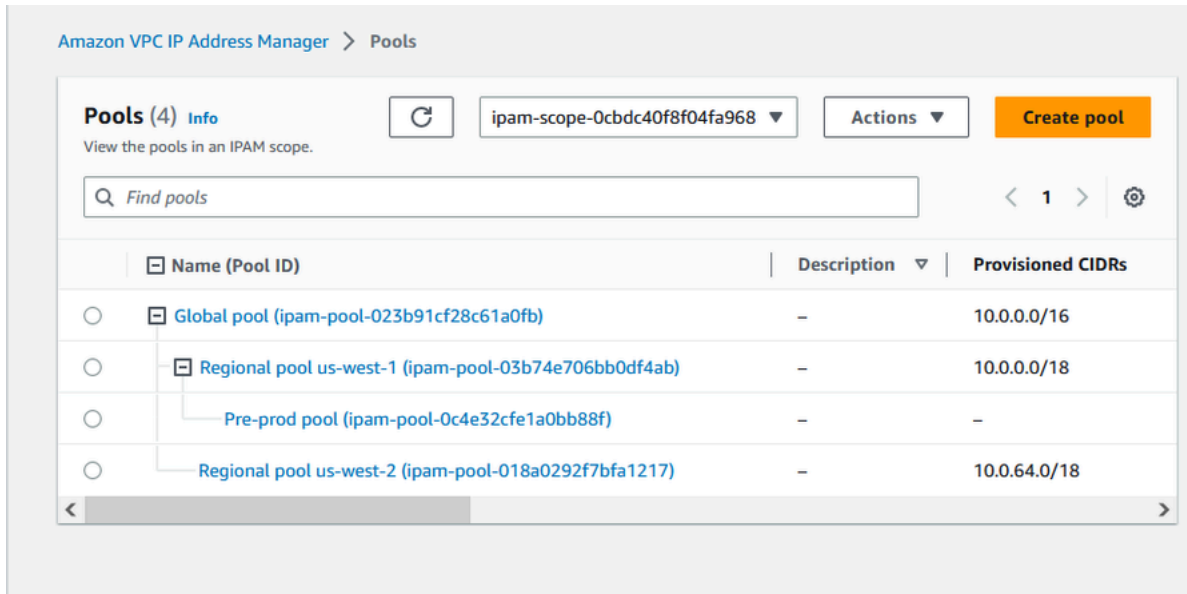
Remove

Add new required tag

You can add up to 49 more tags.

4. 選擇 Create pool (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

請按照本節中的步驟，使用 AWS Resource Access Manager (RAM) 來共用生產前 IPAM 集區。

本節由兩個小節組成：

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

步驟 6.1. 在 AWS RAM 啟用資源共用

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。在共用 IPAM 集區之前，請完成本節中的步驟來啟用與 AWS RAM 共用資源的功能。

啟用資源共用

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

The screenshot displays the AWS Resource Access Manager (RAM) console interface. On the left, a navigation sidebar is visible under the heading 'Resource Access Manager'. It includes a close button (X) and two main sections: 'Shared by me' and 'Shared with me'. Each section lists 'Resource shares', 'Shared resources', and 'Principals'. Below these sections are 'Permissions library' and 'Settings', which is currently selected and highlighted in orange. The main content area on the right shows the 'Settings' page for RAM. At the top, it reads 'Resource Access Manager > Settings'. A 'Settings' box contains a checked checkbox for 'Enable sharing with AWS Organizations' with a link icon. Below the checkbox, a note states: 'If you enable sharing with the accounts of your organization, you can share resources without using invitations. You can enable sharing in the organization's management account. The organization must support all features.' A 'Save settings' button is located at the bottom right of the settings box.

您現在可以與組織的其他成員共用 IPAM 集區。

步驟 6.2. 使用 AWS RAM 共用 IPAM 集區

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 AWS RAM 共用 IPAM 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，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 AWS RAM 共用集區。
5. 選擇 Create a resource share (建立資源共用)。

The screenshot shows the AWS IPAM console interface. At the top, a green banner indicates 'Sent request to provision 10.0.0/20'. The breadcrumb navigation is 'Amazon VPC IP Address Manager > Pools > ipam-pool-07bdd12d7c94e4693'. The main heading is 'Pre-prod pool (ipam-pool-07bdd12d7c94e4693)'. Below this is a 'Pool summary' table with the following data:

Pool ID	Description	IPAM ID	Scope ID
ipam-pool-07bdd12d7c94e4693	-	ipam-005f921c17ebd5107	ipam-scope-0a158dde35c51107b
Pool ARN	Owner ID	Compliance status	Overlap status
arn:aws:ec2::320805250157:ipam-pool/ipam-pool-07bdd12d7c94e4693	320805250157	-	-

Below the summary is a navigation bar with tabs: Pool details, Monitoring, IP space visualization, CIDRs, Allocations, Resources, Compliancy, Resource sharing (selected), and Tags. The 'Resource sharing' section is active, showing a 'Create resource share' button highlighted with an orange box. Below this is a search bar 'Filter resource shares' and a table with columns 'Resource share ARN', 'Status', and 'Created at'. The table is currently empty, displaying 'No shares' and 'This resource is not part of any resource share.' with a 'Create resource share' button below it.

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用。
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。

Specify resource share details

Enter a name for the resource share and select the resources that you want to share.

Resource share name

Name

Provide a descriptive name for the resource share.

Pre-prod dev pool

Resources - optional

Choose the resources to add to the resource share.

Select resource type

IPAM Pools

Filter by attributes or search by keyword

<input type="checkbox"/>	ARN	Locale
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-06fb4cace4bc1e551	None
<input checked="" type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-07bdd12d7c94e4693	us-west-1
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-0b8123821c7ef5319	us-east-1
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-0d21e78124564dbb6	us-west-2
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-0e0ed41b1a362ebc9	us-west-1

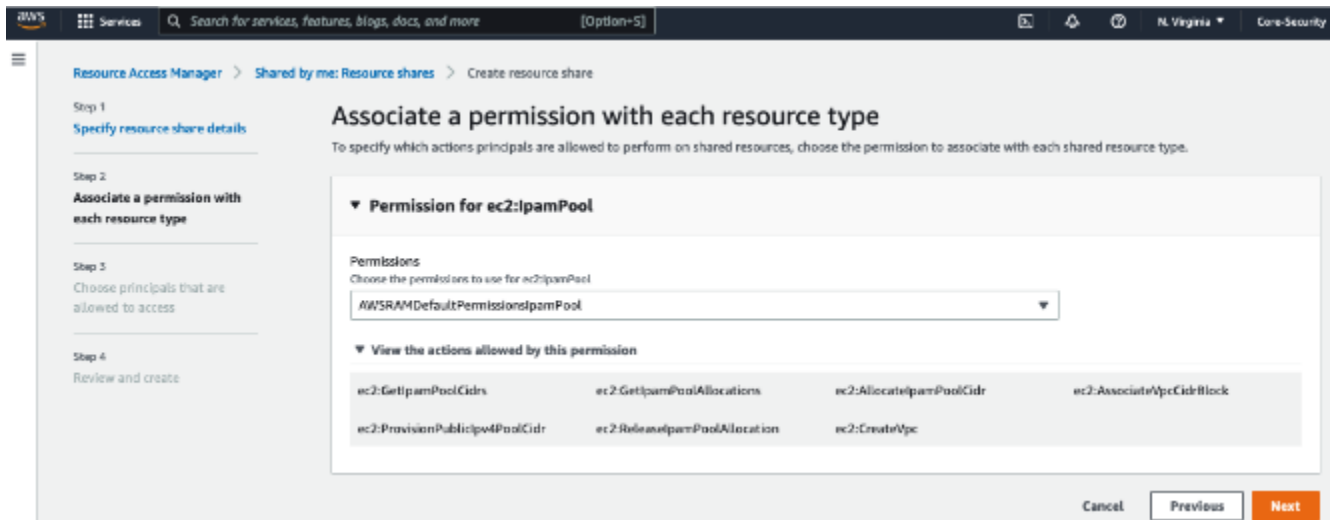
Selected resources (1)

Deselect

<input type="checkbox"/>	Resource ID ↗	Resource Type
<input type="checkbox"/>	ipam-pool-07bdd12d7c94e4693	ec2:IpamPool

9. 選擇 Next (下一步)。

10. 保持選取預設的 `AWSRAMDefaultPermissionsIpamPool` 權限。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 Next (下一步)。
12. 在主體下，選擇僅允許在組織內共用。輸入 AWS Organizations 組織單位 ID (如 [AWS Organizations 如何與 IPAM 整合](#) 中所述)，然後選擇新增。

Grant access to principals

Specify the principals that are allowed access to the shared resources. A principal can be any of the following: An entire organization or organizational unit (OU) in AWS Organizations, an AWS account, IAM role, or IAM user.

Principals - *optional*

Allow sharing with anyone

You can share resources with any AWS accounts, roles, and users. If you are in an organization, you can also share with the entire organization or organizational units in that organization.

Allow sharing only within your organization

You can share resources with the entire organization, organizational units, or AWS accounts, roles, and users in that organization.

Principals

You can add multiple principals of different types.

Organizational unit (OU) ▼

ou-fssg-q5brfv9c

Organizational unit ID format: ou-{4-32 characters}-{8-32 characters}.

Add

▼ Selected principals (0)

The following principals will be allowed access to the shared resources.

Deselect

Principal ID	Type
--------------	------

No selected principals.

Cancel

Previous

Next

13. 選擇 Next (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 [AWS Organizations 如何與 IPAM 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 Create VPC (建立 VPC)。
3. 請執行下列動作：
 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。

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

 VPC only VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

IPv4 CIDR block [Info](#)

 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 IPAM pool

us-west-1

The locale of the IPAM pool must be equal to the current region.

Netmask

256 IPs ▼

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 [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 Create VPC (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。

⊗ **There was an error creating your VPC**
The resource is missing one or more of the resource tags required by the IPAM pool.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

VPC only

VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

Example VPC

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input

IPAM-allocated IPv4 CIDR block

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

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name

×

Value - *optional*

Q Example VPC

×

Remove

Q environment

×

Q pre-prod

×

Remove

Add new tag

You can add 48 more tags.

8. VPC 已成功建立，且 VPC 符合生產前集區上的標籤規則：




✔ You successfully created vpc-07701f4fcc6549b8d / Example VPC

VPC > Your VPCs > vpc-07701f4fcc6549b8d

vpc-07701f4fcc6549b8d / Example VPC

Actions ▼

Details [Info](#)

VPC ID  vpc-07701f4fcc6549b8d	State  Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0b14c6b1ccb2338bb	Main route table rtb-0a89b32824730ec5c	Main network ACL acl-0dee4236e2f7502c8
Default VPC No	IPv4 CIDR 10.0.0.0/24	IPv6 pool -	IPv6 CIDR -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID  320805250157	

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 主控台下的範例資源共用。如需詳細指示，請參閱《AWS Resource Access Manager 使用者指南》中的[在 AWS 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 AWS RAM 啟用資源共用](#) 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。

Delete IPAM Demo IPAM (ipam-080d0c4b98089b437) ✕

Deleting this IPAM will permanently remove it. To confirm deletion, type *delete* in the field.

Cascade delete
Enables you to quickly delete an IPAM, private scopes, pools in private scopes, and any allocations in the pools in private scopes. You cannot delete the IPAM with this option if there is a pool in your public scope. No VPC resources will be deleted.

Cancel Delete

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) 整合 IPAM 與 AWS Organizations 時，[IPAM 會在每個成員帳戶中自動建立服務連結角色](#)。使用每個 AWS Organizations 成員帳戶登入 IAM，然後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 AWS CLI 建立 IPAM 和集區

請按照本教學課程中的步驟，使用 AWS CLI 建立 IPAM、建立 IP 地址集區，以及使用 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：

- IPAM 執行於 AWS 區域 1、AWS 區域 2

- 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。如需更多詳細資訊，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](#)
- [步驟 2：建立 IPAM](#)
- [步驟 3：建立 IPv4 地址集區](#)
- [步驟 4：在最上層集區佈建 CIDR](#)
- [步驟 5. 利用最上層集區中的 CIDR 建立區域集區](#)
- [步驟 6：在區域集區中佈建 CIDR](#)
- [步驟 7. 建立 RAM 共用以啟用跨帳戶的 IP 指派](#)
- [步驟 8. 建立 VPC](#)
- [步驟 9. 清除](#)

步驟 1：在您的組織中啟用 IPAM

此為選用步驟。完成此步驟可在您的組織中啟用 IPAM，並使用 AWS CLI 來設定您的委派 IPAM。如需有關 IPAM 帳戶角色的詳細資訊，請參閱 [將 IPAM 與組 AWS 織中的帳戶整合](#)。

只有 AWS Organizations 管理帳戶才能提出此請求。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 111111111111
```

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

作業區域選項可決定 IPAM 集區用於哪些 AWS 區域。如需有關作業區域的詳細資訊，請參閱 [建立 IPAM](#)。

使用 AWS CLI 建立 IPAM

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
```

建立 IPAM 時，AWS 會自動執行以下操作：

- 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 地址。私有範圍專用於不透過公有網際網路存取的 IP 地址。

```
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`。如果集區的地區設定為 `None`，則該集區不可用於任何 AWS 區域的 VPC 資源。您只能在集區中手動分配 IP 地址空間以保留空間。

使用 AWS CLI 為您的所有 AWS 資源建立 IPv4 地址集區

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。如需更多詳細資訊，請參閱 [佈建集區的 CIDR](#)。

使用 AWS CLI 在集區中佈建 CIDR 區塊

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，在預設情況下，集區屬於該 IPAM 的 AWS 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 AWS CLI 建立包含先前集區之 CIDR 的集區

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 AWS CLI 將 CIDR 區塊指派給區域集區

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状态。

```
{
  "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
```

下列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 與組 AWS 織中的帳戶整合](#) 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 共用功能僅適用於本地 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 AWS CLI，檢視 IP 地址歷史記錄

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。如需有關使用 AWS CLI 的一般資訊，請參閱《AWS Command Line Interface 使用者指南》中的[使用 AWS CLI](#)。

目錄

- [概要](#)
- [案例](#)

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 地址
- 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 的 AWS 區域才可執行。
- 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 地址歷程記錄](#)。

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 地址歷程記錄](#)。

```
{
  "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"
  }
]
}

```

若連接至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 (如 NAT 閘道、VPC 中的 Lambda 網路介面和其他 AWS 服務一樣)，則 ResourceOwnerId 為 amazon-aws 而非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 地址歷程記錄](#)。

```
{  
  "HistoryRecords": [  
    {  
      "ResourceOwnerId": "123456789012",  
      "ResourceRegion": "us-east-1",  
      "ResourceType": "subnet",  
      "ResourceId": "subnet-0864c82a42f5bffd",  
      "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
```

- 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 地址歷程記錄](#)。

```
{
  "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 地址歷程記錄](#)。

```
{
  "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 地址歷程記錄](#)。

```

{
  "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 地址歷程記錄](#)。

```

{
  "HistoryRecords": [
    {
      "ResourceOwnerId": "123456789012",
      "ResourceRegion": "us-east-1",
      "ResourceType": "subnet",
      "ResourceId": "subnet-0864c82a42f5bffd",
      "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？

於此範例中，將 54.0.0.9/32 指派給彈性 IP 地址，而該地址不屬於與您 IPAM 整合的 AWS Organization。

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. 由於在此範例中，將 54.0.0.9/32 指派給彈性 IP 地址，而該地址不屬於與您 IPAM 整合的 AWS Organization，因此，未傳回任何無記錄。

```
{
  "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 位址和自治系統編號 (ASN)，您可以在中執行這些應用程式，AWS 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出貨預先通知，但對於這些組織，他們可以將其 ASN 帶入其 ASN。AWS

使 AWS 用您自己的自主系統號碼 (BYOASN) 可讓您使用自己的公有 ASN (而非 ASN) 通告所攜帶的 IP 位址。AWS 當您使用 BYOASN 時，源自您 IP 位址的流量會承載您的 ASN 而非 ASN，而且允許根據您的 IP 位址和 AWS ASN 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給 IPAM 的公用 ASN，並且已將 BYOIP CIDR 帶入 AWS 並將其佈建到公用範圍中的集區。您可以隨時將 ASN 帶到 IPAM，但要使用它，您必須與您帶入帳戶的 CIDR 建立關聯。AWS 此教學課程假設您已執行下列作業：如需詳細資訊，請參閱 [教學課程：將 IP 地址帶入 IPAM](#)。
- 您可以立即在廣告之間變更您自己的 AWS ASN 或 ASN，但您僅限於每小時從 AWS ASN 變更為自己的 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 AWS 使用 IP 位址範圍 [教學課程：將 IP 地址帶入 IPAM](#)，則需要 IP 位址 CIDR 範圍。您還需要一個私鑰。您可以使用將 AWS IP 位址 CIDR 範圍帶到時建立的私密金鑰，也可以按照 EC2 使用者指南中的 [建立私密金鑰並產生 X.509 憑證中所述建立新的私密金鑰](#)。
- 當您使用 IP 位址範圍時 [教學課程：將 IP 地址帶入 IPAM](#)，您會 [建立 X.509 憑證，並將 X.509 憑證上傳到 RIR 中的 RDAP 記錄](#)。AWS 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。

教學步驟

使用 AWS 控制台或完成以下步驟 AWS CLI。

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 是您要帶到 IPAM 的出貨預先通知，而 YYYYMMDD 是訊息的到期日 (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. 使用私密金鑰簽署訊息。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「簽名」下，輸入簽名。
9. (選擇性) 若要啟動設定其他 ASN，請選擇啟動設定其他出貨預先通知 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「關聯的 BYOASN」下，選擇您提供的出貨預先通知。AWS 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. 透過包含您的 ASN 與授權訊息來佈建您的出貨預先通知。簽名是使用您的私鑰簽名的消息。

```
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。如果要求成功，您應該會在幾分鐘後看到已佈建的 ProvisionStatus 設定。

```
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：

- 若要僅撤銷您的 ASN 廣告並返回使用 Amazon ASN，同時保持 CIDR 廣告，您必須使用 asn 參數 advertise-byoip-cidr 的特殊 AWS 值呼叫。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
```

- 要同時撤銷您的 CIDR 和 ASN 廣告，您可以致電。 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
```

- 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
```

- 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
```

- 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

本節中的教學課程將引導您完成使用 IPAM 將公用 IP 位址空間帶入 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。
- 簡化將公用 IP 空間帶入的程序 AWS：您可以使用 IPAM 將公用 IP 位址空間上載一次，然後使用 IPAM 在各個區域中散發您的公用 IP。如果沒有 IPAM，您必須在每個 AWS 區域上載您的公共 IP。

Important

- 在開始本教學之前，請在 Amazon EC2 使用者指南中針對您的 [BYOIP 地址範圍完成上線先決條件](#)中的步驟。

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。這樣可確保您有充分的靈活性，可以跨 AWS 區域劃分您的公有 IP 地址。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定為 /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。

- 將 IPv4 位址範圍帶到之後 AWS，您就可以使用範圍內的所有 IP 位址，包括第一個位址 (網路位址) 和最後一個位址 (廣播位址)。

目錄

- [使用 AWS 管理主控台和 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#)
- [僅使用 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#)

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

請依照下列步驟，使用 AWS 管理主控台和 CLI 將 IPv4 或 IPv6 CIDR 帶到 IPAM。AWS

Important

- 在開始本教學之前，請在 Amazon EC2 使用者指南中針對您的 [BYOIP 地址範圍完成上線先決條件](#)中的步驟。

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。這樣可確保您有充分的靈活性，可以跨 AWS 區域劃分您的公有 IP 地址。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定為 /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。

- 將 IPv4 位址範圍帶到之後 AWS，您就可以使用範圍內的所有 IP 位址，包括第一個位址 (網路位址) 和最後一個位址 (廣播位址)。

目錄

- [使用 AWS 管理主控台和 CLI 將您自己的 IPv4 CIDR 帶到 IPAM AWS](#)

- [使用 AWS 管理主控台，自攜 IPv6 CIDR 至 IPAM](#)

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

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

Important

- 您目前無法在 Local Zones 中佈建或公告 BYOIP 地址範圍。
- 此教學課程假設您已完成下列各節中的步驟：
 - [將 IPAM 與組 AWS 織中的帳戶整合](#).
 - [建立 IPAM](#).
- 本教學課程的每個步驟都必須由三個「Organ AWS izations」帳戶中的其中一個完成：
 - 管理帳戶。
 - 在 [將 IPAM 與組 AWS 織中的帳戶整合](#) 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 命名的設定檔和 IAM 角色](#)
- [步驟 2：建立最上層 IPAM 集區](#)
- [步驟 3。在最上層集區內建立一個區域集區](#)
- [步驟 4. 共用區域集區](#)
- [步驟 5：建立公有 IPv4 集區](#)
- [步驟 6：在公有 IPv4 集區佈建公有 IPv4 CIDR](#)
- [步驟 7：在公有 IPv4 集區中建立彈性 IP 地址](#)
- [步驟 8：建立彈性 IP 地址與 EC2 執行個體的關聯](#)
- [步驟 9：公告 CIDR](#)
- [步驟 10：清除](#)

步驟 1：建立 AWS CLI 命名的設定檔和 IAM 角色

若要以單一使用 AWS 者的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 IAM 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。有關如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱 [AWS Identity and Access Management 使用者指南中的 AWS CLI 中的使用 IAM 角色](#)。

為您將在本教學課程中使用的三個 AWS 帳戶中，每個建立一個角色和一個具名的設定檔：

- 要 `management-account` 求 Organ AWS izations 管理帳戶的設定檔。
- 設定 `ipam-account` 為 IPAM 管理員的 Organ AWS izations 成員帳戶所呼叫的設定檔。
- 要 `member-account` 求組織中組 Organ AWS izations 成員帳戶的設定檔，此設定檔將從 IPAM 集區配置 CIDR。

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。在本自學課程的其餘部分中，您會注意到範例 AWS CLI 指令將 `--profile` 選項與其中一個具名的設定檔搭配使用，以指示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)。

AWS 地區設定是您希望此 IPAM 集區可供配置使用的區域。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。

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，選擇以下其中一個選項：

- BYOIP：您正在將自己的 IPv4 或 IPv6 地址範圍 (BYOIP) 帶到此集區。
- Amazon 擁有：您希望 Amazon 將此 IPv6 地址範圍佈建到此集區。

11. 執行以下任意一項：

- 如果您在上一步驟中選擇 BYOIP，則在要佈建的 CIDR 下，選擇要為集區佈建的 CIDR。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)。請求中需內含 CIDR 和 BYOIP 訊息和憑證簽章，以便我們確認您擁有該公有空間。如需 BYOIP 必要條件清單，包括如何獲取此 BYOIP 訊息和憑證簽章，請參閱 [使用 AWS 管理主控台和 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#)。

 Important

雖然大部分佈建都會在兩小時內完成，但最多可能需要一週的時間才能完成可公開廣告範圍的佈建程序。

- 如果選擇了 Amazon 擁有，則請在網路遮罩長度下選擇從 /40 到 /52 的網路遮罩長度。預設值為 /52。

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。

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。

AWS 地區設定是您希望此 IPAM 集區可供配置使用的區域。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。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)。您選擇的服務決定了 CIDR 將廣告的 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。

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，在最上層集區內的某集區佈建 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)。建立第一個地區集區後，您可以在區域集區內建立較小的集區 (例如 /25)。
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。

步驟 4. 共用區域集區

請依照本節中的步驟，使用 AWS Resource Access Manager (RAM) 共用 IPAM 集區。

在 AWS RAM 啟用資源共用

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在共用 IPAM 集區之前，請先完成本節中的步驟，以啟用與 AWS RAM 資源共用。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile management-account` 項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，請在 <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 [啟用共用對象] 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。

使用以下方式共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共享區域集區。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](#)。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile ipam-account` 項。

若要使用共用 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. 選擇專用範圍，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 [建立資源共用]。
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的 ARN。
9. 選擇下一步。
10. 選擇AWSRAMPermissionIpamPoolByoipCidrImport權限。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 地址 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。的值`--principals`是的是的帳戶 ID **member-account**。`--permission-arns` 值為 `AWSRAMDefaultPermissionsIpamPool` 許可的 ARN。

步驟 5：建立公有 IPv4 集區

建立公有 IPv4 集區是將公有 IPv4 地址攜至 AWS 以便透過 IPAM 進行管理的必要步驟。此步驟應由將佈建彈性 IP 地址的成員帳戶完成。

Important

- 此步驟必須使用 AWS CLI，由該成員帳戶完成。

- 公用 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。

若要使用建立公用 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"
}
```

步驟 6：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。您可以使用的最不特定 IPv4 字首為 /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`)。

Important

此步驟必須使用 AWS CLI，由該成員帳戶完成。

若要使用建立公用 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。

步驟 7：在公有 IPv4 集區中建立彈性 IP 地址

完成 Amazon EC2 使用者指南中[分配彈性 IP 地址](#)中的步驟，以從公用 IPv4 集區建立彈性 IP 地址 (EIP)。當您在 AWS 管理主控台中開啟 EC2 時，配置 EIP 所在的 AWS 區域必須與您在建立用於 BYOIP CIDR 的集區時選擇的 Locale 選項相符。

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。

步驟 8：建立彈性 IP 地址與 EC2 執行個體的關聯

完成[將彈性 IP 地址與 Amazon EC2 使用者指南中的執行個體或網路界面](#)建立關聯中的步驟，以將 EIP 與 EC2 執行個體建立關聯。當您在 AWS 管理主控台中開啟 EC2 時，關聯 EIP 所在的 AWS 區域必須與您在建立用於 BYOIP CIDR 的集區時選擇的 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。

步驟 9：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 產生關聯後，您就可以在已設定服務 EC2 (EIP/ VPC) AWS 的集區中開始廣告您帶到的 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 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。

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 地址關聯](#) 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，取消 EIP 關聯的 AWS 區域必須與您在建立用於 BYOIP CIDR 的集區時選擇的 Locale 選項相符。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 地址](#) 中的步驟，以從公有 IPv4 集區釋放彈性 IP 地址 (EIP)。當您在 AWS 管理主控台中開啟 EC2 時，配置 EIP 所在的 AWS 區域必須與您在建立用於 BYOIP CIDR 的集區時選擇的 `Locale` 選項相符。

步驟 4：從公有 IPv4 集區解除佈建公有 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 中的最後一個 IP 地址。輸入網路遮罩為 /32 的 IP 地址。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-2 --pool-id ipv4pool-ec2-09037ce61cf068f9a --cidr 130.137.245.255/32 --profile member-account
```

輸出結果會顯示已解除佈建的 CIDR。

```
{
  "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
  "DeprovisionedAddresses": [
    "130.137.245.255"
  ]
}
```

Important

必須針對 CIDR 範圍中的每個 IP 地址重新執行此命令。若 CIDR 是 /24，則必須執行此命令才能解除佈建 /24 CIDR 中的全部 256 個 IP 地址。

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。

步驟 5：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。必須使用 AWS CLI 完成此步驟。

```
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。

步驟 6：刪除 RAM 共用並停用與 AWS Organizations 整合的 RAM。

此步驟必須各自由 IPAM 帳戶和管理帳戶完成。如果您使用刪 AWS CLI 除 RAM 共用並停用 RAM 整合，請使用 `--profile ipam-account` 和 `--profile management-account` 選項。

- 依序完成在 RAM 使用指南中[刪除 AWS RAM 中的資源共用和停用與 Organ AWS izations](#) 的 AWS 資源共用中的步驟，以刪除 RAM 共用並停用與 Organ AWS izations 的 RAM 整合。

步驟 7：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 來共用集區，請使用選 `--profile ipam-account` 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。

步驟 8：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 來共用集區，請使用選 `--profile ipam-account` 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。

使用 AWS 管理主控台，自攜 IPv6 CIDR 至 IPAM

請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 AWS CLI

Important

- 您目前無法在 Local Zones 中佈建或公告 BYOIP 地址範圍。
- 此教學課程假設您已完成下列各節中的步驟：
 - [將 IPAM 與組 AWS 織中的帳戶整合](#).
 - [建立 IPAM](#).
- 本教學課程的每個步驟都必須由三個「Organ AWS izations」帳戶中的其中一個完成：
 - 管理帳戶。
 - 在 [將 IPAM 與組 AWS 織中的帳戶整合](#) 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](#)
- [步驟 2. 在最上層集區內建立一個區域集區](#)
- [步驟 3. 共用區域集區](#)
- [步驟 4：建立 VPC](#)
- [步驟 5：公告 CIDR](#)
- [步驟 6：清除](#)

步驟 1：建立最上層 IPAM 集區

由於您要建立一個包含區域集區的頂層 IPAM 集區，而且我們將從區域集區分配空間給資源，因此您將在區域集區上設定地區設定，而不是頂層集區。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。

當您選擇 IPv6 時，會出現一個切換選項，讓您控制是否 AWS 可以在此集區中公開通告 CIDR。保留此選項為啟用狀態。


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. 確認 Allow CIDRs in this pool to be publicly advertisable (允許此集區中的 CIDR 可公開公告) 已選取。
10. 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。

AWS 地區設定是您希望此 IPAM 集區可供配置使用的區域。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。

11. 在公有 IP 來源下，預設會選取 BYOIP。
12. 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，將 IPv6 CIDR 佈建至頂層集區內的集區時，您可以使用的最特定 IPv6 位址範圍是公開廣告的 CIDR 的 /48，而不可公開廣告的 CIDR 則為 /60。請求中需內含 CIDR 和 BYOIP 訊息和憑證簽章，以便我們確認您擁有該公有空間。如需 BYOIP 必要條件清單，包括如何獲取此 BYOIP 訊息和憑證簽章，請參閱 [使用 AWS 管理主控台和 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#)。

 Important

雖然大部分佈建都會在兩小時內完成，但最多可能需要一週的時間才能完成可公開廣告範圍的佈建程序。

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。

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。

AWS 地區設定是您希望此 IPAM 集區可供配置使用的區域。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)。您選擇的服務決定了 CIDR 將廣告的 AWS 服務。目前唯一的選擇是 EC2 (EIP/VPC)，也就是說，從這個集區配置的 CIDR 可以廣告用於 Amazon EC2 服務和 Amazon VPC 服務 (適用於與虛擬私人雲端相關聯的 CIDR)。
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，將 IPv6 CIDR 佈建至頂層集區內的集區時，您可以使用的最特定 IPv6 位址範圍是公開廣告的 CIDR 的 /48，而不可公開廣告的 CIDR 則為 /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 (地區設定) 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

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

在 AWS RAM 啟用資源共用

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在共用 IPAM 集區之前，請先完成本節中的步驟，以啟用與 AWS RAM 資源共用。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile management-account` 項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，開啟 AWS RAM 主控台，網址為 <https://console.aws.amazon.com/ram/>。
2. 在左側導覽窗格中，選擇 [設定]，選擇 [啟用共用對象] 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。

使用以下方式共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共享區域集區。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](#)。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile ipam-account` 項。

若要使用共用 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. 選擇專用範圍，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 [建立資源共用]。
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的 ARN。
9. 選擇下一步。
10. 選擇 `AWSRAMPermissionIpamPoolByoipCidrImport` 權限。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 地址 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。的值 `--principals` 是帳戶 ID **member-account**。`--permission-arns` 值為 `AWSRAMDefaultPermissionsIpamPool` 許可的 ARN。

步驟 4：建立 VPC

完成《Amazon VPC 使用者指南》中 [建立 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，您建立 VPC 所在的 AWS 區域必須與您在建立用於 BYOIP CIDR 的集區時所選擇的Locale選項相符。
- 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。

建立 VPC 時，AWS 會將 IPAM 集區中的 CIDR 配置給虛擬私人雲端。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，您就可以在已設定服務 EC2 (EIP/ VPC) AWS 的集區中開始廣告您帶到的 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 使用者指南》中[刪除 VPC](#)中的步驟。當您在 AWS 管理主控台中開啟 VPC 時，刪除 VPC 的 AWS 地區必須符合您在建立用於 BYOIP CIDR 的集區時Locale選擇的選項。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 Organ AWS izations 的 RAM 整合

此步驟必須各自由 IPAM 帳戶和管理帳戶完成。

- 依序完成在 RAM 使用指南中[刪除 AWS RAM 中的資源共用和停用與 Organ AWS izations](#)的AWS 資源共用中的步驟，以刪除 RAM 共用並停用與 Organ AWS izations 的 RAM 整合。

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 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS

請按照下列步驟操作，僅使用 CLI 將 IPv4 或 IPv6 CIDR 帶到 IPAM。AWS

Important

- 在開始本教學之前，請在 Amazon EC2 使用者指南中針對您的 [BYOIP 地址範圍完成上線先決條件](#) 中的步驟。

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。這樣可確保您有充分的靈活性，可以跨 AWS 區域劃分您的公有 IP 地址。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定為 /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。

- 將 IPv4 位址範圍帶到之後 AWS，您就可以使用範圍內的所有 IP 位址，包括第一個位址 (網路位址) 和最後一個位址 (廣播位址)。

目錄

- [僅使用 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#)
- [僅使用 CLI 將您自己的 IPv6 CIDR 帶到 IPAM AWS](#)

僅使用 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS

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

- 您目前無法在 Local Zones 中佈建或公告 BYOIP 地址範圍。
- 此教學課程假設您已完成下列各節中的步驟：
 - [將 IPAM 與組 AWS 織中的帳戶整合](#).
 - [建立 IPAM](#).
- 本教學課程的每個步驟都必須由三個「Organ AWS izations」帳戶中的其中一個完成：
 - 管理帳戶。
 - 在 [將 IPAM 與組 AWS 織中的帳戶整合](#) 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 命名的設定檔和 IAM 角色](#)
- [步驟 2：建立 IPAM](#)
- [步驟 3：建立最上層 IPAM 集區](#)
- [步驟 4：在最上層集區佈建 CIDR](#)
- [步驟 5：在最上層集區內建立一個區域集區。](#)
- [步驟 6：在區域集區中佈建 CIDR](#)
- [步驟 7. 共用區域集區](#)
- [步驟 8：建立公有 IPv4 集區](#)
- [步驟 9：在公有 IPv4 集區佈建公有 IPv4 CIDR](#)
- [步驟 10：在公有 IPv4 集區中建立彈性 IP 地址](#)
- [步驟 11：公告 CIDR](#)
- [步驟 12：清除](#)

步驟 1：建立 AWS CLI 命名的設定檔和 IAM 角色

若要以單一使用 AWS 者的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 IAM 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。有關如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱 [AWS Identity and Access Management 使用者指南](#) 中的 [AWS CLI 中的使用 IAM 角色](#)。

為您將在本教學課程中使用的三個 AWS 帳戶中，每個建立一個角色和一個具名的設定檔：

- 要 `management-account` 求「Organ AWS izations」管理帳戶的設定檔。
- 設定 `ipam-account` 為 IPAM 管理員的 Organ AWS izations 成員帳戶所呼叫的設定檔。
- 要 `member-account` 求組織中組 Organ AWS izations 成員帳戶的設定檔，此設定檔將從 IPAM 集區配置 CIDR。

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。在本自學課程的其餘部分中，您會注意到範例 AWS CLI 指令將 `--profile` 選項與其中一個具名的設定檔搭配使用，以指示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。

若要為您的所有 AWS 資源建立 IPv4 位址集區，請使用 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)。請求中需內含 CIDR 和 BYOIP 訊息和憑證簽章，以便我們確認您擁有該公有空間。如需 BYOIP 必要條件清單，包括如何獲取此 BYOIP 訊息和憑證簽章，請參閱 [僅使用 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#)。

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 時才需新增 `--cidr-authorization-context`。最上層集區內的區域集區可省略 `--cidr-authorization-context` 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. 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-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --cidr-authorization-  
context Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|  
RSAPSS",Signature="W3gdQ9PZHLjPmInGM~cvGx~KCIsmAu0P7EN07VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d  
hApR89Kt6GxRY0dRaNx8yt-uoZWzxcT2yIhWngy-  
du9pnEHB0X6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXE1T5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-  
oS9AZ1afBbrFxrjFWRCTJhc7Cg3ASbR0-VWNci-  
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpggcWGVJdQ__" --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

雖然大部分佈建都會在兩小時內完成，但最多可能需要一週的時間才能完成可公開廣告範圍的佈建程序。

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
```

下列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。集區上需有 `--locale`，且其必須是您在建立 IPAM 時設定的作業區域之一。AWS 地區設定是您希望此 IPAM 集區可供配置使用的區域。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。

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`。您選擇的服務決定了 CIDR 將廣告的 AWS 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 AWS CLI 建立區域集區

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。請注意，在最上層集區內的某集區佈建 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)。建立第一個地區集區後，您可以在區域集區內建立較小的集區 (例如 /25)。

此步驟必須由 IPAM 帳戶完成。

若要使用將 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. 共用區域集區

請依照本節中的步驟，使用 AWS Resource Access Manager (RAM) 共用 IPAM 集區。

在 AWS RAM 啟用資源共用

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在共用 IPAM 集區之前，請先完成本節中的步驟，以啟用與 AWS RAM 資源共用。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile management-account` 項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，請在 <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 [啟用共用對象] 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。

使用以下方式共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共享區域集區。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](#)。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile ipam-account` 項。

若要使用共用 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. 選擇專用範圍，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 [建立資源共用]。
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的 ARN。
9. 選擇下一步。
10. 選擇AWSRAMPermissionIpamPoolByoipCidrImport權限。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 地址 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。的值--principals是的是的帳戶 ID **member-account**。--permission-arns 值為 AWSRAMDefaultPermissionsIpamPool 許可的 ARN。

步驟 8：建立公有 IPv4 集區

建立公有 IPv4 集區是將公有 IPv4 地址攜至 AWS 以便透過 IPAM 進行管理的必要步驟。此步驟通常由不同的帳戶完成，該 AWS 帳戶想要佈建彈性 IP 地址。

此步驟必須由該成員帳戶完成。

Important

公用 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。

若要使用建立公用 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"  
}
```

步驟 9：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。

此步驟必須由該成員帳戶完成。

若要使用建立公用 IPv4 集區 AWS CLI

- 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"
    }
  ]
}
```

步驟 10：在公有 IPv4 集區中建立彈性 IP 地址

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。

若要從公用 IPv4 集區建立 EIP，請使用 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"
    }
  ]
}
```

步驟 11：公告 CIDR

本節中的步驟必須由 IPAM 帳戶完成。將彈性 IP 位址 (EIP) 與執行個體或 Elastic Load Balancer 產生關聯之後，您就可以開始在已--aws-service ec2定義的集區中廣告您帶到 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。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 IPAM 帳戶完成。

開始使用 CIDR 做廣告 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"
  }
}
```

步驟 12：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 即將使用的集區時所輸入的 `--locale` 選項相符。

使用清理 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": []
  }
]
}

```

5. 釋出公有 IPv4 集區之 CIDR 中的最後一個 IP 地址。輸入網路遮罩為 /32 的 IP 地址。必須針對 CIDR 範圍中的每個 IP 地址重新執行此命令。若 CIDR 是 /24，則必須執行此命令才能解除佈建 /24 CIDR 中的全部 256 個 IP 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 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.255/32 --profile member-account
```

輸出結果會顯示已解除佈建的 CIDR。

```

{
  "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
  "DeprovisionedAddresses": [
    "130.137.245.255"
  ]
}

```

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": []
    }
  ]
}
```

7. 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` 的值必須與您在建立 BYOIP CIDR 即將使用的集區時所輸入的地區設定選項相符。

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-0d8f3646b61ca5987 --profile ipam-account
```

該輸出結果會顯示 IPAM 中的分配情況。

```
{
  "IpamPoolAllocations": []
}
```

8. 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"
  }
}
```

9. 刪除 RAM 共用並停用與 AWS Organizations 整合的 RAM。依序完成在 RAM 使用指南中[刪除 AWS RAM 中的資源共用和停用與 Organ AWS izations](#) 的 AWS 資源共用中的步驟，以刪除 RAM 共用並停用與 Organ AWS izations 的 RAM 整合。

此步驟必須各自由 IPAM 帳戶和管理帳戶完成。如果您使用刪 AWS CLI 除 RAM 共用並停用 RAM 整合，請使用 `--profile ipam-account` 和 `--profile management-account` 選項。

10. 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"
  }
}
```

11. 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"
  }
}
```

12. 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"
  }
}

```

13. 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"
    },
],
}
}
```

僅使用 CLI 將您自己的 IPv6 CIDR 帶到 IPAM AWS

請依照下列步驟，僅使用 AWS CLI，自攜 IPv6 CIDR 至 IPAM，並分配 VPC。

Important

- 您目前無法在 Local Zones 中佈建或公告 BYOIP 地址範圍。
- 此教學課程假設您已完成下列各節中的步驟：
 - [將 IPAM 與組 AWS 織中的帳戶整合](#).
 - [建立 IPAM](#).
- 本教學課程的每個步驟都必須由三個「Organ AWS izations」帳戶中的其中一個完成：
 - 管理帳戶。
 - 在 [將 IPAM 與組 AWS 織中的帳戶整合](#) 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 命名的設定檔和 IAM 角色](#)
- [步驟 2：建立 IPAM](#)
- [步驟 3：建立 IPAM 集區](#)
- [步驟 4：在最上層集區佈建 CIDR](#)
- [步驟 5：在最上層集區內建立一個區域集區。](#)
- [步驟 6：在區域集區中佈建 CIDR](#)
- [步驟 7. 共用區域集區](#)
- [步驟 8：使用 IPv6 CIDR 建立 VPC](#)
- [步驟 9：公告 CIDR](#)

• [步驟 10：清除](#)

步驟 1：建立 AWS CLI 命名的設定檔和 IAM 角色

若要以單一使用 AWS 者的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 IAM 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。有關如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱 AWS Identity and Access Management 使用者指南中的 [AWS CLI 中的使用 IAM 角色](#)。

為您將在本教學課程中使用的三個 AWS 帳戶中，每個建立一個角色和一個具名的設定檔：

- 要 `management-account` 求「Organ AWS izations」管理帳戶的設定檔。
- 設定 `ipam-account` 為 IPAM 管理員的 Organ AWS izations 成員帳戶所呼叫的設定檔。
- 要 `member-account` 求組織中組 Organ AWS izations 成員帳戶的設定檔，此設定檔將從 IPAM 集區配置 CIDR。

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。在本自學課程的其餘部分中，您會注意到範例 AWS CLI 指令將 `--profile` 選項與其中一個具名的設定檔搭配使用，以指示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。

選擇是否要讓此 IPAM 集區 CIDR 透 AWS 過公用網際網路廣告 (--publicly-advertisable或)。--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。

若要為所有 AWS 資源建立 IPv6 位址集區，請使用 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，將 IPv6 CIDR 佈建至頂層集區內的集區時，您可以使用的最特定 IPv6 位址範圍是公開廣告的 CIDR 的 /48，而不可公開廣告的 CIDR 則為 /60。請求中需內含 CIDR 和 BYOIP 訊息和憑證簽章，以便我們確認您擁有該公有空間。如需 BYOIP 必要條件清單，包括如何獲取此 BYOIP 訊息和憑證簽章，請參閱 [僅使用 CLI 將您自己的公用 IPv4 CIDR 帶到 IPAM AWS](#)。

只有在最上層集區中佈建 BYOIP CIDR 時才需新增 `--cidr-authorization-context`。最上層集區內的區域集區可省略 `--cidr-authorization-context` 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. 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-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-CR7HqMwzcgdS9R1pBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxFnp7RAJDvF1mBwxmSgH~CvP6L0N3y00Xmp4JENB9uM7sM1u6oeoutGyyhXFeYPz1GSRdcdfKNKaimvPCqVsxGN5AwSi1KQ8byNqoa~G3dvs8ueSawispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --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

雖然大部分佈建都會在兩小時內完成，但最多可能需要一週的時間才能完成可公開廣告範圍的佈建程序。

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
```

下列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`。您選擇的服務決定了 CIDR 將廣告的 AWS 服務。目前唯一的選擇是 `ec2`，這表示從這個集區配置的 CIDR 可廣告用於 Amazon EC2 服務和 Amazon VPC 服務 (適用於與 VPC 相關聯的 CIDR)。

使用 AWS CLI 建立區域集區

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，將 CIDR 佈建至頂層集區內的集區時，您可以帶來的最特定 IPv6 位址範圍是 /48 (適用於可公開廣告的 CIDR)，而不可公開廣告的 CIDR 則為 /60。

此步驟必須由 IPAM 帳戶完成。

若要使用將 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

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

在 AWS RAM 啟用資源共用

建立 IPAM 之後，您會想要與組織中的其他帳戶共用區域集區。在共用 IPAM 集區之前，請先完成本節中的步驟，以啟用與 AWS RAM 資源共用。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile management-account` 項。

啟用資源共用

1. 使用 AWS Organizations 管理帳戶，請在 <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 [啟用共用對象] 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。

使用以下方式共用 IPAM 集區 AWS RAM

在本節中，您將與另一個 AWS Organizations 成員帳戶共享區域集區。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](#)。如果您使用啟 AWS CLI 用資源共用，請使用選 `--profile ipam-account` 項。

若要使用共用 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. 選擇專用範圍，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 [建立資源共用]。
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的 ARN。
9. 選擇下一步。
10. 選擇 `AWSRAMPermissionIpamPoolByoipCidrImport` 權限。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。

- 若要允許 **member-account** 帳戶從 IPAM 集區配置 IP 地址 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。的值 `--principals` 是帳戶 ID **member-account**。`--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。

若要使用 AWS CLI

- 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

建立具有在 IPAM 中配置 CIDR 的 VPC 之後，您就可以開始在已定義的集區中廣告您帶到 AWS 的 CIDR。--aws-service ec2 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。

開始使用 CIDR 做廣告 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。

使用清理 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。依序完成在 RAM 使用指南中 [刪除 AWS RAM 中的資源共用和停用與 Organ AWS izations](#) 的 AWS 資源共用中的步驟，以刪除 RAM 共用並停用與 Organ AWS izations 的 RAM 整合。

此步驟必須各自由 IPAM 帳戶和管理帳戶完成。如果您使用刪 AWS CLI 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"  
      }  
    ]  
  }  
}
```


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，您可以將 CIDR 從公用 IPv4 集區移至 IPAM。您無法將 IPv6 CIDR 移動至 IPAM。

本教學假設您已經使用在 [Amazon EC2 中 AWS 使用自己的 IP 地址 \(BYOIP\)](#) 中所述的程序成功引入 IP 位址範圍，現在您想要將該 IP 位址範圍傳輸到 IPAM。如果您是第一次使 AWS 用新的 IP 位址，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](#)。

Important

- 本教學課程假設您已完成 [建立 IPAM](#) 中的步驟。
- 本教程的每個步驟必須由以下兩個 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 命名的設定檔和 IAM 角色](#)
- [步驟 2：取得您 IPAM 的公有範圍 ID](#)
- [步驟 3：建立 IPAM 集區](#)
- [步驟 4：使用分享 IPAM 集區 AWS RAM](#)
- [步驟 5：將現有的 BYOIP IPV4 CIDR 傳輸至 IPAM](#)
- [步驟 6：檢視 IPAM 中的 CIDR](#)
- [步驟 7：清除](#)

步驟 1：建立 AWS CLI 命名的設定檔和 IAM 角色

若要以單一使用 AWS 者的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 IAM 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。有關如何為 AWS 帳戶建立 IAM 角色和具名設定檔的詳細資訊，請參閱 [AWS Identity and Access Management 使用者指南](#) 中的 [AWS CLI 中的使用 IAM 角色](#)。

為您將在本教學課程中使用的三個 AWS 帳戶中，每個建立一個角色和一個具名的設定檔：

- 要 `ipam-account` 求做為 IPAM 管理員之 AWS 帳戶的設定檔。
- `byoip-owner-account` 針對擁有 BYOIP CIDR 之組織中 AWS 帳戶所呼叫的設定檔。

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。在本自學課程的其餘部分中，您會注意到範例 AWS CLI 指令將 `--profile` 選項與其中一個具名的設定檔搭配使用，以指示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`。您選擇的服務決定了 CIDR 將廣告的 AWS 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 AWS CLI 為傳輸的 BYOIP CIDR 建立 IPv4 地址集區

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：您將需要 `OwnerId` 在下一步中。

```
{
  "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：使用分享 IPAM 集區 AWS RAM

請遵循本節中的步驟來共用 IPAM 集區，以 AWS RAM 便其他 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 AWS CLI 共用 IPv4 地址集區

1. 檢視 IPAM 集區的可用 AWS RAM 權限。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"  
  
  }  
  
}
```

由於在 RAM 中建立資源共用，此 byoip-owner-account 帳號現在可以將 CIDR 移至 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 位址範圍帶到之後 AWS，您就可以使用範圍內的所有 IP 位址，包括第一個位址 (網路位址) 和最後一個位址 (廣播位址)。

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權限：

- ec2:MoveByoipCidrToIpam
- ec2:ImportByoipCidrToIpam

Note

您可以在此步驟中使 AWS CLI 用 AWS Management Console 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 指令會使用將 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` 值為 BYOIP CIDR 的「AWS 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
```

下列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。

使用以檢視 IPAM 集區中傳輸的 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` 值為 BYOIP CIDR 的「AWS 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。

若要使用清理本自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：使用分享 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。請確定此 `--region` 值符合 BYOIP CIDR 的「AWS 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 集區之 CIDR 中的最後一個 IP 地址。輸入網路遮罩為 /32 的 IP 地址。必須針對 CIDR 範圍中的每個 IP 地址重新執行此命令。若 CIDR 是 /24，則必須執行此命令才能解除佈建 /24 CIDR 中的全部 256 個 IP 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 deprovision-public-ipv4-pool-cidr --region us-east-1 --profile byoip-owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.255/32
```

輸出結果會顯示已解除佈建的 CIDR。

```
{
  "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
```

```

    "DeprovisionedAddresses": [
        "130.137.249.255"
    ]
}

```

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，使用公有範圍和 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 CIDR 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 Create pool (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 Create pool (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 Create pool (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 Create pool (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，如果希望該子網路集區可供其他 AWS 帳戶使用，則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 Delete (刪除)。
7. [刪除子網路](#)。
8. [刪除 VPC](#)。

清理完成。

IPAM 中的 Identity and Access Management

AWS 使用安全登入資料來識別您並授予您對 AWS 資源的存取權。您可以使用 AWS Identity and Access Management (IAM) 的功能，來允許其他使用者、服務和應用程式完整地或有所限制地使用您的 AWS 資源，而不共享您的安全憑證。

本節說明專為 IPAM 建立的 AWS 服務連結角色，以及附加至 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 VPC 身分和存取管理的詳細資訊，請參閱《Amazon VPC 使用者指南》中的[Amazon VPC 的 Identity and Access Management](#)。

目錄

- [IPAM 的服務連結角色](#)
- [IPAM 的 AWS 受管政策](#)
- [範例 政策](#)

IPAM 的服務連結角色

AWS Identity and Access Management 中的服務連結角色 (IAM) 可讓 AWS 服務能代表您呼叫其他 AWS 服務。如需服務連結角色的詳細資訊，請參閱《IAM 使用者指南》中的[使用服務連結角色](#)。

IPAM 目前只有一個服務連結角色：AWSServiceRoleForIPAM。

授予服務連結角色的許可

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[IPAM 的 AWS 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 與組 AWS 織中的帳戶整合](#)，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](#)。

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。

請依照下列步驟執行，透過 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](#)。

IPAM 的 AWS 受管政策

如果您以單一 AWS 帳戶使用 IPAM 並建立一個 IPAM，則會自動在您的 IAM 帳戶中建立 `AWSIPAMServiceRolePolicy` 受管政策，並連接至 `AWSServiceRoleForIPAM` [服務連結角色](#)。

如果啟用 IPAM 與 AWS Organizations 的整合，則會自動在您的 IAM 帳戶以及您的每個 AWS Organizations 成員帳戶中建立 `AWSIPAMServiceRolePolicy` 受管政策，並將該受管政策連接至 `AWSServiceRoleForIPAM` 服務連結角色。

此受管政策可讓 IPAM 執行以下操作：

- 監控所有 AWS 組織成員中與聯網資源關聯的 CIDR。
- 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。

下例顯示建立之受管政策的詳細資訊。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Sid": "IPAMDiscoveryDescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchMetricsPublishActions",
      "Effect": "Allow",
      "Action": "cloudwatch:PutMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/IPAM"
        }
      }
    }
  ]
}

```

上例中的第一個陳述式可讓 IPAM 監控您的單一 AWS 帳戶或您 AWS Organization 成員使用的 CIDR。

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。AWS 管理主控台會透過這些指標來顯示 IPAM 集區和範圍內的配置相關資料。如需更多詳細資訊，請參閱 [使用 IPAM 儀表板監控 CIDR 使用情況](#)。

AWS 受管政策更新

檢視自本服務開始追蹤受管政策異動以來的 AWS 受管政策更新相關詳細資訊。

變更	描述	日期
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
AWSIPAMServiceRolePolicy	兩個動作已新增至 AWSIPAMServiceRole	2023 年 1 月 25 日

變更	描述	日期
	Policy 受管政策 (ec2:GetIpamDiscoveredAccounts 和 ec2:GetIpamDiscoveredResourceCidrs)，可讓 IPAM 在資源探索期間監控 AWS 帳戶和資源 CIDR。	
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用於完整 IPAM 使用的所有相關 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，您可能需要針對 AWS Organizations、AWS Resource Access Manager(RAM) 和 Amazon CloudWatch 等服務加入其他 IAM 動作。

```
{
  "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](#)。

名稱	預設	可調整
Amazon 提供的 IPv6 CIDR 區塊網路遮罩長度	/52	是。請聯絡 AWS 支援中心，如《AWS 一般參考》中的 AWS Service Quotas 所述。
每個區域集區的 Amazon 提供的 IPv6 CIDR 區塊	1	是。請聯絡 AWS 支援中心，如《AWS 一般參考》中的 AWS Service Quotas 所述。
可帶入 IPAM 的自治系統編號 (ASN)	5	是。請聯絡 AWS 支援中心，如《AWS 一般參考》中的 AWS Service Quotas 所述。
每個集區的 CIDR 數目	50	是
每個組織的 IPAM 管理員	1	否
每個區域的 IPAM	1	否
集區深度 (集區層數)	10	是
每個範圍的集區數目	50	是
每個 IPAM 的資源探索關聯	5	是

名稱	預設	可調整
每個區域的資源探索	1	否
資源使用率指標	50	是。請聯絡 AWS 支援中心，如《AWS 一般參考》中的 AWS Service Quotas 所述。
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。

IPAM 定價

本節描述如何檢視與定價相關的資訊和您目前的 IPAM 成本。

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。

以下列方式檢視目前的成本和用量 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. [請在以下位置開啟 AWS Cost Management 主控台。](https://console.aws.amazon.com/cost-management/home) <https://console.aws.amazon.com/cost-management/home>
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。他們每個人都代表一個不同的 AWS 區域。
5. 按一下 Apply (套用)。

舉例來說，如果您選取 USE1-IP AddressManager IP 小時 (小時)，而 us-east-1 是您的 IP AM 本地區域，則您會看到 IPAM 在所有區域中按 IPAM 計費的作用中 IP 小時數和費用。如果以小時為單位的使用量為 18，這意味著您可以在 18 小時內擁有 1 個活動 IP 地址，3 個不同區域中的 3 個 IP 地址每個活動時間為 6 小時，或者這些 IP 地址的任何組合最多可達 18 小時。

如需詳細資訊 AWS Cost Explorer，請參閱 AWS Cost Management 使用者指南 AWS Cost Explorer 中的使用 [分析成本](#)。

相關資訊

以下相關資源可協助您使用此服務。

- [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。

IPAM 的文件歷史紀錄

下表說明 IPAM 的各個版本。

功能	說明	版本日期
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)	現在，可以將自有的自治系統編號 (ASN) 帶入 AWS。	2023 年 11 月 17 日
AWS 受管政策更新 - 更新至現有政策	現有 AWSIPAMServiceRolePolicy 已更新。	2023 年 11 月 17 日
AWS 受管政策更新 - 更新至現有政策	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
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 - 更新至現有政策	現有 AWSIPAMServiceRolePolicy 已更新。	2023 年 1 月 25 日

功能	說明	版本日期
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 的帳戶共用 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。如需更多詳細資訊，請參閱 建立 IPv6 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。