



IP 地址管理器

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: IP 地址管理器

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆或者贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 IPAM？	1
IPAM 的工作原理	2
IPAM 入门	3
访问 IPAM	3
为 IPAM 配置集成选项	4
将 IPAM 与 AWS Organization 中的账户集成	4
将 IPAM 与组织外部的账户集成	7
将 IPAM 用于单个账户	9
创建 IPAM	9
计划 IP 地址预置	12
示例 IPAM 池计划	13
创建 IPv4 池	15
创建 IPv6 池	23
分配 CIDR	30
创建使用 IPAM 池 CIDR 的 VPC	30
手动将 CIDR 分配到池以预留 IP 地址空间	31
管理 IPAM 中的 IP 地址空间	33
使用 IPAM 自动更新前缀列表	34
它解决的问题	34
工作原理	34
何时使用	34
先决条件	35
设置步骤	35
更改 VPC CIDR 的监控状态	40
创建额外范围	41
删除 IPAM	42
删除池	44
删除范围	45
从池中取消预置 CIDR	46
编辑 IPAM 池	47
启用成本分配	48
将 VPC IPAM 与 Infoblox 基础设施集成	49
集成过程概述	49
何时使用此集成	49

先决条件	35
用于 Infoblox 的 IAM 角色	50
在 VPC IPAM 中配置 Infoblox 集成	50
后续步骤	51
启用预置私有 IPv6 GUA CIDR	51
强制使用 IPAM 通过 SCP 进行 VPC 创建	53
创建 VPC 时强制使用 IPAM	53
创建 VPC 时强制使用 IPAM 池	54
对除给定 OU 列表之外的所有 OU 强制实施 IPAM	55
从 IPAM 中排除组织单位	56
OU 排除项工作原理	56
添加或移除 OU 排除项	58
修改 IPAM 等级	63
修改 IPAM 运营区域	65
将 CIDR 预置到池	66
在范围之间移动 VPC CIDR	67
定义 IPv4 分配策略	68
释放分配	73
使用 AWS RAM 共享 IPAM 池	75
使用资源发现	77
创建资源发现	78
查看资源发现详细信息	79
共享资源发现	81
将资源发现与 IPAM 关联	83
取消关联资源发现	84
删除资源发现	84
跟踪 IPAM 中的 IP 地址使用情况	86
使用 IPAM 控制面板监控 CIDR 使用情况	86
按资源监控 CIDR 使用情况	89
使用 Amazon CloudWatch 监控 IPAM	92
管理警报	93
池和范围指标	94
资源利用率指标	97
查看 IP 地址历史记录	102
查看公有 IP 见解	105
教程	109

开始通过 AWS CLI 使用 IPAM	109
先决条件	35
创建 IPAM	110
获取 IPAM 范围 ID	110
创建顶级 IPv4 池	110
创建区域 IPv4 池	111
创建开发 IPv4 池	112
创建使用 IPAM 池 CIDR 的 VPC	113
验证 IPAM 池的分配情况	114
故障排除	114
清理资源	115
后续步骤	116
使用控制台创建 IPAM 和池	116
前提条件	35
AWS Organizations 如何与 IPAM 集成	117
步骤 1：委派 IPAM 管理员	118
步骤 2：创建 IPAM	119
步骤 3：创建顶级 IPAM 池	122
步骤 4：创建区域 IPAM 池	127
步骤 5：创建预生产开发池	131
步骤 6：共享 IPAM 池	135
步骤 7：创建一个 VPC，其具有从 IPAM 池分配的 CIDR	140
步骤 8：清除	144
使用 AWS CLI 创建 IPAM 和池	145
步骤 1：在企业中启用 IPAM	146
步骤 2：创建 IPAM	147
步骤 3：创建 IPv4 地址池	149
步骤 4：向顶级池预置 CIDR	150
步骤 5。使用来自顶级池的 CIDR 创建区域池	151
步骤 6：向区域池预置 CIDR	153
第 7 步。创建 RAM 共享以启用跨账户的 IP 分配	155
步骤 8：创建 VPC	156
第 9 步。清理	156
使用 AWS CLI 查看 IP 地址历史记录	157
概述	157
场景	158

自带 ASN 到 IPAM 中	165
ASN 的载入先决条件	166
教程步骤	167
将 IP 地址带入 IPAM	170
验证域控制权	171
使用 AWS 控制台和 CLI 实现 BYOIP	177
仅使用 AWS CLI 实现 BYOIP	200
使用 IPAM 自带 IP 到 CloudFront	244
将 BYOIP IPv4 CIDR 传输到 IPAM	247
第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色	248
步骤 2：获取 IPAM 的公有范围 ID	249
步骤 3：创建 IPAM 池	249
步骤 4：使用 AWS RAM 共享 IPAM 池	251
步骤 5：将现有的 BYOIP IPV4 CIDR 传输到 IPAM	254
步骤 6：在 IPAM 中查看 CIDR	256
步骤 7：清除	256
为子网 IP 分配规划 VPC IP 地址空间	259
第 1 步：创建 VPC	261
步骤 2：创建资源规划池	261
步骤 3：创建子网池	262
步骤 4：创建子网	263
步骤 5：清除	263
从 IPAM 池中分配连续弹性 IP 地址	264
步骤 1：创建 IPAM	265
步骤 2：创建 IPAM 池并预置 CIDR	267
步骤 3：从池中分配弹性 IP 地址	271
步骤 4：将弹性 IP 地址与 EC2 实例相关联	272
步骤 5：跟踪和监控池使用情况	272
清理	274
IPAM 中的 Identity and Access Management	275
IPAM 的服务相关角色	275
服务相关角色权限	275
创建服务相关角色	275
编辑服务相关角色	276
删除服务相关角色	277
IPAM 的托管策略	277

对 AWS 托管策略的更新	279
策略示例	281
配额	284
定价	287
查看定价信息	287
使用 AWS Cost Explorer 查看您当前的费用和使用情况	287
相关信息	288
文档历史记录	289

什么是 IPAM ？

Amazon VPC IP 地址管理器 (IPAM) 是一项 VPC 功能，可让您更轻松计划、跟踪和监控 AWS 工作负载的 IP 地址。您可以使用 IPAM 自动化工作流，从而更加高效地管理 IP 地址。

您可使用 IPAM 执行以下操作：

- 将 IP 地址空间组织到路由域和安全域
- 监控正在使用的 IP 地址空间并监控正在根据业务规则使用空间的资源
- 查看企业中 IP 地址分配的历史记录
- 使用特定的业务规则自动将 CIDR 分配给 VPC
- 对网络连接问题进行故障排除
- 启用自带 IP (BYOIP) 地址的跨区域和跨账户共享
- 向池预置 Amazon 提供的连续 IPv6 CIDR 块以创建 VPC

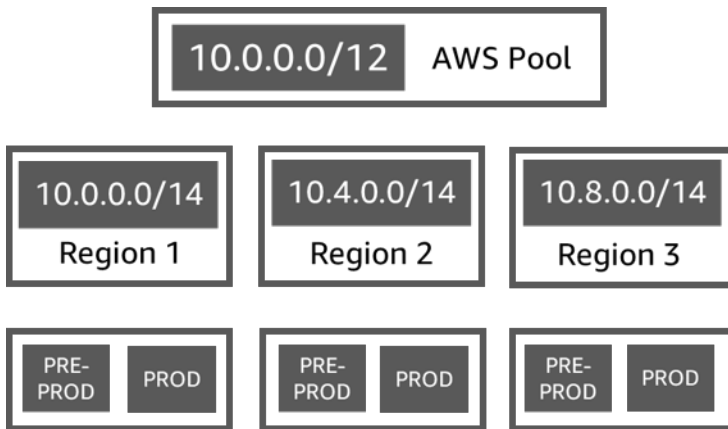
本指南由以下部分组成：

- [IPAM 的工作原理](#)：IPAM 概念和术语。
- [IPAM 入门](#)：通过 AWS Organizations 启用公司范围内的 IP 地址管理，创建 IPAM 和计划 IP 地址使用的步骤。
- [管理 IPAM 中的 IP 地址空间](#)：管理 IPAM、范围、池和分配的步骤。
- [跟踪 IPAM 中的 IP 地址使用情况](#)：使用 IPAM 监控和跟踪 IP 地址使用情况的步骤。
- [Amazon VPC IP 地址管理器教程](#)：创建 IPAM 和池、分配 VPC CIDR 并将公有 IP 地址 CIDR 自带到 IPAM 中的详细分步教程。

IPAM 的工作原理

为了帮助您开始使用 IPAM，本主题介绍了一些主要概念。

下图显示了顶级 IPAM 池内多个 AWS 区域的 IPAM 池层次结构。每个 AWS 区域池中有两个 IPAM 开发池，一个池用于预生产，一个池用于生产资源。有关 IPAM 概念的更多信息，请参阅示意图下方的说明。



要使用 Amazon VPC IP 地址管理器，您首先需要创建 IPAM。

创建 IPAM 时，您可以选择要在其中创建 IPAM 的 AWS 区域。创建 IPAM 时，AWS VPC IPAM 会自动为 IPAM 创建两个范围。范围以及池和分配是 IPAM 的关键组成部分。

- 范围是 IPAM 中最高级别的容器。创建 IPAM 时，系统将自动为您创建默认公有范围和默认私有范围。每个范围代表单个网络的 IP 空间。私有范围适用于所有无法向互联网公布的 IP 地址。公有范围通常适用于可以从 AWS 向互联网公布的所有 IP 地址。请注意，在[将 BYOIPv6 地址预置到 IPAM 池](#)时，您可以将这些地址配置为不可公开发布，尽管其属于公有范围。范围使您能够跨多个未连接的网络重复使用 IP 地址，而不会导致 IP 地址重叠或冲突。在范围内，您可以创建 IPAM 池。
- 池是连续 IP 地址范围（或 CIDR）的集合。IPAM 池使您能够根据路由和安全需求组织 IP 地址。您可以在一个顶级池中拥有多个池。例如，如果您对开发和生产应用程序有不同的路由和安全需求，则可以为每个应用程序创建一个池。在 IPAM 池中，您将 CIDR 分配给 AWS 资源。
- 分配是从一个 IPAM 池到另一个资源或 IPAM 池的 CIDR 分配。当您创建 VPC 并为 VPC 的 CIDR 选择 IPAM 池时，CIDR 将从预置给 IPAM 池的 CIDR 中分配。您可以使用 IPAM 监控和管理分配。

IPAM 可以管理并监控公有和私有 IPv6 空间。有关公有和私有 IPv6 地址的更多信息，请参阅《Amazon VPC 用户指南》中的[IPv6 地址](#)。

要开始使用并创建 IPAM，请参阅[IPAM 入门](#)。

IPAM 入门

按照本部分中的步骤来开始使用 IPAM。本部分旨在帮助您快速开始使用 IPAM，但您可能会发现，通过本部分中的步骤所能实现的目标并不符合您的需求。有关使用 IPAM 的不同方式的信息，请参阅 [计划 IP 地址预置](#) 和 [Amazon VPC IP 地址管理器教程](#)。

在本部分中，您将首先访问 IPAM，然后决定是否要委托 IPAM 账户。到本部分结束时，您将已经创建一个 IPAM，创建了多个 IP 地址池，并将池中的 CIDR 分配给了 VPC。

任务

- [访问 IPAM](#)
- [为 IPAM 配置集成选项](#)
- [创建 IPAM](#)
- [计划 IP 地址预置](#)
- [从 IPAM 池中分配 CIDR](#)

访问 IPAM

与其他 AWS 服务一样的是，您可以使用以下方法创建、访问和管理 IPAM：

- AWS 管理控制台：提供您可用来创建和管理 IPAM 的 Web 界面。请参阅 <https://console.aws.amazon.com/ipam/>。
- AWS Command Line Interface (AWS CLI)：为众多 AWS 服务（包括 Amazon VPC）提供命令。AWS CLI 在 Windows、macOS 和 Linux 上受支持。要获取 AWS CLI，请参阅 [AWS Command Line Interface](#)。
- AWS 开发工具包：提供特定于语言的 API。AWS 开发工具包关注许多连接详细信息，比如计算签名、处理请求重试和处理错误。有关更多信息，请参阅 [AWS 开发工具包](#)。
- 查询 API：提供了您使用 HTTPS 请求调用的低级别 API 操作。使用查询 API 是访问 IPAM 的最直接方式。但它需要您的应用程序处理低级别的详细信息，例如生成哈希值以签署请求以及处理错误。有关更多信息，请参阅 [Amazon EC2 API 参考](#) 中的 Amazon IPAM 操作。

本指南主要侧重于使用 AWS 管理控制台来创建、访问和管理 IPAM。在关于如何在控制台中完成流程的每个描述中，我们都包括了指向《AWS CLI 命令参考》的链接，以便您可以使用 AWS CLI 执行相同的任务。

如果您是第一次使用 IPAM 的用户，请查看 [IPAM 的工作原理](#) 了解 IPAM 在 Amazon VPC 中的角色，然后继续执行 [为 IPAM 配置集成选项](#) 中的说明。

为 IPAM 配置集成选项

本部分介绍如何将 IPAM 与 Organizations AWS、其他 AWS 账户集成，或者将其用于单个 AWS 账户的选项。

在开始使用 IPAM 之前，您必须选择本部分中的一个选项，才能使 IPAM 能够监控与 EC2 网络资源关联的 CIDR 并存储指标：

- 要使 IPAM 与 AWS Organizations 集成，从而使 Amazon VPC IPAM 服务管理和监控所有 AWS Organizations 成员账户创建的联网资源，请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)。
- 与 AWS Organizations 集成后，要将 IPAM 与组织外部的账户集成，请参阅 [将 IPAM 与组织外部的账户集成](#)。
- 要将单个 AWS 账户用于 IPAM，并使 Amazon VPC IPAM 服务能够管理和监控您使用单个账户创建的联网资源，请参阅 [将 IPAM 用于单个账户](#)。

如果您没有选择其中一个选项，您仍可以创建 IPAM 资源，例如池，但是在控制面板中看不到指标，也无法监控资源的状态。

内容

- [将 IPAM 与 AWS Organization 中的账户集成](#)
- [将 IPAM 与组织外部的账户集成](#)
- [将 IPAM 用于单个账户](#)

将 IPAM 与 AWS Organization 中的账户集成

或者，您可以按照本部分中的步骤将 IPAM 与 AWS Organizations 集成并委托成员账户作为 IPAM 账户。

IPAM 账户负责创建 IPAM 并使用它来管理和监控 IP 地址的使用情况。

将 IPAM 与 AWS Organizations 集成和委托 IPAM 管理员具有以下益处：

- 与您的企业共享 IPAM 池：当您委派一个 IPAM 账户时，IPAM 会启用企业中的其他 AWS Organizations 成员账户，用于从使用 AWS Resource Access Manager (RAM) 共享的 IPAM 池

中分配 CIDR。有关设置企业的更多信息，请参阅 AWS Organizations 用户指南中的[什么是 AWS Organizations ?](#)。

- 监控企业中的 IP 地址使用情况：当您委派 IPAM 账户时，您将授予 IPAM 权限，以监控所有账户的 IP 使用情况。因此，IPAM 会将现有 VPC 在其他 AWS Organizations 成员账户之间使用的 CIDR 自动导入 IPAM 中。

如果您不委派 AWS Organizations 成员账户作为 IPAM 账户，IPAM 将只监控您用于创建 IPAM 的 AWS 账户中的资源。

Note

将与 AWS Organizations 集成时：

- 必须通过在 AWS 管理控制台中使用 IPAM 或 [enable-ipam-organization-admin-account](#) AWS CLI 命令来启用与 AWS Organizations 的集成。这将确保创建与 AWSServiceRoleForIPAM 服务相关角色。如果通过使用 AWS Organizations 控制台或 [register-delegated-administrator](#) AWS CLI 命令启用对 AWS Organizations 的受信任访问，则不会创建与 AWSServiceRoleForIPAM 服务相关的角色，也无法管理或监控企业内的资源。
- IPAM 账户必须是 AWS Organizations 成员账户。您不能将 AWS Organizations 管理账户作为 IPAM 账户。要检查您的 IPAM 是否已与 AWS Organizations 集成，请使用以下步骤并在组织设置中查看集成的详细信息。
- IPAM 针对在企业成员账户中监控的每个活动 IP 地址向您收取费用。有关定价的更多信息，请参阅 [IPAM 定价](#)。
- 您必须在 AWS Organizations 中拥有账户，以及设置有一个或多个成员账户的管理账户。有关账户类型的更多信息，请参阅 AWS Organizations 用户指南中的[术语和概念](#)。有关设置企业的更多信息，请参阅[开始使用 AWS Organizations](#)。
- IPAM 账户必须使用附加了允许 iam:CreateServiceLinkedRole 操作的 IAM policy 的 IAM 角色。创建 IPAM 时，将自动创建 AWSServiceRoleForIPAM 服务相关角色。
- 与 AWS Organizations 管理账户关联的 IAM 用户必须使用附加了以下 IAM policy 操作的 IAM 角色：
 - ec2:EnableIpamOrganizationAdminAccount
 - organizations:EnableAwsServiceAccess
 - organizations:RegisterDelegatedAdministrator
 - iam:CreateServiceLinkedRole

有关创建 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 [创建向 IAM 用户委托权限的角色](#)。

- 与 AWS Organizations 管理账户关联的用户可使用附加了以下 IAM 策略操作的 IAM 角色，以列出您当前的 AWS Organizations 委派管理员：`organizations:ListDelegatedAdministrators`

AWS Management Console

要选择 IPAM 账户

1. 使用 AWS Organizations 管理账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在 AWS 管理控制台中，选择您要在其中与 IPAM 合作的 AWS 区域。
3. 在导航面板中选择组织设置。
4. 仅当您以 AWS Organizations 管理账户身份登录控制台时，委派选项才可用。选择 Delegate（委派）。
5. 对于 IPAM 账户，输入 AWS 账户 ID。IPAM 管理员必须是 AWS Organizations 成员账户。
6. 选择保存更改。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

- 要使用 AWS CLI 委托 IPAM 管理员账户，请使用以下命令：[enable-ipam-organization-admin-account](#)

当您将 Organizations 成员账户委派为 IPAM 账户时，IPAM 会自动在企业中的所有成员账户中创建服务相关的 IAM 角色。IPAM 通过在每个成员账户中担任服务相关的 IAM 角色、发现资源及其 CIDR 并将其与 IPAM 集成来监控这些账户中的 IP 地址使用情况。无论其企业单位如何，IPAM 都可以发现所有成员账户中的资源。例如，如果有成员账户创建了 VPC，您将在 IPAM 控制台的资源部分中看到 VPC 及其 CIDR。

⚠ Important

委派 IPAM 管理员的 AWS Organizations 管理账户的角色现已完成。要继续使用 IPAM，IPAM 管理员账户必须登录 Amazon VPC IPAM 并创建 IPAM。

将 IPAM 与组织外部的账户集成

本部分介绍如何将 IPAM 与组织外部的 AWS 账户集成。要完成本部分中的步骤，您必须先完成 [将 IPAM 与 AWS Organization 中的账户集成](#) 中的步骤并委派 IPAM 账户。

将 IPAM 与组织外部的 AWS 账户集成后，您能够执行以下操作：

- 通过单个 IPAM 账户管理组织外部的 IP 地址。
- 与其他 AWS Organizations 中其他 AWS 账户托管的第三方服务共享 IPAM 池。

将 IPAM 与组织外部的 AWS 账户集成后，您可以直接与其他组织的所需账户共享 IPAM 池。

目录

- [注意事项和限制](#)
- [过程概述](#)

注意事项和限制

本部分包含将 IPAM 与组织外部的账户集成的注意事项和限制：

- 当您与其他账户共享资源发现时，唯一交换的数据是 IP 地址和账户状态监控数据。您可以在共享之前，使用 [get-ipam-discovered-resource-cidrs](#) 和 [get-ipam-discovered-accounts](#) CLI 命令或 [GetIpamDiscoveredResourceCidrs](#) 和 [GetIpamDiscoveredAccounts](#) API 查看此数据。对于监控整个组织资源的资源发现，不会共享任何组织数据（例如组织中的组织单位名称）。
- 创建资源发现后，资源发现会监控所有者账户中的所有可见资源。如果所有者账户是为自己的多个客户创建资源的第三方服务 AWS 账户，则资源发现能够发现这些资源。如果第三方 AWS 服务账户与最终用户 AWS 账户共享资源发现，则最终用户能够查看第三方 AWS 服务的其他客户资源。因此，第三方 AWS 服务应谨慎创建和共享资源发现，或针对每个客户使用不同的 AWS 账户。

过程概述

本部分介绍如何将 IPAM 与组织外部的 AWS 账户集成。其中涉及本指南其他部分所涵盖的主题。保持此页面可见，并在新窗口中打开以下链接主题，以便您可以返回此页面获取指导。

将 IPAM 与组织外部的 AWS 账户集成时，此过程涉及 4 个 AWS 账户：

- 主组织所有者 – 组织 1 的 AWS Organizations 管理账户。
- 主组织 IPAM 账户 – 组织 1 的 IPAM 委托管理员账户。
- 辅助组织所有者 – 组织 2 的 AWS Organizations 管理账户。
- 辅助组织管理员账户 – 组织 2 的 IPAM 委托管理员账户。

步数

1. 主组织所有者将其组织的一名成员委托为主组织 IPAM 账户 (请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)) 。
2. 主组织 IPAM 账户创建 IPAM (请参阅 [创建 IPAM](#)) 。
3. 辅助组织所有者将其组织的一名成员委托为辅助组织管理员账户 (请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)) 。
4. 辅助组织管理员账户创建资源发现并使用 AWS RAM 将其与主组织 IPAM 账户共享 (请参阅 [创建资源发现以与其他 IPAM 集成](#) 和 [与其他 AWS 账户共享资源发现](#)) 。资源发现必须在主组织 IPAM 所在的同一主区域中创建。
5. 主组织 IPAM 账户使用 AWS RAM 接受资源共享邀请 (请参阅《AWS RAM 用户指南》中的 [接受和拒绝资源共享邀请](#)) 。
6. 主组织 IPAM 账户将资源发现与其 IPAM 相关联 (请参阅 [将资源发现与 IPAM 关联](#)) 。
7. 主组织 IPAM 账户现在可以监控和/或管理由辅助组织中的账户创建的 IPAM 资源。
8. (可选) 主组织 IPAM 账户与辅助组织中的成员账户共享 IPAM 池 (请参阅 [使用 AWS RAM 共享 IPAM 池](#)) 。
9. (可选) 如果主组织 IPAM 账户希望在辅助组织中停止资源发现，可将资源发现与 IPAM 取消关联 (请参阅 [取消关联资源发现](#)) 。
10. (可选) 如果辅助组织管理员账户希望停止参与主组织的 IPAM，可以取消共享已共享的资源发现 (请参阅《AWS RAM 用户指南》中的 [更新 AWS RAM 中的资源共享](#)) 或删除资源发现 (请参阅 [删除资源发现](#)) 。

将 IPAM 用于单个账户

如果选择不[将 IPAM 与 AWS Organization 中的账户集成](#)，则可以将 IPAM 与单个 AWS 账户一起使用。

当您在下一部分创建 IPAM 时，将自动在 AWS Identity and Access Management (IAM) 中为 Amazon VPC IPAM 服务创建服务相关角色。

服务相关角色是一种 IAM 角色，允许 AWS 服务代表您访问其他 AWS 服务。它们通过自动创建和管理特定 AWS 服务执行所需操作需要的权限简化了权限管理过程，从而简化了这些服务的设置和管理。

IPAM 使用服务相关角色来监控和存储与 EC2 联网资源关联的 CIDR 的指标。有关服务相关角色及 IPAM 如何使用它的更多信息，请参阅[IPAM 的服务相关角色](#)。

Important

如果您将 IPAM 与单个 AWS 账户一起使用，则必须确保用于创建 IPAM 的 AWS 账户使用附加了允许 `iam:CreateServiceLinkedRole` 操作的 IAM policy 的 IAM 角色。创建 IPAM 时，将自动创建 `AWSServiceRoleForIPAM` 服务相关角色。有关管理 IAM 策略的更多信息，请参阅 IAM 用户指南中的[编辑 IAM 策略](#)。

一旦单个 AWS 账户有权创建 IPAM 服务相关角色，请转到[创建 IPAM](#)。

创建 IPAM

按照本部分中的步骤创建 IPAM。如果您已委派了 IPAM 管理员，则 IPAM 账户应完成这些步骤。

Important

创建 IPAM 时，系统将要求您允许 IPAM 将数据从源账户复制到 IPAM 委托账户中。要将 IPAM 与 AWS Organizations 集成，IPAM 需要您的权限才能跨账户（从成员账户到委派的 IPAM 成员账户）和跨 AWS 区域（从运营区域到 IPAM 的主区域）复制源和 IP 使用详细信息。对于单一账户 IPAM 用户，IPAM 需要您的权限才能跨运营区域将资源和 IP 使用详细信息复制到 IPAM 的主区域。

创建 IPAM 时，您可以选择允许 IPAM 管理 IP 地址 CIDR 的 AWS 区域。这些 AWS 区域被称为运营区域。IPAM 仅发现和监控您选择作为运营区域的 AWS 区域中的资源。IPAM 不会在您选择的运营区域之外存储任何数据。

下面的层次结构示例演示了您在创建 IPAM 时分配的 AWS 区域将如何影响将可用于以后创建的池的区域。

- 在 AWS 区域 1 和 AWS 区域 2 中运营的 IPAM
 - 私有范围
 - 顶级 IPAM 池
 - AWS 区域 2 中的区域 IPAM 池
 - 开发池
 - AWS 区域 2 中 VPC 的分配

您只能创建一个 IPAM。有关增加与 IPAM 相关的配额的更多信息，请参阅 [IPAM 的配额](#)。

AWS Management Console

创建 IPAM

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在 AWS 管理控制台中，选择您要在其中创建 IPAM 的 AWS 区域。在主操作区域创建 IPAM。
3. 在服务主页上，选择创建 IPAM。
4. 选择 Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (允许 Amazon VPC IP 地址管理器将数据从源账户复制到 IPAM 委托账户中)。如果未选中此选项，则无法创建 IPAM。
5. 选择 IPAM 等级。有关每种套餐中提供的功能以及与套餐相关的费用的更多信息，请参阅 [Amazon VPC 定价页面](#) 中的 IPAM 选项卡。
6. 在运营区域下，选择此 IPAM 可以在其中管理和发现资源的 AWS 区域。默认情况下，您要在其中创建 IPAM 的 AWS 区域被选为运营区域之一。例如，如果您在 AWS 区域 us-east-1 中创建此 IPAM，但是您希望稍后创建区域 IPAM 池，以便在 us-west-2 中向 VPC 提供 CIDR，请在此选择 us-west-2。如果忘记了运营区域，可以稍后返回并编辑 IPAM 设置。

Note

如果您在免费等级中创建 IPAM，则可以为 IPAM 选择多个运营区域，但唯一可在运营区域中使用的 IPAM 功能是[公共 IP 洞察功能](#)。您无法跨 IPAM 运营区域中使用免费等级中的其他功能，例如 BYOIP。你只能在 IPAM 的主区域中只能使用这些功能。要跨运营区域使用所有 IPAM 功能，[请在高级等级中创建 IPAM](#)。

7. 选择是否要启用私有 IPv6 GUA CIDR。有关此选项的更多信息，请参阅[启用预置私有 IPv6 GUA CIDR](#)。
8. 选择是否要启用计量模式。有关此选项的更多信息，请参阅[启用成本分配](#)。
9. 选择创建 IPAM。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令创建、修改和查看与 IPAM 相关的详细信息：

1. 创建 IPAM：[create-ipam](#)
2. 查看您创建的 IPAM：[describe-ipams](#)
3. 查看自动创建的范围：[describe-ipam-scopes](#)
4. 修改现有的 IPAM：[modify-ipam](#)

完成这些步骤后，IPAM 已执行以下操作：

- 创建了您的 IPAM。您可以通过在控制台左侧导航窗格中选择 IPAM 来查看 IPAM 和当前选定的运营区域。
- 创建了一个私有和一个公有范围。您可以通过在导航窗格中选择范围来查看范围。有关范围的更多信息，请参阅[IPAM 的工作原理](#)。

计划 IP 地址预置

按照本部分中的步骤，使用 IPAM 池计划 IP 地址预置。如果您已经配置了 IPAM 账户，则这些步骤应该由该账户完成。公有范围和私有范围中池的创建过程不同。本节包括在私有范围中创建区域池的步骤。有关 BYOIP 和 BYOASN 教程，请参阅 [教程](#)。

Important

要跨 AWS 账户使用 IPAM 池，您必须将 IPAM 与 AWS Organizations 集成，否则某些功能可能无法正常工作。有关更多信息，请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)。

在 IPAM 中，池是连续 IP 地址范围（或 CIDR）的集合。池使您能够根据路由和安全需求组织 IP 地址。您可以为您的 IPAM 区域以外的 AWS 区域创建池。例如，如果您对开发和生产应用程序有不同的路由和安全需求，则可以为每个应用程序创建一个池。

在本部分的第一步中，您将创建顶级池。然后，您将在顶级池中创建一个区域池。在区域池中，您可以根据需要创建其他池，例如生产和开发环境池。默认情况下，您最多可以创建深度为 10 的池。有关 IPAM 配额的信息，请参阅 [IPAM 的配额](#)。

Note

术语 provision（预置）和 allocate（分配）在本用户指南和 IPAM 控制台中使用。Provision（预置）在您将 CIDR 添加到 IPAM 池时使用。Allocate（分配）在您将 IPAM 池中的 CIDR 与资源关联时使用。

以下示例显示了池结构的层次结构，您可以通过完成本部分中的步骤来创建这些结构：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 私有范围
 - 顶级池
 - AWS 区域 1 中的区域池
 - 开发池
 - VPC 的分配

此结构可以作为您可能希望如何使用 IPAM 的示例，但是您可以使用 IPAM 来满足企业的需求。有关最佳实践的更多信息，请参阅 [Amazon VPC IP Address Manager Best Practices](#)。

如果您正在创建单个 IPAM 池，请完成 [创建顶级 IPv4 池](#) 中的步骤，然后跳至 [从 IPAM 池中分配 CIDR](#)。

内容

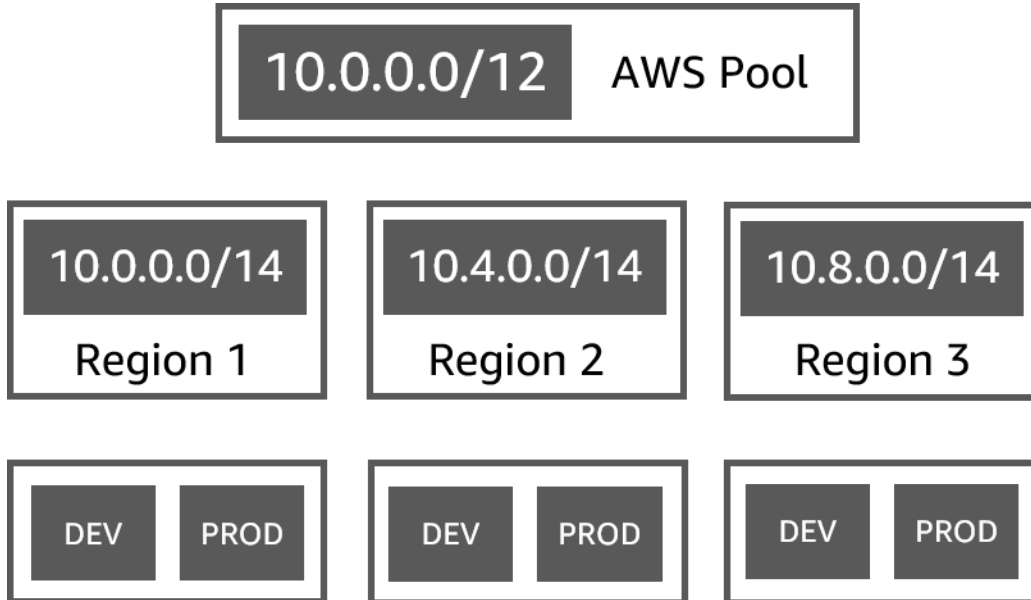
- [示例 IPAM 池计划](#)
- [创建 IPv4 池](#)
- [在 IPAM 中创建 IPv6 地址池](#)

示例 IPAM 池计划

您可以使用 IPAM 满足企业的需求。本部分提供有关如何组织 IP 地址的示例。

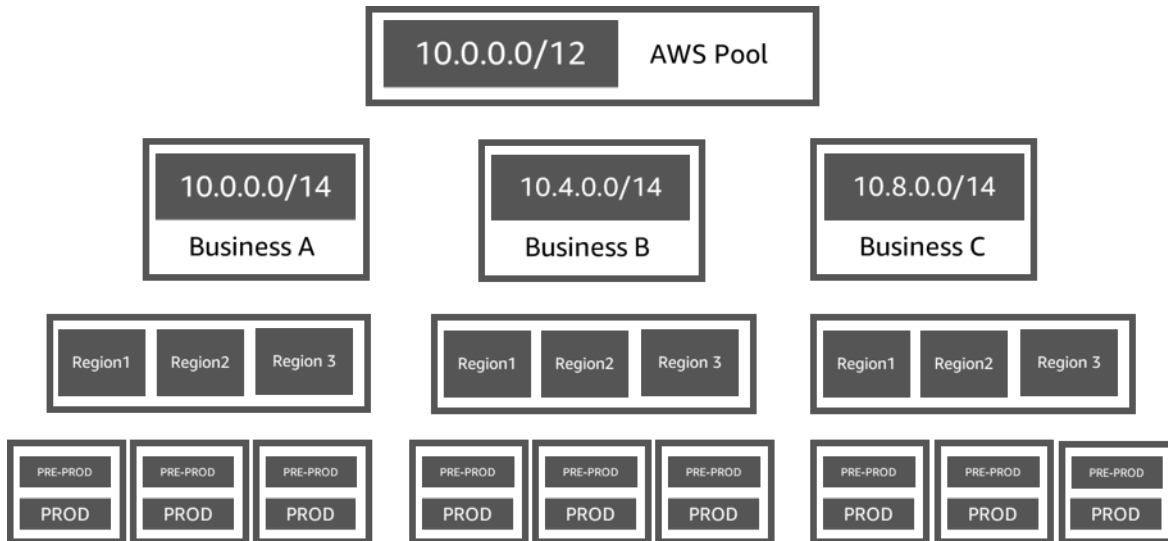
多个 AWS 区域中的 IPv4 池

以下示例显示了顶级池内多个 AWS 区域的 IPAM 池层次结构。每个 AWS 区域池中有两个 IPAM 开发池，一个池用于开发资源，一个池用于生产资源。



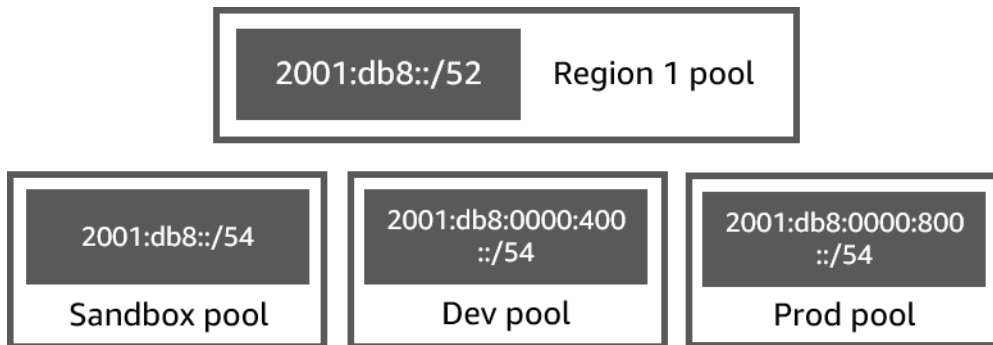
适用于多个业务线的 IPv4 池

以下示例显示了顶级池内多个业务线的 IPAM 池层次结构。每条业务线的每个池包含三个 AWS 区域池。每个区域池中有两个 IPAM 开发池，一个池用于预生产资源，一个池用于生产资源。



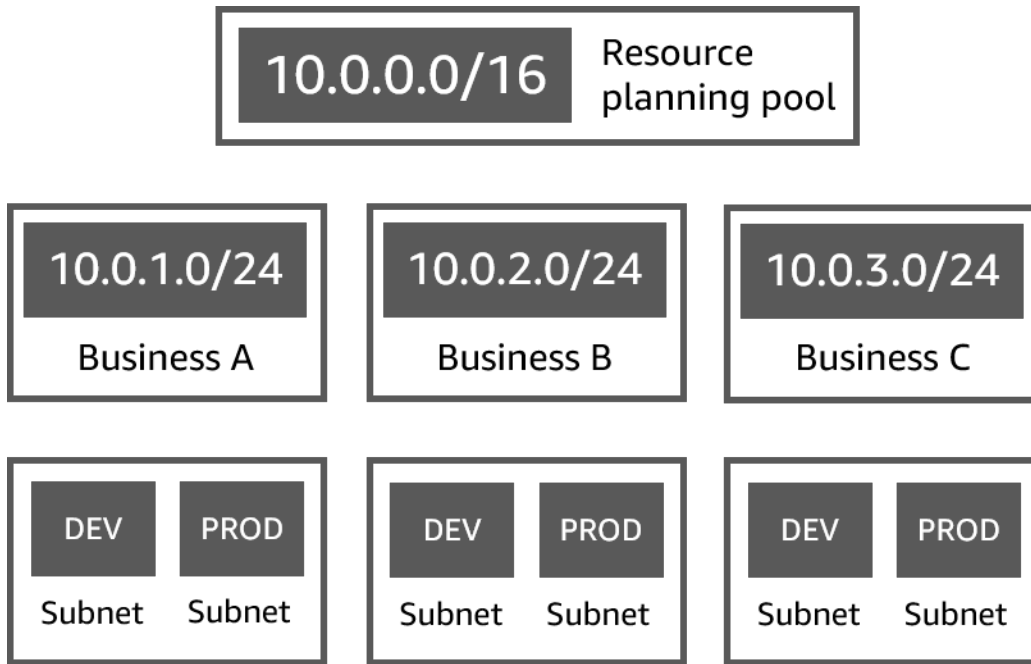
一个 AWS 区域中的 IPv6 池

以下示例显示了区域池内多个业务线的 IPAM IPv6 池层次结构。每个区域池中有三个 IPAM 池，分别用于沙盒资源、开发资源以及生产资源。



适用于多个业务线的子网池

以下示例显示了多个业务线和 dev/prod 子网池的资源规划池的层次结构。有关使用 IPAM 规划子网 IP 地址空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。



创建 IPv4 池

按照本部分中的步骤创建 IPv4 IPAM 池层次结构。

以下示例显示了池结构的层次结构，您可以使用本指南中的说明创建这些结构。在本部分中，您将创建 IPv4 IPAM 池层次结构：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 私有范围
 - 顶级池 (10.0.0.0/8)
 - AWS 区域 2 中的区域池 (10.0.0.0/16)
 - 开发池 (10.0.0.0/24)
 - VPC 的分配 (10.0.0.0/25)

在前述示例中，所使用的 CIDR 仅为示例。它们说明，顶级池中的每个资源池都预置了顶级 CIDR 的一部分。

内容

- [创建顶级 IPv4 池](#)
- [创建区域 IPv4 池](#)
- [创建开发 IPv4 池](#)

创建顶级 IPv4 池

按照本部分中的步骤创建 IPv4 顶级 IPAM 池。创建池时，您需要为池预置 CIDR 以供使用。然后，将该空间分配给分配。分配是从一个 IPAM 池到另一个 IPAM 池或资源的 CIDR 分配。

以下示例显示了池结构的层次结构，您可以使用本指南中的说明创建这些结构。在此步骤中，您正在创建顶级 IPAM 池：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 私有范围
 - 顶级池 (10.0.0.0/8)
 - AWS 区域 1 中的区域池 (10.0.0.0/16)
 - 非生产 VPC 的开发池 (10.0.0.0/24)
 - VPC 的分配 (10.0.0.0/25)

在前述示例中，所使用的 CIDR 仅为示例。它们说明，顶级池中的每个资源池都预置了顶级 CIDR 的一部分。

创建 IPAM 池时，您可以为在 IPAM 池中进行的分配配置规则。

分配规则使您能够配置以下内容：

- 如果 IPAM 在此池的 CIDR 范围内发现 CIDR，是否应该自动将 CIDR 导入 IPAM 池
- 池内分配所需的网络掩码长度
- 池中资源的所需标签
- 池中资源的所需区域设置。区域设置是 IPAM 池可用于分配的 AWS 区域。

分配规则决定了资源是合规还是不合规。有关合规性的其他信息，请参阅 [按资源监控 CIDR 使用情况](#)。

Important

分配规则中没有显示另外一条隐式规则。如果资源位于 IPAM 池中（该池是 AWS Resource Access Manager (RAM) 中的共享资源），必须将资源所有者配置为 AWS RAM 中的主体。有关使用 RAM 共享池的更多信息，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。

以下示例说明了如何使用分配规则控制对 IPAM 池的访问：

Example

当您根据路由和安全需求创建池时，您可能希望只允许某些资源使用池。在这种情况下，您可以设置一个分配规则，说明任何想要此池中的 CIDR 的资源都必须具有与分配规则标签要求匹配的标签。例如，您可通过设置分配规则，说明只有带标签 prod 的 VPC 才可以从 IPAM 池中获取 CIDR。您还可以设置一条规则，指出从此池中分配的 CIDR 不得超过 /24。在这种情况下，从此池使用大于 /24 的 CIDR 创建资源违反了池上的分配规则，导致创建失败。CIDR 大于 /24 的现有资源被标记为不合规。

Important

本主题介绍了如何使用 AWS 提供的 IP 地址范围创建顶级 IPv4 池。如果要导入自带 IPv4 地址范围到 AWS (BYOIP)，需要满足一些先决条件。有关更多信息，请参阅 [教程：将 IP 地址导入 IPAM](#)。

AWS Management Console

如需创建池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择池。
3. 选择创建池。
4. 在 IPAM 范围下，选择要使用的私有范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。

默认情况下，创建池时，默认的私有范围被选中。私有作用域中的池必须为 IPv4 池。公有作用域中的池可以是 IPv4 池，也可以是 IPv6 池。公开范围适用于所有公有空间。


5. (可选) 添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 范围。
7. 在地址系列下，选择 IPv4。
8. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
9. 对于区域设置，选择无。您将在区域池中设置区域设置。

区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。例如，您只能从与 VPC 的区域共享区域设置的 IPAM 池中为 VPC 分配 CIDR。请注意，当您为池选择了区域设置后，无法对其进行

修改。如果 IPAM 的主区域由于中断而不可用，并且池的区域设置与 IPAM 的主区域不同，则该池仍可用于分配 IP 地址。

10. (可选) 您可以在没有 CIDR 的情况下创建池，但是在为该池预置 CIDR 之前，无法使用该池进行分配。要预置 CIDR，请选择添加新 CIDR。输入要为池预置的 IPv4 CIDR。如果要将从自带 IPv4 或 IPv6 IP 地址范围导入 AWS，需要满足一些先决条件。有关更多信息，请参阅 [教程：将 IP 地址带入 IPAM](#)。
11. 为此池选择可选的分配规则：

- 自动导入发现的资源：如果 Locale (区域设置) 被设置为 None (无)，则此选项不可用。如果选中此选项，IPAM 将持续查找此池的 CIDR 范围内的资源，并将其作为分配自动导入到 IPAM 中。请注意以下几点：
 - 为了成功导入，不得将分配给这些资源的 CIDR 分配给其他资源。
 - 无论 IPAM 是否符合池的分配规则，都将导入 CIDR，因此可能会导入资源且随后会将资源标记为不合规。
 - 如果 IPAM 发现多个重叠的 CIDR，IPAM 将仅导入最大的 CIDR。
 - 如果 IPAM 发现多个具有匹配 CIDR 的 CIDR，IPAM 将只随机导入其中一个。

 Warning

- 创建 IPAM 后，请在创建 VPC 时选择 IPAM 分配的 CIDR 块选项。否则，您为 VPC 选择的 CIDR 可能会与 IPAM CIDR 分配重叠。
 - 如果您已在 IPAM 池中分配了 VPC，则无法自动导入具有重叠 CIDR 的 VPC。例如，假设您在 IPAM 池中分配了具有 10.0.0.0/26 CIDR 的 VPC，则无法导入具有 10.0.0.0/23 CIDR (将涵盖 10.0.0.0/26 CIDR) 的 VPC。
 - 将现有的 VPC CIDR 分配自动导入 IPAM 需要一些时间才能完成。
- 最短网络掩码长度：此 IPAM 池中的 CIDR 分配所需的符合要求的最小网络掩码长度以及可以从池中分配的最大大小的 CIDR 块。最短网络掩码长度必须小于最大网络掩码长度。IPv4 地址的可能网络掩码长度为 0 - 32。IPv6 地址的可能网络掩码长度为 0 - 128。
 - 默认网络掩码长度：添加到此池的分配的默认网络掩码长度。例如，如果为此池预置的 CIDR 是 **10.0.0.0/8** 并且您在此处输入 **16**，则此池中任何新分配的网络掩码长度都将默认为 /16。
 - 最大网络掩码长度：此池中的 CIDR 分配所需的最大网络掩码长度。此值表示可以从池中分配的最小大小的 CIDR 块。

- 标记要求：资源分配池中的空间所需的标签。如果资源在分配空间后更改了标签，或者如果池中的分配标记规则发生了更改，则该资源可能会被标记为不合规。
- 区域设置：使用此池中的 CIDR 的资源所需的区域设置。自动导入的没有此区域设置的资源将被标记为不合规。不会自动导入到池中的资源将不允许从池中分配空间，除非它们位于此区域设置。

Note

分配规则仅适用于该资源池中的[托管资源](#)。这些规则不适用于池内池中的资源。

12. (可选) 为池选择 Tags (标签)。
13. 选择创建池。
14. 请参阅[创建区域 IPv4 池](#)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令在您的 IPAM 中创建或编辑顶级池：

1. 创建池：[create-ipam-pool](#)。
2. 创建池后对其进行编辑以修改分配规则：[modify-ipam-pool](#)。

创建区域 IPv4 池

按照本部分中的步骤在顶级池中创建区域池。如果您只需要顶级池，不需要其他区域和开发池，请跳至[从 IPAM 池中分配 CIDR](#)。

Note

公有范围和私有范围中池的创建过程不同。本节包括在私有范围中创建区域池的步骤。有关 BYOIP 和 BYOASN 教程，请参阅[教程](#)。

以下示例显示了池结构的层次结构，您可以按照本指南中的说明创建这些结构。在此步骤中，您正在创建区域 IPAM 池：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 私有范围
 - 顶级池 (10.0.0.0/8)
 - AWS 区域 1 中的区域池 (10.0.0.0/16)
 - 非生产 VPC 的开发池 (10.0.0.0/24)
 - VPC 的分配 (10.0.0.0/25)

在前述示例中，所使用的 CIDR 仅为示例。它们说明，顶级池中的每个资源池都预置了顶级 CIDR 的一部分。

AWS Management Console

要在顶级池中创建区域池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择池。
3. 选择创建池。
4. 在 IPAM 范围下，选择您在创建顶层池时使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
5. （可选）添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 池。然后选择您在上一部分中创建的顶级池。
7. 如果您在公共范围内创建此池，则会看到一个地址系列选项。选择 IPv4。
8. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
9. 选择池的区域设置。选择区域设置可确保池与从中分配的资源之间没有跨区域依赖关系。可用的选项来自您在创建 IPAM 时选择的运营区域。

区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。例如，您只能从与 VPC 的区域共享区域设置的 IPAM 池中为 VPC 分配 CIDR。请注意，当您为池选择了区域设置后，无法对其进行修改。如果 IPAM 的主区域由于中断而不可用，并且池的区域设置与 IPAM 的主区域不同，则该池仍可用于分配 IP 地址。

Note

如果您在免费套餐中创建池，则只能选择与 IPAM 的主区域相匹配的区域设置。要跨区域使用所有 IPAM 功能，请[升级到高级等级](#)。

10. 如果您在公共范围内创建此池，则会看到一个服务选项。选择 EC2 (EIP/VPC)。您选择的服务将决定可传播 CIDR 的 AWS 服务。目前，唯一的选择是 EC2 (EIP/VPC)，这意味着从此池中分配的 CIDR 在 Amazon EC2 服务 (适用于弹性 IP 地址) 和 Amazon VPC 服务 (适用于与 VPC 关联的 CIDR) 中是可传播的。
11. (可选) 选择要为池预置的 CIDR。您可以在没有 CIDR 的情况下创建池，但是在为该池预置 CIDR 之前，您将无法使用该池进行分配。您可以通过编辑池随时将 CIDR 添加到池中。
12. 这里的分配规则选项与创建顶级池时的选项相同。请参阅 [创建顶级 IPv4 池](#) 以了解创建池时可用的选项。区域池的分配规则不是从顶级池继承来的。如果您不在此应用任何规则，则不会为池设置分配规则。
13. (可选) 为池选择 Tags (标签)。
14. 配置完池后，选择创建池。
15. 请参阅[创建开发 IPv4 池](#)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令在您的 IPAM 中创建区域池：

1. 获取要在其中创建池的范围的 ID：[describe-ipam-scopes](#)
2. 获取要在其中创建池的池的 ID：[describe-ipam-pools](#)
3. 创建池：[create-ipam-pool](#)
4. 查看新池：[describe-ipam-pools](#)

根据需要，重复这些步骤以在顶级池中创建额外的池。

创建开发 IPv4 池

按照本部分中的步骤在区域池中创建开发池。如果您只需要顶层和区域池，不需要开发池，请跳至 [从 IPAM 池中分配 CIDR](#)。

以下示例显示了池结构的层次结构，您可以使用本指南中的说明创建这些结构。在此步骤中，您正在创建一个开发 IPAM 池：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 私有范围
 - 顶级池 (10.0.0.0/8)
 - AWS 区域 1 中的区域池 (10.0.0.0/16)
 - 非生产 VPC 的开发池 (10.0.0.0/24)
 - VPC 的分配 (10.0.1.0/25)

在前述示例中，所使用的 CIDR 仅为示例。它们说明，顶级池中的每个资源池都预置了顶级 CIDR 的一部分。

AWS Management Console

在区域池中创建开发池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择池。
3. 选择创建池。
4. 在 IPAM 范围下，选择您在创建顶层池和区域池时使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
5. (可选) 添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 池。然后选择区域池。
7. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
8. (可选) 选择要为池预置的 CIDR。您只能预置已经预置到顶级池中的 CIDR。您可以在没有 CIDR 的情况下创建池，但是在为该池预置 CIDR 之前，您将无法使用该池进行分配。您可以通过编辑池随时将 CIDR 添加到池中。
9. 这里的分配规则选项与创建顶层和区域池时的选项相同。请参阅 [创建顶级 IPv4 池](#) 以了解创建池时可用的选项。池的分配规则不是从层次结构中其上方的池中继承来的。如果您不在此应用任何规则，则不会为池设置分配规则。
10. (可选) 为池选择标签。
11. 配置完池后，选择创建池。

12. 请参阅[从 IPAM 池中分配 CIDR](#)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令在您的 IPAM 中创建区域池：

1. 获取要在其中创建池的范围的 ID：[describe-ipam-scopes](#)
2. 获取要在其中创建池的池的 ID：[describe-ipam-pools](#)
3. 创建池：[create-ipam-pool](#)
4. 查看新池：[describe-ipam-pools](#)

根据需要，重复这些步骤以在区域池中创建额外的开发池。

在 IPAM 中创建 IPv6 地址池

AWS 在其许多服务（包括 EC2、VPC 和 S3）之间提供 IPv6 连接，使您能够使用 IPv6 增加的地址空间和增强的安全功能。IPv6 设计用于解决 IPv4 的这一基本限制。通过转移到 128 位地址空间，IPv6 提供了大量唯一的 IP 地址。这种大规模的地址扩展使互联技术的连续扩散成为可能，从智能手机和物联网设备到云基础设施不一而足。

此外，您可以使用 IPAM 来确保使用连续的 IPv6 CIDR 创建 VPC。连续分配的 CIDR 是按顺序分配的 CIDR。它们使您能够简化安全和网络规则；IPv6 CIDR 可以跨网络和安全结构（如访问控制列表、路由表、安全组和防火墙）聚合在单个条目中。

按照本部分中的步骤创建 IPAM IPv6 池层次结构。创建池时，您可以为池预置 CIDR 以供使用。池将该 CIDR 中的空间分配给池内的分配。分配是从一个 IPAM 池到另一个资源或 IPAM 池的 CIDR 分配。

Note

AWS 同时提供公有和私有 IPv6 寻址。AWS 认为公有 IP 地址是从 AWS 公开发布在互联网上的，而私有 IP 地址不是，也不能从 AWS 公开发布在互联网上。如果希望自己的私有网络支持 IPv6，并且不打算将流量从这些地址路由到互联网，则可在私有范围内创建 IPv6 池。有关公有和私有 IPv6 地址的更多信息，请参阅《Amazon VPC 用户指南》中的[IPv6 地址](#)。

以下示例显示了池结构的层次结构，您可以使用本指南中的说明创建这些结构。在本部分中，您将创建 IPv6 IPAM 池层次结构：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 范围
 - AWS 区域 1 中的区域池 (2001:db8::/52)
 - 开发池 (2001:db8::/54)
 - VPC 的分配 (2001:db8::/56)

在前述示例中，所使用的 CIDR 仅为示例。它们说明，区域池中的开发池预置了区域池 CIDR 的一部分。

内容

- [在 IPAM 中创建区域 IPv6 池](#)
- [在 IPAM 中创建开发 IPv6 池](#)

在 IPAM 中创建区域 IPv6 池

按照本部分中的步骤创建 IPv6 区域 IPAM 池。当您向池预置 Amazon 提供的 IPv6 CIDR 块时，必须将其预置到已选择区域设置 (AWS 区域) 的池中。创建池时，您可以为池预置 CIDR 以供稍后使用或添加。然后，将该空间分配给分配。分配是从一个 IPAM 池到另一个 IPAM 池或资源的 CIDR 分配。

以下示例显示了池结构的层次结构，您可以使用本指南中的说明创建这些结构。在此步骤中，您将创建 IPv6 区域 IPAM 池：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 范围
 - AWS 区域 1 中的区域池 (2001:db8::/52)
 - 开发池 (2001:db8::/54)
 - VPC 的分配 (2001:db8::/56)

在前述示例中，所使用的 CIDR 仅为示例。它们说明，IPv6 区域池中的每个池都预置了 IPv6 区域 CIDR 的一部分。

创建 IPAM 池时，您可以为在 IPAM 池中进行的分配配置规则。

分配规则使您能够配置以下内容：

- 池内分配所需的网络掩码长度
- 池中资源的所需标签
- 池中资源的所需区域设置。区域设置是 IPAM 池可用于分配的 AWS 区域。

分配规则决定了资源是合规还是不合规。有关合规性的其他信息，请参阅 [按资源监控 CIDR 使用情况](#)。

Note

分配规则中没有显示另外一条隐式规则。如果资源位于 IPAM 池中（该池是 AWS Resource Access Manager (RAM) 中的共享资源），必须将资源所有者配置为 AWS RAM 中的主体。有关使用 RAM 共享池的更多信息，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。

以下示例说明了如何使用分配规则控制对 IPAM 池的访问：

Example

当您根据路由和安全需求创建池时，您可能希望只允许某些资源使用池。在这种情况下，您可以设置一个分配规则，说明任何想要此池中的 CIDR 的资源都必须具有与分配规则标签要求匹配的标签。例如，您可通过设置分配规则，说明只有带标签 prod 的 VPC 才可以从 IPAM 池中获取 CIDR。

Note

- 本主题旨在介绍如何使用 AWS 提供的 IPv6 地址范围或使用私有 IPv6 范围创建 IPv6 区域池。如果要引入 AWS (BYOIP) 的自有 IPv4 或 IPv6 IP 地址范围，需要满足一些先决条件。有关更多信息，请参阅 [教程：将 IP 地址带入 IPAM](#)。
- 如果要在私有范围内创建 IPv6 池，则可使用私有 IPv6 GUA 或 ULA 范围。要使用私有 GUA 范围，必须先在 IPAM 上启用该选项（请参阅 [启用预置私有 IPv6 GUA CIDR](#)）。

AWS Management Console

如需创建池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。

2. 在导航窗格中，选择池。
3. 选择创建池。
4. 在 IPAM 范围下，选择一个私有或公有范围。如果希望自己的私有网络支持 IPv6，并且不打算将流量从这些地址路由到互联网，则可选择私有范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。

默认情况下，创建池时，默认的私有范围被选中。

5. (可选) 添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 范围。
7. 对于地址系列，选择 IPv6。如果在公有范围内创建此池，则该池中的所有 CIDR 都可以公开发布。
8. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
9. 选择池的区域设置。要向池预置 Amazon 提供的 IPv6 CIDR 块，必须向已选择区域设置 (AWS 区域) 的池预置该 IPv6 CIDR 块。选择区域设置可确保池与从中分配的资源之间没有跨区域依赖关系。可用选项来自创建 IPAM 时为其选择的运营区域。您可以随时添加其他运营区域。

区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。例如，您只能从与 VPC 的区域共享区域设置的 IPAM 池中为 VPC 分配 CIDR。请注意，当您为池选择了区域设置后，无法对其进行修改。如果 IPAM 的主区域由于中断而不可用，并且池的区域设置与 IPAM 的主区域不同，则该池仍可用于分配 IP 地址。

Note

如果您在免费套餐中创建池，则只能选择与 IPAM 的主区域相匹配的区域设置。要跨区域使用所有 IPAM 功能，请[升级到高级等级](#)。

10. (可选) 如果要在公有范围内创建 IPv6 池，请在服务下选择 EC2 (EIP/VPC)。您选择的服务将决定可传播 CIDR 的 AWS 服务。目前，唯一的选择是 EC2 (EIP/VPC)，这意味着从此池中分配的 CIDR 在 Amazon EC2 服务 (适用于弹性 IP 地址) 和 Amazon VPC 服务 (适用于与 VPC 关联的 CIDR) 中是可传播的。
11. (可选) 如果要在公有范围内创建 IPv6 池，请在公有 IP 源选项下选择 Amazon 拥有，让 AWS 为该池提供 IPv6 地址范围。如本页顶部所述，本主题介绍了如何使用 AWS 提供的 IP 地址范围创建 IPv6 区域池。如果要将自带 IPv4 或 IPv6 地址范围导入 AWS (BYOIP)，需要满足一些先决条件。有关更多信息，请参阅 [教程：将 IP 地址带入 IPAM](#)。

12. (可选) 您可以创建不含 CIDR 的池，但是在为其预调配 CIDR 之前，您将无法使用该池进行分配。要预置 CIDR，请执行下列某项操作：
 - 如果要在公有范围内创建具有 Amazon 拥有的公有 IP 源的 IPv6 池来预置 CIDR，则在要预置的 CIDR 下选择添加 Amazon 拥有的 CIDR，然后选择 CIDR 的网络掩码大小 (介于 /40 和 /52 之间)。在下拉菜单中选择网络掩码长度时，您会看到网络掩码长度及网络掩码所代表的 /56 CIDR 数量。默认情况下，您可以向区域池添加一个 Amazon 提供的 IPv6 CIDR 块。有关提高默认限制的信息，请参阅 [IPAM 的配额](#)。
 - 如果要在私有范围内创建 IPv6 池，则可使用私有 IPv6 GUA 或 ULA 范围：
 - 有关私有 IPv6 寻址的重要详细信息，请参阅《Amazon VPC 用户指南》中的 [私有 IPv6 地址](#)。
 - 要使用私有 IPv6 ULA 范围，则在要预置的 CIDR 下选择按网络掩码添加 ULA CIDR 并选择网络掩码大小，或者选择输入私有 IPv6 CIDR 并输入 ULA 范围。有效的 IPv6 ULA 空间是指任何低于 fd00:: /8 且不与 Amazon 预留范围 fd00:: /16 重叠的空间。
 - 要使用私有 IPv6 GUA 范围，必须先在 IPAM 上启用该选项 (请参阅 [启用预置私有 IPv6 GUA CIDR](#))。启用私有 IPv6 GUA CIDR 后，在输入私有 IPv6 CIDR 中输入 IPv6 GUA。
13. 为此池选择可选的分配规则：
 - 最短网络掩码长度：此 IPAM 池中的 CIDR 分配所需的符合要求的最小网络掩码长度以及可以从池中分配的最大大小的 CIDR 块。最短网络掩码长度必须小于最大网络掩码长度。IPv6 地址的可能网络掩码长度为 0 - 128。
 - 默认网络掩码长度：添加到此池的分配的默认网络掩码长度。例如，如果为此池预置的 CIDR 是 2001:db8:: /52 并且您在此处输入 56，则此池中任何新分配的网络掩码长度都将默认为 /56。
 - 最大网络掩码长度：此池中的 CIDR 分配所需的最大网络掩码长度。此值表示可以从池中分配的最小大小的 CIDR 块。例如，如果您在此处输入 /56，则可以为此池中的 CIDR 分配的最小网络掩码长度为 /56。
 - 标记要求：资源分配池中的空间所需的标签。如果资源在分配空间后更改了标签，或者如果池中的分配标记规则发生了更改，则该资源可能会被标记为不合规。
 - 区域设置：使用此池中的 CIDR 的资源所需的区域设置。自动导入的没有此区域设置的资源将被标记为不合规。不会自动导入到池中的资源将不允许从池中分配空间，除非它们位于此区域设置。
14. (可选) 为池选择 Tags (标签)。
15. 选择创建池。

16. 请参阅[在 IPAM 中创建开发 IPv6 池](#)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令在 IPAM 中创建或编辑 IPv6 区域池：

1. 如果要启用预置私有 IPv6 GUA CIDR，请使用 [modify-ipam](#) 修改 IPAM，然后纳入用于 `enable-private-gua` 的选项。有关更多信息，请参阅 [启用预置私有 IPv6 GUA CIDR](#)。
2. 使用 [create-ipam-pool](#) 创建池。
3. 向池预置 CIDR：[provision-ipam-pool-cidr](#)。
4. 创建池后对其进行编辑以修改分配规则：[modify-ipam-pool](#)。

在 IPAM 中创建开发 IPv6 池

按照本部分中的步骤在 IPv6 区域池中创建开发池。如果您只需要区域池，不需要开发池，请跳至 [从 IPAM 池中分配 CIDR](#)。

以下示例显示了池结构的层次结构，您可以使用本指南中的说明创建这些结构。在此步骤中，您正在创建一个开发 IPAM 池：

- IPAM 在 AWS 区域 1 和 AWS 区域 2 中运营
 - 范围
 - AWS 区域 1 中的区域池 (2001:db8::/52)
 - 开发池 (2001:db8::/54)
 - VPC 的分配 (2001:db8::/56)

在前述示例中，所使用的 CIDR 仅为示例。它们说明，顶级池中的每个资源池都预置了顶级 CIDR 的一部分。

AWS Management Console

在 IPv6 区域池中创建开发池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。

2. 在导航窗格中，选择池。
3. 选择创建池。
4. 在 IPAM 范围下，选择一个范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
5. (可选) 添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 池。然后在源池下，选择 IPv6 区域池。
7. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
8. (可选) 选择要为池预置的 CIDR。您只能预置已经预置到顶级池中的 CIDR。您可以在没有 CIDR 的情况下创建池，但是在为该池预置 CIDR 之前，您将无法使用该池进行分配。您可以通过编辑池随时将 CIDR 添加到池中。
9. 此处的分配规则选项与创建 IPv6 区域池时的选项相同。请参阅 [在 IPAM 中创建区域 IPv6 池](#) 以了解创建池时可用的选项。池的分配规则不是从层次结构中其上方的池中继承来的。如果您不在此应用任何规则，则不会为池设置分配规则。
10. (可选) 为池选择标签。
11. 配置完池后，选择创建池。
12. 请参阅 [从 IPAM 池中分配 CIDR](#)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令在 IPAM 中创建 IPv6 区域池：

1. 获取要在其中创建池的范围的 ID：[describe-ipam-scopes](#)
2. 获取要在其中创建池的池的 ID：[describe-ipam-pools](#)
3. 创建池：[create-ipam-pool](#)
4. 查看新池：[describe-ipam-pools](#)

根据需要重复这些步骤，以在 IPv6 区域池中创建其他开发池。

从 IPAM 池中分配 CIDR

IPAM 的其中一个重要功能是能够分配和管理 IP 地址空间。创建 VPC 时，必须指定 IP 地址 CIDR 块，该块定义了可用于该 VPC 的 IP 地址范围。IPAM 通过提供整个 IP 地址清单的全局视图简化了这一流程，从而帮助您策略性地在多个 VPC 之间分配和重复使用 IP 前缀。

这种地址空间分配对于确保没有重叠的 IP 范围至关重要，重叠的 IP 范围可能会导致路由冲突和连接问题。IPAM 还允许您预留 IP 地址空间用于将来的 VPC 扩展，从而无需以后进行复杂的重新编号。

按照本部分中的步骤将 IPAM 池中的 CIDR 分配给资源。

Note

术语 provision (预置) 和 allocate (分配) 在本用户指南和 IPAM 控制台中使用。Provision (预置) 在您将 CIDR 添加到 IPAM 池时使用。Allocate (分配) 在您将 IPAM 池中的 CIDR 与资源关联时使用。

您可以通过以下方式从 IPAM 池分配 CIDR：

- 使用与 IPAM 集成的 AWS 服务，例如 Amazon VPC，然后选择将 IPAM 池用于 CIDR 的选项。IPAM 会自动为您创建池中的分配。
- 在 IPAM 池中手动分配 CIDR，以便将其预留以供以后用于与 IPAM 集成的 AWS 服务，例如 Amazon VPC。

本章节将指导您完成两个选项：如何使用与 IPAM 集成的 AWS 服务以预置 IPAM 池 CIDR，以及如何手动预留 IP 地址空间。

内容

- [创建使用 IPAM 池 CIDR 的 VPC](#)
- [手动将 CIDR 分配到池以预留 IP 地址空间](#)

创建使用 IPAM 池 CIDR 的 VPC

借助 Amazon Virtual Private Cloud (Amazon VPC)，您可以在自己定义的逻辑隔离的虚拟网络中启动 AWS 资源。这个虚拟网络与您在数据中心中运行的传统网络极其相似，并会为您提供使用 AWS 的可扩展基础设施的优势。

虚拟私有云 (VPC) 是仅适用于您的 AWS 账户的虚拟网络。它在逻辑上与 AWS 云中的其他虚拟网络隔绝。您可以为 VPC 指定 IP 地址范围、添加子网、添加网关以及关联安全组。

按照《Amazon VPC 用户指南》中的[创建 VPC](#) 中的步骤操作。当您到达为 VPC 选择 CIDR 的步骤时，您可以选择使用 IPAM 池中的 CIDR。

如果选择在创建 VPC 时使用 IPAM 池的选项，AWS 会在 IPAM 池中分配 CIDR。您可以通过在 IPAM 控制台的内容窗格中选择池并查看池的 Resources (资源) 选项卡来查看 IPAM 中的分配。

Note

要了解使用 AWS CLI 的完整说明 (包括创建 VPC) ，请参阅 [Amazon VPC IP 地址管理器教程](#) 部分。

手动将 CIDR 分配到池以预留 IP 地址空间

按照本部分中的步骤将 CIDR 手动分配给池。为了在 IPAM 池中预留 CIDR 以供以后使用，您可以执行此操作。您还可以在 IPAM 池中预留空间以表示本地网络。IPAM 将为您管理该预留，并指出是否有 CIDR 与您的本地 IP 空间重叠。

AWS Management Console

要手动分配 CIDR

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池) 。
3. 默认情况下，默认的私有范围被选中。如果您不想使用默认的私有范围，请从内容窗格顶部的下拉菜单中选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 在内容窗格中，选择池。
5. 选择 Actions (操作) > Create custom allocation (创建自定义分配) 。
6. 选择是否添加要分配的特定 CIDR (例如，对 IPv4 使用 10.0.0.0/24 或对 IPv6 使用 2001:db8::/52) ，或者通过仅选择网络掩码长度来按大小添加 CIDR (例如，对 IPv4 使用 /24 或对 IPv6 使用 /52) 。
7. 选择 Allocate。
8. 您可以通过选择导航窗格中的 Pools (池) 、选择一个池并查看该池的 Allocations (分配) 选项卡以查看 IPAM 中的分配。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令手动将 CIDR 分配给池：

1. 获取要在其中创建分配的 IPAM 池的 ID：[describe-ipam-pools](#)。
2. 创建分配：[allocate-ipam-pool-cidr](#)。
3. 查看分配：[get-ipam-pool-allocations](#)。

要发布手动分配的 CIDR，请参阅 [释放分配](#)。

管理 IPAM 中的 IP 地址空间

此部分中的任务是可选的。请注意，本部分为一组程序，都与使用 IPAM 相关。按字母顺序排列这些过程。

如果您想完成此部分中的任务，并且已委派了 IPAM 账户，则应该由 IPAM 管理员完成这些任务。

按照本部分中的步骤管理 IPAM 中的 IP 地址空间。

内容

- [使用 IPAM 自动更新前缀列表](#)
- [更改 VPC CIDR 的监控状态](#)
- [创建额外范围](#)
- [删除 IPAM](#)
- [删除池](#)
- [删除范围](#)
- [从池中取消预置 CIDR](#)
- [编辑 IPAM 池](#)
- [启用成本分配](#)
- [将 VPC IPAM 与 Infoblox 基础设施集成](#)
- [启用预置私有 IPv6 GUA CIDR](#)
- [强制使用 IPAM 通过 SCP 进行 VPC 创建](#)
- [从 IPAM 中排除组织单位](#)
- [修改 IPAM 等级](#)
- [修改 IPAM 运营区域](#)
- [将 CIDR 预置到池](#)
- [在范围之间移动 VPC CIDR](#)
- [使用 IPAM 策略定义公有 IPv4 分配策略](#)
- [释放分配](#)
- [使用 AWS RAM 共享 IPAM 池](#)

- [使用资源发现](#)

使用 IPAM 自动更新前缀列表

[托管前缀列表](#)是一组 CIDR 块，您可以在安全组规则和路由表中引用这些块，而无需指定单个 IP 地址。例如，可以创建一个包含所有三个 CIDR 的前缀列表，并在单个规则中引用它，而不必为 10.1.0.0/16、10.2.0.0/16 和 10.3.0.0/16 创建单独的安全组规则。

这些变量分为两种类型：

- 客户管理的前缀列表：您定义和管理的 IP 范围
- AWS 管理的前缀列表：AWS 服务的 IP 范围（例如 S3 或 CloudFront）

IPAM 功能通过使您的 CIDR 条目与网络更改保持同步，自动管理客户管理的前缀列表。

它解决的问题

如果没有自动化，网络团队在基础设施发生变化时需要花费大量时间手动更新前缀列表，并在不同环境和区域之间维护一致的前缀列表。

IPAM 通过允许您创建自动填充前缀列表的规则来解决此问题。您可以使用两种方法：引用 IPAM 池中的 CIDR，或者基于实际的 AWS 资源创建规则，例如“包含所有标记为 env=prod 的 VPC”、“包含 us-east-1 中的所有子网”或“包含账户 123456789 拥有的所有弹性 IP 地址”。当您添加或删除这些资源时，IPAM 会自动使用其 CIDR 更新前缀列表。

工作原理

您可以创建规则，告诉 IPAM 要将哪些 IP 地址包含在前缀列表中。例如，“包含所有标记为 env=prod 的 VPC CIDR”。当您添加或删除生产 VPC 时，IPAM 会自动更新前缀列表。

何时使用

- 安全组：创建一条规则“包含所有标记为 env=prod 的 VPC”，这样，当您添加新的生产 VPC 时，它们会自动被允许出现在您的安全组规则中
- 多区域：在多个区域部署相同的 IPAM 规则，无需手动复制 CIDR 条目即可保持前缀列表一致。
- 动态基础设施：创建/删除 VPC 或子网时，它们的 CIDR 会自动添加到前缀列表/从前缀列表中删除，无需手动更新。

先决条件

在开始之前，请确保您满足以下条件：

- 启用了[高级层的 IPAM](#)
- [客户管理的前缀列表](#) (或在设置过程中创建一个)
- IPAM 和 EC2 前缀列表操作的 [IAM 权限](#)

设置步骤

步骤 1：创建 IPAM 前缀列表解析器

通过创建 IPAM 前缀列表解析器来定义要在前缀列表中包含哪些 CIDR。

AWS Management Console

创建 IPAM 前缀列表解析器

1. 打开 [IAM 控制台](#)。
2. 在导航窗格中，选择前缀列表解析器。
3. 选择创建前缀列表解析器。
4. 在步骤 1：配置解析器详细信息中，选择以下项：
 - IPAM：IPAM 实例
 - 地址系列：IPv4 或 IPv6
 - 名称标签 - 可选：描述性名称
 - 描述 - 可选：描述
 - 标签：资源标签
5. 选择下一步。
6. 在步骤 2：配置规则中，选择添加规则。您最多可以添加 99 个规则。

Important

您可以创建一个不含任何 CIDR 选择规则的前缀列表解析器，但它会生成空版本 (不含任何 CIDR)，直到您添加规则为止。

7. 选择以下规则类型之一：

- 静态 CIDR：固定不变的 CIDR 列表（例如，跨区域复制的手动列表）
- IPAM 池 CIDR：来自特定 IPAM 池的 CIDR（例如，来自 IPAM 生产池的所有 CIDR）

如果选择此选项，请选择以下项：

- IPAM 范围：选择 IPAM 范围以搜索资源
- 条件：
 - 属性
 - IPAM 池 ID：选择包含资源的 IPAM 池
 - CIDR（如 10.24.34.0/23）
 - 运算：等于/不等于
 - 值：要匹配条件的值
- 范围资源 CIDR：来自 IPAM 范围内的 VPC、子网、EIP 等 AWS 资源的 CIDR

如果选择此选项，请选择以下项：

- IPAM 范围：选择 IPAM 范围以搜索资源
- 资源类型：选择资源（例如 VPC 或子网）。
- 条件：
 - 属性：
 - 资源 ID：资源的唯一 ID（例如 vpc-1234567890abcdef0）
 - 资源所有者（例如 111122223333）
 - 资源区域（例如 us-east-1）
 - 资源标签（例如：键：name，值：dev-vpc-1）
 - CIDR（如 10.24.34.0/23）
 - 运算：等于/不等于
 - 值：要匹配条件的值

8. 选择下一步。

9. 选择验证并创建。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用下面的 AWS CLI 命令创建 IPAM 前缀列表解析器：

- 使用 [create-ipam-prefix-list-resolver](#) 命令并保存步骤 2 返回的解析器 ID。

步骤 2：创建用于连接到前缀列表的解析器目标

通过创建解析器目标，将解析器链接到现有前缀列表。使用步骤 1 中返回的解析器 ID。

AWS Management Console

创建 IPAM 前缀列表解析器目标

1. 在 IPAM 控制台中，选择前缀列表解析器。
2. 选择在步骤 1 中创建的解析器。
3. 在解析器详细信息页面上，选择目标选项卡。
4. 选择创建目标。
5. 配置目标：
 - 区域：选择存在现有托管前缀列表或要创建托管前缀列表的区域。
 - 前缀列表：选择现有托管前缀列表或创建新的托管前缀列表
6. 在所需版本下，选择以下选项之一：
 - 始终跟踪最新版本：如果希望前缀列表在基础设施变更时保持最新状态，而无需人工干预，请选择此选项进行自动更新。
 - 跟踪特定版本：如果需要可预测、可控的更新，并且希望手动批准对前缀列表的更改，请选择此选项以获得稳定性。
7. 选择创建目标。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用下面的 AWS CLI 命令创建 IPAM 前缀列表解析器目标：

- 使用步骤 1 中的解析器 ID 和现有的前缀列表 ID，执行 [create-ipam-prefix-list-resolver-target](#) 命令。

IPAM 现在会根据规则自动更新前缀列表。前缀列表将填充符合您条件的 CIDR。

步骤 3：监控版本和同步

创建前缀列表解析器和目标后，前缀列表解析器会根据规则生成 CIDR 版本，然后目标会将这些 CIDR 从解析器同步到特定托管前缀列表。每个版本都是在特定时刻与规则匹配的 CIDR 的快照。每次由于基础设施变更导致 CIDR 列表发生变化时，版本号都会递增。

版本示例：

初始状态（版本 1）

生产环境：

- vpc-prod-web (10.1.0.0/16) - 标记为 env=prod
- vpc-prod-db (10.2.0.0/16) - 标记为 env=prod

解析器规则：包含所有标记为 env=prod 的 VPC

版本 1 CIDR：10.1.0.0/16、10.2.0.0/16

基础架构变更（版本 2）

添加了新的 VPC：

- vpc-prod-api (10.3.0.0/16) - 标记为 env=prod

IPAM 会自动检测更改并创建新版本。

版本 2 CIDR：10.1.0.0/16、10.2.0.0/16、10.3.0.0/16

本节介绍如何使用 AWS 控制台或 AWS CLI 监控版本创建以及如何使用 AWS CLI 监控同步成功情况。

此外，建议您针对故障指标设置 CloudWatch 警报，因为您可能需要重新评估和调整 CIDR 选择规则，以保持版本和前缀列表大小的限制范围内。有关与 IPAM 前缀列表相关的 CloudWatch 指标的列表，请参阅 [IPAM 前缀列表解析器指标](#)。

AWS Management Console

查看创建的版本并监控目标同步

1. 在 IPAM 控制台中，选择前缀列表解析器。
2. 选择在步骤 1 中创建的解析器。
3. 在解析器详细信息页面上，选择版本选项卡。在这里，您将看到解析器创建的任何版本以及版本中的所有 CIDR。
4. 在解析器详细信息页面上，选择监控选项卡。在此视图中，[IPAM 前缀列表解析器指标](#)以图表形式呈现：
 - 前缀列表解析器版本创建成功
 - 前缀列表解析器版本创建失败
5. 在监控选项卡中，还可以通过选择为前缀列表解析器版本创建创建警报来配置 CloudWatch 警报。您将定向到 CloudWatch 控制台，其中已为指标部分配置了警报。有关如何完成告警创建的更多信息，请参阅《Amazon CloudWatch 用户指南》中的[根据静态阈值创建 CloudWatch 告警](#)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用下面的 AWS CLI 命令监控版本和同步：

1. 使用 [get-ipam-prefix-list-resolver-version-entries](#) 命令查看解析器创建的最新版本。
2. 使用 [describe-ipam-prefix-list-resolver-targets](#) 命令监控解析器目标同步状态。

监视器命令显示：

- state - 当前同步状态 (create-complete、modify-complete 等)
- lastSyncedVersion - 上次成功同步的版本
- desiredVersion - 要同步到的目标版本
- stateMessage - 同步失败时的错误详细信息

Important

为了支持回滚 workflow，IPAM 将为其每个目标保留前 10 个前缀列表解析器版本的副本；此外，如果超过此阈值的版本再有 7 天未被引用，IPAM 将删除这些版本。

步骤 4：（可选）启用和禁用 IPAM 前缀列表同步

如果已将托管前缀列表配置为 IPAM 前缀列表目标，并且您想要更改前缀列表而无需访问 IPAM 前缀列表解析器目标的权限，则可以[修改托管前缀列表](#)并禁用与 IPAM 前缀列表解析器的同步。禁用后，前缀列表 CIDR 不会自动更新，您可以对其进行更改。启用后，前缀列表 CIDR 将根据关联的解析器的 CIDR 选择规则自动更新。

更改 VPC CIDR 的监控状态

请按照本部分中的步骤更改 VPC CIDR 的监控状态。如果您不希望 IPAM 管理或监控 VPC 并允许分配给该 VPC 的 CIDR 可供使用，则可能需要将 VPC CIDR 从已监控更改为已忽略。如果您希望 IPAM 管理或监控 VPC CIDR，则可能需要将 VPC CIDR 从已忽略更改为已监控。

Note

- 不能忽略公有范围内的 VPC CIDR。
- 如果忽略 CIDR，您仍然需要为 CIDR 中的活动 IP 地址付费。有关更多信息，请参阅 [IPAM 定价](#)。
- 如果忽略 CIDR，您仍然可以查看 CIDR 中的 IP 地址历史记录。有关更多信息，请参阅 [查看 IP 地址历史记录](#)。

您可以将 VPC CIDR 的监控状态更改为已监控或已忽略：

- **已监控**：IPAM 已检测到 VPC CIDR，正在监控该 VPC CIDR 是否与其他 CIDR 和分配规则合规性重叠。
- **已忽略**：已选择该 VPC CIDR 免于监控。不会评估忽略的 VPC CIDR 是否与其他 CIDR 或分配规则合规性重叠。选择忽略 VPC CIDR 后，从 IPAM 池中分配给它的任何空间都将返回到池中，并且不会通过自动导入再次导入该 VPC CIDR（如果在池中设置了自动导入分配规则）。

AWS Management Console

更改分配给 VPC 的 CIDR 的监控状态

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Resources (资源)。
3. 从内容窗格顶部的下拉菜单中，选择要使用的私有范围。
4. 在内容窗格中，选择 VPC 并查看 VPC 的详细信息。
5. 在 VPC CIDR 下，选择分配给 VPC 的 CIDR 之一，然后选择操作 > 标记为已忽略或取消标记为已忽略。
6. 选择 Mark as ignored (标记为已忽略) 或 Unmark as ignored (取消标记为已忽略)。

Command line

请使用以下 AWS CLI 命令更改 VPC CIDR 的监控状态：

1. 获取范围 ID：[describe-ipam-scopes](#)
2. 查看 VPC CIDR 的当前监控状态：[get-ipam-resource-cidrs](#)
3. 更改 VPC CIDR 的状态：[modify-ipam-resource-cidr](#)
4. 查看 VPC CIDR 的新监控状态：[get-ipam-resource-cidrs](#)

创建额外范围

按照本部分中的步骤创建额外范围。

范围是 IPAM 中最高级别的容器。创建 IPAM 时，IPAM 会为您创建两个默认范围。每个范围代表单个网络的 IP 空间。私有范围适用于所有私有空间。公开范围适用于所有公有空间。范围使您能够跨多个未连接的网络重复使用 IP 地址，而不会导致 IP 地址重叠或冲突。

创建 IPAM 时，将为您创建默认范围（一个私有范围和一个公有范围）。您可以创建额外的私有范围。您不能创建额外的公有范围。

如果需要对多个断开连接的私有网络的支持，可以创建额外的专有范围。其他私有范围允许您创建池和管理使用相同 IP 空间的资源。

⚠ Important

如果 IPAM 发现了带有私有 IPv4 或私有 IPv6 CIDR 的资源，则资源 CIDR 将会导入到默认私有范围中，并且不会出现在您创建的任何其他私有范围中。您可以将 CIDR 从默认私有范围移动到另一个私有范围。有关信息，请参阅[在范围之间移动 VPC CIDR](#)。

AWS Management Console

要创建额外私有范围

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Scopes (范围)。
3. 选择 Create scope (创建范围)。
4. 选择要向其添加范围的 IPAM。
5. 添加范围的描述。
6. 选择 Create scope (创建范围)。
7. 您可以通过在导航窗格中选择 Scopes (范围) 来查看 IPAM 中的范围。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令创建额外的私有范围：

1. 查看您的当前范围：[describe-ipam-scopes](#)
2. 创建一个新的私有范围：[create-ipam-scope](#)
3. 查看您的当前范围以查看新范围：[describe-ipam-scopes](#)

删除 IPAM

如果不再需要 IPAM、需要重组 IP 地址管理或者想要用新的 IPAM 配置重新开始，则可能需要将其删除。删除 IPAM 可以帮助简化 IP 地址管理，并且与不断变化的业务或运营要求保持一致。

按照本部分中的步骤删除 IPAM。有关增加可以拥有的 IPAM 的默认数量而不是删除现有 IPAM 的信息，请参阅[IPAM 的配额](#)。

Note

删除 IPAM 将删除与 IPAM 关联的所有受监控数据，包括 CIDR 的历史数据。

AWS Management Console

要删除 IPAM

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 IPAM。
3. 在内容窗格中，选择 IPAM。
4. 选择 Actions (操作) > Delete IPAM (删除 IPAM) 。
5. 请执行以下操作之一：
 - 选择 Cascade delete (级联删除) 以删除 IPAM、私有作用域、私有作用域中的池，以及私有作用域中池中的所有分配。如果公有作用域中存在池，则无法使用此选项删除 IPAM。如果使用此选项，IPAM 将执行以下操作：
 - 取消分配在私有作用域池中分配给 VPC 资源 (如 VPC) 的所有 CIDR。

Note

启用此选项不会删除任何 VPC 资源。与资源关联的 CIDR 将不再从 IPAM 池中分配，但 CIDR 本身将保持不变。

- 取消预置在私有作用域中预置给 IPAM 池的所有 IPv4 CIDR。
 - 删除私有作用域中的所有 IPAM 池。
 - 删除 IPAM 中的所有非原定设置私有作用域。
 - 删除原定设置的公有和私有作用域以及 IPAM。
- 如果未选择 Cascade delete (级联删除) 复选框，则在删除 IPAM 之前，必须执行以下操作：
- 释放 IPAM 池内的分配。有关更多信息，请参阅 [释放分配](#)。
 - 取消预置为 IPAM 中的池预置的 CIDR。有关更多信息，请参阅 [从池中取消预置 CIDR](#)。
 - 删除任何其他非默认范围。有关更多信息，请参阅 [删除范围](#)。
 - 删除 IPAM 池。有关更多信息，请参阅 [删除池](#)。

6. 输入 **delete**，然后选择 Delete (删除)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令删除 IPAM：

1. 查看当前的 IPAM：[describe-ipams](#)
2. 删除 IPAM：[delete-ipam](#)
3. 查看已更新的 IPAM：[describe-ipams](#)

要创建新的 IPAM，请参阅 [创建 IPAM](#)。

删除池

AWS 中的 IPAM 池表示可在特定 AWS 环境或组织中分配和管理的 IP 地址的定义范围。池用于整理 IP 地址空间，实现自动化 IP 地址管理，并在您的云基础架构中执行 IP 地址治理策略。

您可能需要删除 IPAM 池，以移除未使用或不必要的 IP 地址空间，然后将其回收用于其他用途。如果 IP 地址池中有分配，则无法删除该地址池。您必须先释放分配和 [从池中取消预置 CIDR](#)，然后才能删除池。

按照本部分中的步骤删除 IPAM 池。

AWS Management Console

删除池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 从内容窗格顶部的下拉菜单中，选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 在内容窗格中，选择要删除其 CIDR 的池。
5. 选择 Actions (操作) > Delete pool (删除池)。

6. 输入 **delete**，然后选择 Delete (删除)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令删除池：

1. 查看池并获取 IPAM 池 ID：[describe-ipam-pools](#)
2. 删除池：[delete-ipam-pool](#)
3. 查看您的池：[describe-ipam-pools](#)

要创建新的池，请参阅 [创建顶级 IPv4 池](#)。

删除范围

如果 IPAM 范围不再用于其预期用途，例如在您重组网络、整合区域或调整 IP 地址分配时，您可能需要将其删除。删除未使用的范围有助于简化 IPAM 配置并优化 AWS 中的 IP 地址管理。

Note

如果满足以下任一条件，您将无法删除范围：

- 范围是默认范围。创建 IPAM 时，会自动创建两个默认范围（一个公有范围，一个私有），且不能删除。要查看范围是否为默认范围，请查看范围详细信息中的范围类型。
- 范围中有一个或多个池。您必须先[删除池](#)，然后才能删除范围。

AWS Management Console

要删除范围

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Scopes (范围)。
3. 在内容窗格中，选择要删除的范围。
4. 选择 Actions (操作) > Delete scope (删除范围)。

5. 输入 **delete** ，然后选择 Delete (删除) 。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令删除范围：

1. 查看范围：[describe-ipam-scopes](#)
2. 删除范围：[delete-ipam-scope](#)
3. 查看更新范围：[describe-ipam-scopes](#)

要创建新范围，请参阅 [创建额外范围](#)。要删除 IPAM，请参阅 [删除 IPAM](#)。

从池中取消预置 CIDR

您可能想要取消预置池 CIDR，以释放 IP 地址空间、简化 IP 地址管理、为网络变更做好准备或满足合规性要求。取消预置池 CIDR 可以更好地控制和优化 IPAM 中的 IP 地址分配，同时确保回收未使用的 IP 空间并使其可供将来使用。如果池中有分配，则无法取消预置 CIDR。要删除分配，请参阅 [the section called “释放分配”](#)。

按照本部分中的步骤从 IPAM 池中取消预置 CIDR。取消预置所有池 CIDR 时，该池不能再用于分配。在使用该池进行分配之前，必须先向池预置一个新的 CIDR。

AWS Management Console

要取消预置池 CIDR

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池) 。
3. 从内容窗格顶部的下拉菜单中，选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 在内容窗格中，选择要取消预置其 CIDR 的池。
5. 选择 CIDRs 选项卡。
6. 选择一个或多个 CIDR 并选择 Deprovision CIDRs (取消预置 CIDR) 。
7. 选择 Deprovision CIDR (取消预置 CIDR) 。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令取消预置池 CIDR：

1. 获取 IPAM 池 ID：[describe-ipam-pools](#)
2. 查看池的当前 CIDR：[get-ipam-pool-cidrs](#)
3. 取消预置 CIDR：[deprovision-ipam-pool-cidr](#)
4. 查看已更新的 CIDR：[get-ipam-pool-cidrs](#)

要为池预置新的 CIDR，请参阅 [从池中取消预置 CIDR](#)。如果要删除池，请参阅 [删除池](#)。

编辑 IPAM 池

您可能需要编辑池以执行以下操作之一：

- 更改池的分配规则。有关分配规则的更多信息，请参阅 [创建顶级 IPv4 池](#)。
- 修改池的名称、描述或其他元数据，以改进 IPAM 中的组织和可见性。
- 更改池选项，例如自动导入已发现的资源，从而优化 IPAM 的自动 IP 地址管理。

按照本部分中的步骤编辑 IPAM 池。

AWS Management Console

要编辑池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，默认的私有范围被选中。如果您不想使用默认的私有范围，请从内容窗格顶部的下拉菜单中选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)
4. 在内容窗格中，选择要编辑其 CIDR 的池。
5. 选择 Actions (操作) > Edit (编辑)。
6. 对池进行您需要的任何更改。有关池配置选项的信息，请参阅 [创建顶级 IPv4 池](#)。

7. 选择更新。

Command line

使用以下 AWS CLI 命令编辑池：

1. 获取 IPAM 池 ID：[describe-ipam-pools](#)
2. 修改池：[modify-ipam-pool](#)

启用成本分配

启用成本分配后，可以将[活动 IP 地址的费用](#)分配给使用 IP 地址的账户，而不是分配给 IPAM 所有者。这对于大型组织非常有用，在这些组织中，委派的 IPAM 管理员使用 IPAM 集中管理 IP 地址，并且每个账户负责自己的使用，从而无需手动计算账单。

在计量模式下[创建 IPAM](#) 或[修改 IPAM](#) 时，可以使用成本分配选项，其中：

- IPAM 所有者（默认）：拥有 IPAM 的 AWS 账户将为 IPAM 中管理的所有活动 IP 地址付费。
- 资源所有者：拥有 IP 地址的 AWS 账户将为活动 IP 地址付费。

要求

- 您的 IPAM 必须与[AWS Organizations 集成](#)。
- IPAM 必须由 AWS 组织中委派的 IPAM 管理员创建。
- IPAM 的主区域必须是默认启用的区域，不能是[选择加入区域](#)。

收费的工作原理

- 尽管您可以在组织内分配 IP 地址费用，但所有 IPAM 费用都将通过[AWS Organizations 整合账单](#)整合到该组织的付款人账户。
- 启用成本分配后，组织成员账户仍可以在其账户账单中查看个人 IPAM 使用情况和费用。
- 启用成本分配后，IPAM ARN 将在个人账户账单上显示，这样资源所有者便可追踪其 IPAM 活动 IP 使用情况。如果您使用[AWS Data Exports](#)，则 IPAM 费用将与关联的 IPAM ARN 一起在整合账户账单和个人账户账单中显示。
- 只有委派管理员组织内的账户才能收到其所拥有资源的费用。组织外部的 IP 地址费用将向 IPAM 所有者收取。

时间限制

- 启用成本分配后，您有 24 小时的时间选择退出。24 小时后，您无法在 7 天内更改设置。7 天后，您可以禁用成本分配。

将 VPC IPAM 与 Infoblox 基础设施集成

Amazon VPC IPAM 和 Infoblox 集成后，会将您的 AWS VPC IP 地址管理器 (IPAM) 连接到 [Infoblox](#)，从而让您能够通过现有的 Infoblox workflow 管理 AWS IP 地址，同时获得云原生 AWS 功能。

此集成解决了避免重复建设 IP 管理系统这一常见的企业难题。您不需要学习新工具以及为 AWS 和本地网络建立单独的流程，只需将 Infoblox 指定为 VPC IPAM 作用域的管理机构，并继续使用熟悉的 Infoblox 界面进行所有 IP 地址操作。

集成过程概述

以下步骤概述了完整的集成过程：

1. 配置 IPAM 作用域 (在本文档中介绍)：Amazon VPC IPAM 委托管理员创建一个新作用域或修改现有作用域，以将 Infoblox 作为其外部管理机构。
2. 配置 Infoblox (在本文档之外介绍)：请参阅[后续步骤](#)。
3. 创建顶级池：Amazon VPC IPAM 委托管理员在链接到 Infoblox 的作用域内创建一个池。最初该池未分配任何 CIDR。
4. 预调配来自外部管理机构的 CIDR：Amazon VPC IPAM 委托管理员为该池预调配一个 CIDR。您可以请求任何可用 CIDR (由 Infoblox 在允许范围内选择)，也可请求特定 CIDR (Infoblox 根据可用性接受或拒绝)。IPAM 会自动与 Infoblox 协调，来获取和预调配批准的 CIDR。
5. 继续使用标准的 IPAM 操作：按照标准的 Amazon VPC IPAM 过程，使用分配的 CIDR 创建子池和 VPC。

何时使用此集成

如果您已经使用或计划使用 Infoblox 进行本地网络管理，并且希望将现有的 IP 管理实践扩展到 AWS 而不建立单独的系统，请使用此集成。

先决条件

在开始配置此集成之前，请确保您满足以下条件：

- VPC IPAM 高级套餐：已在您的 AWS 账户中启用。有关更多信息，请参阅 [VPC IPAM 高级套餐](#)。
- 所需 IAM 权限：详见以下所列
- Infoblox 资源标识符：由您的 Infoblox 管理员提供

用于 Infoblox 的 IAM 角色

创建一个供 Infoblox 主体代入的 IAM 角色，或使用一个现有的角色。该角色需要以下权限：

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

有关如何为 IAM 角色或策略添加这些权限的说明，请参阅《IAM 用户指南》中的 [添加和删除 IAM 身份权限](#)。

Note

除了启用此集成所需的这些权限外，Infoblox 可能还需要 VPC IPAM 发现权限。

在 VPC IPAM 中配置 Infoblox 集成

您可以在 AWS VPC IPAM 控制台或 AWS CLI 中创建或修改作用域时启用 Infoblox 集成。

Important

Infoblox 集成仅适用于私有作用域，不适用于公有作用域。

创建具有 Infoblox 集成的新作用域

1. 通过 <https://console.aws.amazon.com/vpc/> 打开 Amazon VPC 控制台。

2. 在导航窗格中，选择 IPAM，然后选择作用域。
3. 选择 Create scope (创建范围)。
4. 对于作用域设置，请执行以下操作：
 - IPAM ID 会自动填充。
 - (可选) 对于名称标签，输入作用域的名称。
 - (可选) 对于描述，输入作用域的描述。
5. 对于作用域管理机构，请选择 Infoblox IPAM。
6. 对于 Infoblox 资源标识符，请按 `<version>.identity.account.<entity_realm>.<entity_id>` 格式输入 Infoblox 资源标识符。
7. 验证您是否具有信息框中所示的所需 IAM 权限。
8. 选择 Create scope (创建范围)。

与此相关的 AWS CLI 命令是 [create-ipam-scope](#)。

修改现有的作用域

要将现有作用域的作用域管理机构从 Amazon VPC IPAM 更改为 Infoblox IPAM，请编辑作用域设置并按照之前过程中的相同配置步骤进行操作。

与此相关的 AWS CLI 命令是 [modify-ipam-scope](#)。

后续步骤

这样就完成了此集成所需的 Amazon VPC IPAM 配置。在配置好作用域管理机构后，您可以在该作用域内创建一个顶级 IPAM 池。有关更多信息，请参阅 [创建顶级 IPv4 池](#)。

此集成还需要配置一个 Infoblox 源池、验证发现作业状态、设置将由 Infoblox 管理的私有作用域、为 Amazon VPC IPAM 启用 Infoblox 管理，以及通过 Infoblox 集成或直接从 Infoblox 门户创建池。

有关此集成所需的 Infoblox 操作的信息，请参阅 Infoblox 文档中的《AWS IPAM 集成用户指南》。

启用预置私有 IPv6 GUA CIDR

如果希望自己的私有网络支持 IPv6，并且不打算将流量从这些地址路由到互联网，则可向私有范围内的 IPAM 池预置私有 IPv6 ULA 或 GLA 范围。

有关私有 IPv6 寻址的重要详细信息，请参阅《Amazon VPC 用户指南》中的[私有 IPv6 地址](#)。

私有 IPv6 地址有两种类型：

- IPv6 ULA 范围：[RFC4193](#) 中定义的 IPv6 地址。这些地址范围总会以“fc”或“fd”开头，因此很容易识别。有效的 IPv6 ULA 空间是指任何低于 fd00::/8 且不与 Amazon 预留范围 fd00::/16 重叠的空间。
- IPv6 GUA 范围：[RFC3587](#) 中定义的 IPv6 地址。使用 IPv6 GUA 范围作为私有 IPv6 地址的选项默认处于禁用状态，必须在启用后才能使用。

要使用 IPv6 ULA 地址范围，可在向 IPAM 池预置 CIDR 时选择 IPv6 选项，再输入 IPv6 ULA 范围。不过，要使用自己的 IPv6 GUA 范围作为私有 IPv6 地址，必须先完成本节中的步骤。默认情况下禁用该选项。

Note

- 在使用私有 IPv6 GUA 范围时，要求使用自己拥有的 IPv6 GUA 范围。
- IPAM 发现具有 IPv6 ULA 和 GUA 地址的资源，并监控池中是否存在重叠的 IPv6 ULA 和 GUA 地址空间。
- 如果要从具有私有 IPv6 地址的资源连接到互联网，必须通过另一个子网中具有公有 IPv6 地址的资源路由流量，才能实现该目的。
- 如果已为 VPC 分配私有 IPv6 GUA 范围，则不能使用与同一 VPC 中私有 IPv6 GUA 空间重叠的公有 IPv6 GUA 空间。
- 支持具有私有 IPv6 ULA 及 GUA 地址范围的资源之间的通信（例如跨 Direct Connect、VPC 对等连接、中转网关或 VPN 连接）。
- 私有 GUA IPv6 范围无法转换为公开传播的 IPv6 GUA 范围。

AWS Management Console

启用预置私有 IPv6 GUA CIDR

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 IPAM。
3. 选择 IPAM，再依次选择操作 > 编辑。
4. 在私有 IPv6 GUA CIDR 下，选择启用向私有 IPv6 IPAM 池预置 GUA CIDR 空间。
5. 选择保存更改。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令启用预置私有 IPv6 GUA CIDR：

1. 使用 [describe-ipams](#) 查看当前的 IPAM
2. 使用 [modify-ipam](#) 修改 IPAM 并纳入用于 `enable-private-gua` 的选项。

启用预置私有 IPv6 GUA CIDR 的选项后，即可为池预置私有 IPv6 GUA CIDR。有关更多信息，请参阅 [将 CIDR 预置到池](#)。

强制使用 IPAM 通过 SCP 进行 VPC 创建

Note

此部分仅在您启用了 IPAM 与 AWS Organizations 集成时适用您。有关更多信息，请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)。

此部分描述如何在 AWS Organizations 中创建服务控制策略，从而要求组织中的成员在创建 VPC 时使用 IPAM。服务控制策略 (SCP) 是一种组织策略，使您能够管理组织中的权限。有关更多信息，请参阅 AWS Organizations 用户指南中的 [服务控制策略](#)。

创建 VPC 时强制使用 IPAM

按照本部分中的步骤，要求组织中的成员在创建 VPC 时使用 IPAM。

要创建 SCP 并将 VPC 创建限制为 IPAM

1. 按照《AWS Organizations 用户指南》中的 [Create a service control policy](#) 中的步骤操作，并在 JSON 编辑器中输入以下文本：

JSON

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

```
"Statement": [{
  "Effect": "Deny",
  "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
  "Resource": "arn:aws:ec2:*:*:vpc/*",
  "Condition": {
    "Null": {
      "ec2:Ipv4IpamPoolId": "true"
    }
  }
}]
}
```

2. 将策略附加到组织中的一个或多个组织单位。有关更多信息，请参阅《AWS Organizations 用户指南》中的 [Attach policies](#) 和 [Detach policies](#)。

创建 VPC 时强制使用 IPAM 池

按照本部分中的步骤，要求组织中的成员在创建 VPC 时使用特定 IPAM 池。

要创建 SCP 并将 VPC 创建限制为 IPAM 池

1. 按照《AWS Organizations 用户指南》中的 [Create a service control policy](#) 中的步骤操作，并在 JSON 编辑器中输入以下文本：

JSON

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

2. 将 ipam-pool-0123456789abcdefg 示例值更改为您希望对用户进行限制的 IPv4 池 ID。

3. 将策略附加到组织中的一个或多个组织单位。有关更多信息，请参阅《AWS Organizations 用户指南》中的 [Attach policies](#) 和 [Detach policies](#)。

对除给定 OU 列表之外的所有 OU 强制实施 IPAM

按照本部分中的步骤，对除给定组织单位 (OU) 列表之外的所有组织单位强制实施 IPAM。本部分介绍的策略需要组织中除您在 `aws:PrincipalOrgPaths` 中指定的 OU 之外的 OU 使用 IPAM 创建和扩展 VPC。列出的 OU 可以在创建 VPC 时使用 IPAM，也可以手动指定 IP 地址范围。

创建 SCP 并对除给定 OU 列表之外的所有 OU 强制实施 IPAM

1. 按照《AWS Organizations 用户指南》中的 [Create a service control policy](#) 中的步骤操作，并在 JSON 编辑器中输入以下文本：

JSON

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

2. 删除示例值 (例如 `o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/`) 并添加您希望可以选择 (但不要求) 使用 IPAM 的 OU 的 AWS Organizations 实体路径。有关实体路径的更多信息，请参阅《IAM 用户指南》中的 [了解 AWS Organizations 实体路径](#) 和 [aws:PrincipalOrgPaths](#)。

3. 将策略附加到组织根。有关更多信息，请参阅《AWS Organizations 用户指南》中的 [Attach policies](#) 和 [Detach policies](#)。

从 IPAM 中排除组织单位

如果您的 IPAM 与 AWS Organizations 集成，则可以将[组织单位 \(OU\)](#) 排除在 IPAM 管理之外。排除 OU 时，IPAM 不会管理该 OU 中账户的 IP 地址。此功能使您可以更灵活地使用 IPAM。

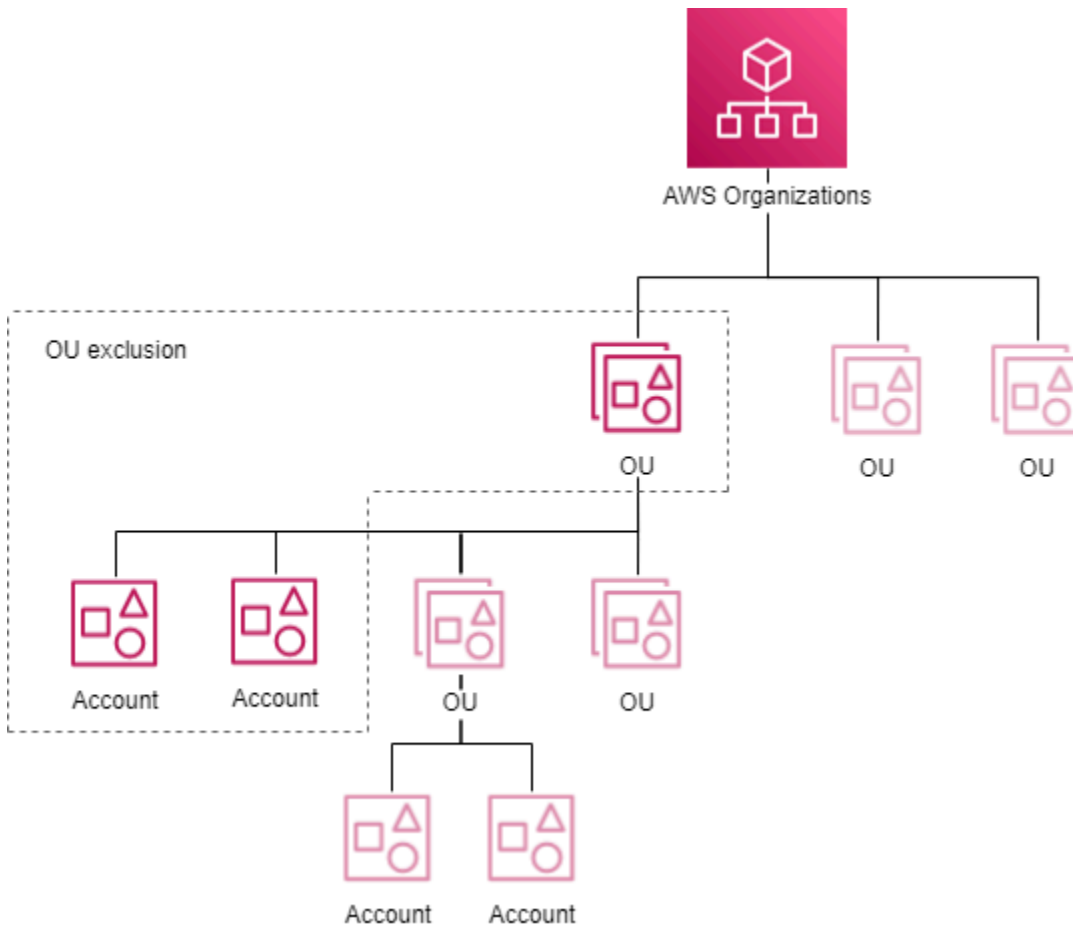
您可以通过以下方式使用 OU 排除项：

- 为业务的特定部分启用 IPAM：如果您在 AWS Organizations 中有多个业务部门或子公司，则现在可以将 IPAM 仅用于需要该功能的业务部门或子公司。
- 将沙盒账户分开：您可以从 IPAM 排除沙盒账户，只关注对 IP 管理真正重要的账户。

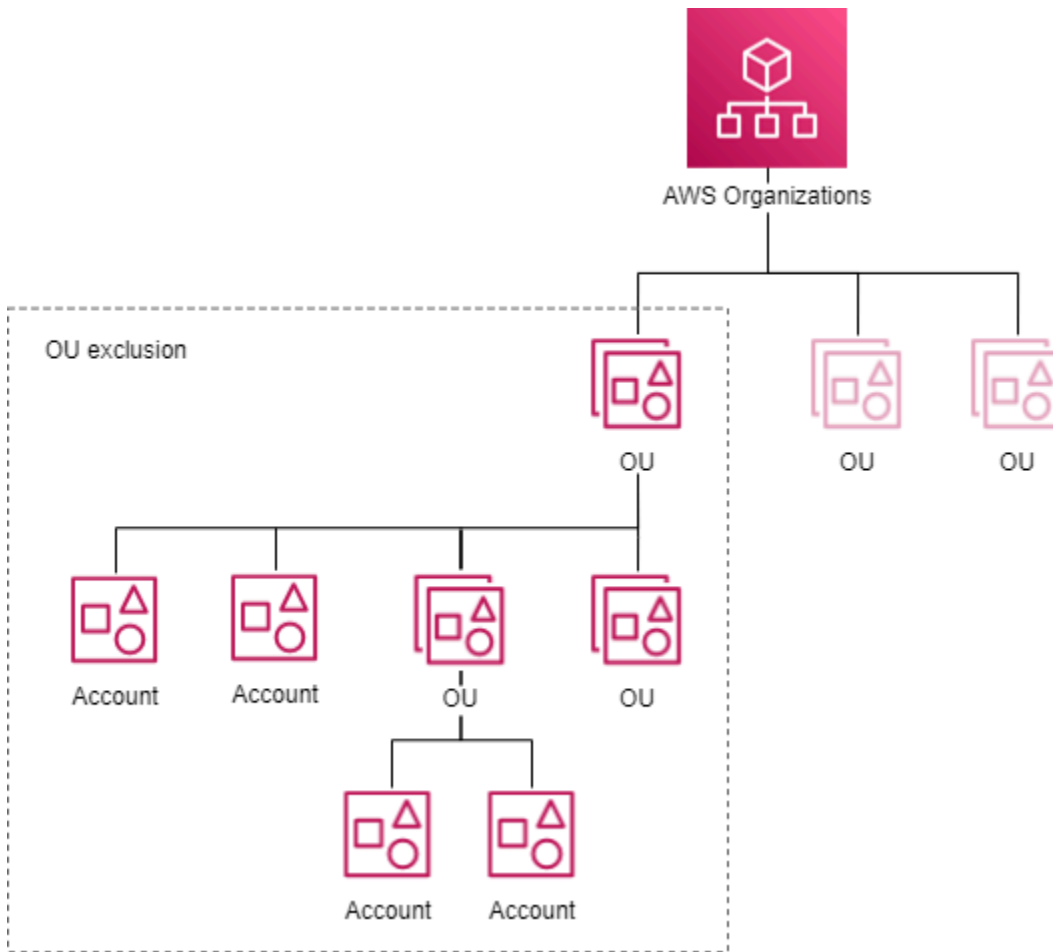
OU 排除项工作原理

本节中的图演示了在 IPAM 中添加 OU 排除项的两个使用案例。

第一张图显示仅对父 OU 添加组织单位 (OU) 排除项的影响。因此，IPAM 不会管理父 OU 中账户的 IP 地址。IPAM 将管理排除项之外的其他 OU 中账户的 IP 地址。



第二张图显示对父 OU 和所有子 OU 添加组织单位 (OU) 排除项的影响。因此, IPAM 不会管理父 OU 中账户或任意子 OU 中账户的 IP 地址。IPAM 将管理排除项之外的 OU 中账户的 IP 地址。



添加或移除 OU 排除项

完成本节中的步骤以添加或移除 OU 排除项。

Note

- 即使委托的 IPAM 管理员账户位于已排除 OU 中，也不会将其排除在外。
- 您的 IPAM 必须与 AWS Organizations 集成才能添加 OU 排除项。组织中必须有 OU。
- 您必须是委托的 IPAM 管理员才能查看、添加或移除 OU 排除项。
- IPAM 需要时间才能发现最近创建的组织单位。
- 每次资源发现可以添加的排除项数量有默认配额。有关更多信息，请参阅 [IPAM 的配额](#) 中的每次资源发现的组织单位排除项数。
- 如果您 [与其他账户共享资源发现](#)，则该账户可以看到其上的 OU 排除项，其中包含资源发现所有者组织的组织 ID、根 ID 和组织单位 ID 等信息。

AWS Management Console

要添加或删除 OU 排除项

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择资源发现。
3. 选择默认资源发现。
4. 选择编辑。
5. 在组织单位排除项下，执行以下操作：
 - 要添加 OU 排除项：
 - 如果要排除 OU 及其所有子 OU：
 - 在表中找到该 OU 并选中该复选框。系统会自动选择所有子 OU。
 - 如果想仅排除父 OU 账户：
 - 在表中找到该 OU 并选中该复选框。系统会自动选择所有子 OU。取消选择所有子 OU。
 - 或者，您可以使用操作列仅选择父 OU 或选择父 OU 和子 OU：
 - 选择所有子 OU：在排除项中包含所有子 OU。选择 OU 后，屏幕上会添加该 OU。每个 OU 均包含 OU 排除项的 ID 和 [实体路径](#)。
 - 仅选择此 OU：在排除项中仅包含此 OU。选择 OU 后，屏幕上会添加该 OU。每个 OU 均包含 OU 排除项的 ID 和 [实体路径](#)。
 - 复制 OU 实体路径：复制组织实体路径以根据需要使用。
 - 如果您已经知道 AWS Organizations 实体路径或者想要构建该路径：
 - 选择输入组织单位排除项，然后输入 OU 排除项的 [实体路径](#)。使用由 / 分隔的 AWS Organizations ID 构建 OU 的路径。以 /* 结尾的路径包含所有子 OU。
 - 示例 1
 - 子 OU 的路径：o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccecc/ou-jkl0-awsddddd/
 - 在此示例中，o-a1b2c3d4e5 是组织 ID，r-f6g7h8i9j0example 是根 ID，ou-ghi0-awsccecc 是 OU ID，ou-jkl0-awsddddd 是子 OU ID。
 - IPAM 不会管理子 OU 中账户的 IP 地址。
 - 示例 2

- 所有子 OU 都将成为排除项一部分的路径：o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccecc/*
 - 在此示例中，IPAM 不会管理 OU (ou-ghi0-awsccecc) 中账户的 IP 地址，也不会管理 OU 所属任何子 OU 中账户的 IP 地址。
- 要移除 OU 排除项：
- 选择已添加的 OU 旁边的 X。OU ID 之后的 /* 表示其是父 OU，而子 OU 是 OU 排除项的一部分。
6. 选择保存更改。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

1. 使用 [describe-ipam-resource-discoveries](#) 查看资源发现详细信息，以获取下一步的默认资源发现的 ID。

输入：

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

输出：

```
{
  "IpamResourceDiscoveries": [
    {
      "OwnerId": "111122223333",
      "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",
      "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-resource-discovery/ipam-res-disco-1234567890abcdef0",
      "IpamResourceDiscoveryRegion": "us-east-1",
      "OperatingRegions": [
```

```
    {
        "RegionName": "us-east-1"
    },
    {
        "RegionName": "us-west-1"
    },
    {
        "RegionName": "us-west-2"
    }
],
"IsDefault": true,
"State": "modify-complete",
"Tags": []
}
]
}
```

2. 使用 [modify-ipam-resource-discovery](#) 以及 `--add-organizational-unit-exclusions` 或 `--remove-organizational-unit-exclusions` 选项，在资源发现中添加或移除组织单位排除项。您需要输入 AWS Organizations 实体路径。使用由 / 分隔的 AWS Organizations ID 构建 OU 的路径。以 /* 结尾的路径包含所有子 OU。在添加或移除参数中不能多次包含相同的实体路径。

- 示例 1

- 子 OU 的路径 : `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccecc/ou-jkl0-awsddddd/`

- 在此示例中，o-a1b2c3d4e5 是组织 ID，r-f6g7h8i9j0example 是根 ID，ou-ghi0-awsccecc 是 OU ID，ou-jkl0-awsdcccc 是子 OU ID。
- IPAM 不会管理子 OU 中账户的 IP 地址。
- 示例 2
 - 所有子 OU 都将成为排除项一部分的路径：o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccecc/*
 - 在此示例中，IPAM 不会管理 OU (ou-ghi0-awsccecc) 中账户的 IP 地址，也不会管理 OU 所属任何子 OU 中账户的 IP 地址。

Note

生成的排除项集不得“重叠”，这意味着两个或多个 OU 排除项不得排除同一 OU。不重叠的实体路径示例：

- 路径 1 =“o-1/r-1/ou-1/”
- 路径 2 =“o-1/r-1/ou-1/ou-2/”

这些路径不重叠，因为路径 1 仅排除 ou-1 下的账户，而路径 2 仅排除 ou-2 下的账户。

重叠的实体路径示例：

- 路径 1 =“o-1/r-1/ou-1/*”
- 路径 2 =“o-1/r-1/ou-1/ou-2/”

这些路径重叠，因为路径 1 同时表示“o-1/r-1/ou-1/”和“o-1/r-1/ou-1/ou-2/”，而“o-1/r-1/ou-1/ou-2/”与路径 2 重叠。

输入：

```
aws ec2 modify-ipam-resource-discovery \
  --ipam-resource-discovery-id ipam-res-disco-1234567890abcdef0 \
  --add-organizational-unit-exclusions OrganizationsEntityPath='o-a1b2c3d4e5/
r-f6g7h8i9j0example/ou-ghi0-awsccecc/*' \
  --remove-organizational-unit-exclusions OrganizationsEntityPath='o-
a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccecc/ou-jkl0-awsdcccc/' \
```

```
--region us-east-1
```

输出：

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

修改 IPAM 等级

IPAM 提供两个等级：免费等级和高级等级。切换到 Amazon VPC IP 地址管理器的高级套餐可以更精细地控制您的 IP 地址管理。随着网络复杂性的增加，这可能会有所帮助，让您能够更好地优化和管理 IP 地址空间。有关免费等级中提供的功能以及与高级等级相关的费用的更多信息，请参阅 [Amazon VPC 定价页面](#) 中的 IPAM 选项卡。

Note

在从高级等级切换到免费等级之前，您必须：

- 删除私有范围池。
- 删除非默认设置私有范围。

- 删除区域设置与 IPAM 主区域不同的池。
- 删除非默认设置资源发现关联。
- 删除分配给不是 IPAM 所有者的账户的池。

AWS Management Console

如需修改 IPAM 等级

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 IPAM。
3. 在内容窗格中，选择 IPAM。
4. 选择操作 > 编辑。

Note

如果您使用的是免费套餐，则会看到您的估计 IPAM 活跃 IP 总数为...

总活跃 IP 数是如果您从免费套餐切换到高级套餐则您的 IPAM 中需要向您收费的活跃 IP 地址数量。活动 IP 地址定义为与附加到 EC2 实例等资源的弹性网络接口 (ENI) 关联的 IP 地址或前缀。

- 此指标仅适用于免费套餐的客户。
- 如果您的 IPAM [与 AWS Organizations 集成](#)，则活动 IP 计数将涵盖所有组织账户。
- 您无法按 IP 类型 (公有/私有) 或类别 (IPv4/IPv6) 查看活动 IP 数的明细。
- IPAM 仅计入受监控账户拥有的 ENI 的 IP。共享子网的计数可能不准确。如果子网所有者或 ENI 所有者不在 IPAM 覆盖范围内，则不包括其 IP 地址。

5. 选择要用于 IPAM 的 IPAM 等级。
6. 选择保存更改。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令查看和修改 IPAM 等级：

1. 查看当前的 IPAM : [describe-ipams](#)
2. 修改 IPAM 等级 : [modify-ipam](#)
3. 查看已更新的 IPAM : [describe-ipams](#)

修改 IPAM 运营区域

运营区域是允许 IPAM 管理 IP 地址 CIDR 的 AWS 区域。IPAM 仅发现和监控您选择作为运营区域的 AWS 区域中的资源。

向 IPAM 添加操作区域使您能够跨多个 AWS 区域管理 IP 地址空间。这可以提高 IP 地址利用率、实现区域分割，并支持地理分布式基础架构。扩大 IPAM 的区域范围可以提高您的整体 IP 地址管理的灵活性和控制。

AWS Management Console

如需修改 IPAM 运营区域

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 IPAM。
3. 在内容窗格中，选择 IPAM。
4. 选择操作 > 编辑。
5. 在 IPAM 设置下，选择要用于 IPAM 的运营区域。
6. 选择保存更改。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令查看和修改 IPAM 运营区域：

1. 查看当前的 IPAM : [describe-ipams](#)
2. 添加或删除 IPAM 运营区域 : [modify-ipam](#)
3. 查看已更新的 IPAM : [describe-ipams](#)

将 CIDR 预置到池

按照本部分中的步骤将 CIDR 预置到池。如果您在创建池时已经预置了 CIDR，则如果池接近完全分配，则可能需要预置额外的 CIDR。要监控池的使用情况，请参阅 [使用 IPAM 控制面板监控 CIDR 使用情况](#)。

Note

术语 provision (预置) 和 allocate (分配) 在本用户指南和 IPAM 控制台中使用。Provision (预置) 在您将 CIDR 添加到 IPAM 池时使用。分配在您将 IPAM 池中的 CIDR 与 VPC 或弹性 IP 地址关联时使用。

AWS Management Console

要将 CIDR 预置到池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，默认的私有范围被选中。如果您不想使用默认的私有范围，请从内容窗格顶部的下拉菜单中选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 在内容窗格中，选择要将 CIDR 添加到其中的池。
5. 选择 Actions (操作) > Provision CIDRs (预置 CIDR)。
6. 请执行以下操作之一：
 - 如果要向公有范围内的池预置 CIDR，请输入网络掩码。
 - 如果要向私有范围内的 IPv4 池预置 CIDR，请输入 CIDR。
 - 如果要向私有范围内的 IPv6 池预置 CIDR，请注意以下几点：
 - 有关私有 IPv6 寻址的重要详细信息，请参阅《Amazon VPC 用户指南》中的 [私有 IPv6 地址](#)。
 - 要使用私有 IPv6 ULA 范围，则在要预置的 CIDR 下选择按网络掩码添加 ULA CIDR 并选择网络掩码大小，或者选择输入私有 IPv6 CIDR 并输入 ULA 范围。私有 IPv6 ULA 的有效范围为 /9 至 /60 (从 fd80::/9 开始)。
 - 要使用私有 IPv6 GUA 范围，必须先在 IPAM 上启用该选项 (请参阅 [启用预置私有 IPv6 GUA CIDR](#))。启用私有 IPv6 GUA CIDR 后，在输入私有 IPv6 CIDR 中输入 IPv6 GUA。

Note

- 默认情况下，您可以向区域池添加一个 Amazon 提供的 IPv6 CIDR 块。有关提高默认限制的信息，请参阅 [IPAM 的配额](#)。
- 您要预置的 CIDR 必须在范围内可用。
- 如果要将 CIDR 预置到池中的资源池，则您要预置的 CIDR 空间必须在池中可用。

7. 选择预置。
8. 您可以通过选择导航窗格中的 Pools (池)、选择一个池并查看该池的 CIDR 选项卡以查看 IPAM 中的 CIDR。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令将 CIDR 预置到池中：

1. 获取 IPAM 池的 ID：[describe-ipam-pools](#)
2. 获取预置到池中的 CIDR：[get-ipam-pool-cidrs](#)
3. 为池预置新的 CIDR：[provision-ipam-pool-cidr](#)
4. 获取预置到池中的 CIDR 并查看新的 CIDR：[get-ipam-pool-cidrs](#)

在范围之间移动 VPC CIDR

在范围之间移动 CIDR 可以优化 IP 地址分配、按区域组织、分离关注点、强制实施合规性以及适应基础设施的变化。这种灵活性有助于随着工作负载的变化高效管理您的 IP 地址空间。

按照本部分中的步骤将一个范围中的 VPC CIDR 移动到另一个范围。

Important

- 您只能移动 VPC CIDR。当您移动 VPC CIDR 时，VPC 的子网 CIDR 也会自动移动。
- 您只能将 VPC CIDR 从一个私有范围移动到另一个私有范围。您不能将 VPC CIDR 从公有范围移动到私有范围，也不能从私有范围移动到公有范围。

- 相同的 AWS 账户必须同时拥有这两个范围。
- 如果 VPC CIDR 当前是从私有范围内的池中分配的，移动请求将成功，但是在您从当前池中释放 VPC CIDR 分配之后，系统才会移动 VPC CIDR。有关释放分配的信息，请参阅[释放分配](#)。

AWS Management Console

移动分配给 VPC 的 CIDR

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Resources (资源)。
3. 从内容窗格顶部的下拉菜单中，选择要使用的范围。
4. 在内容窗格中，选择 VPC 并查看 VPC 的详细信息。
5. 在 VPC CIDRs (VPC CIDR) 下，选择分配给资源的 CIDR 之一，然后选择 Actions (操作) > Move CIDR to different scope (将 CIDR 移至其他范围)。
6. 选择要将 VPC CIDR 移动到的范围。
7. 选择 Move CIDR to different scope (将 CIDR 移至其他范围)。

Command line

使用以下 AWS CLI 命令移动 VPC CIDR：

1. 获取当前范围内的 VPC CIDR：[get-ipam-resource-cidrs](#)
2. 移动 VPC CIDR：[modify-ipam-resource-cidr](#)
3. 获取其他范围内的 VPC CIDR：[get-ipam-resource-cidrs](#)

使用 IPAM 策略定义公有 IPv4 分配策略

IPAM 策略是一组规则，这些规则用于定义如何将 IPAM 池中的公有 IPv4 地址分配给 AWS 资源。每条规则都将 AWS 服务映射到该服务将用于获取 IP 地址的 IPAM 池。单个策略可以有多个规则，并且可以应用于多个 AWS 区域。如果 IPAM 池中的地址耗尽，则服务将回退到 Amazon 提供的 IP 地址。策略可以应用于 AWS Organizations 中的各个 AWS 账户或实体。如果您[自带 IP \(BYOIP\)](#)，这将有助于降低您的 AWS 公有 IPv4 成本。

IPAM 策略的使用场景

使用 IPAM 策略具有以下优势：

- 通过使用 BYOIP 地址降低公有 IPv4 成本
- 集中控制您的 AWS 资源使用的 IP 池
- 确保整个组织的 IP 分配保持一致

工作原理

当您在强制执行 IPAM 策略的账户中创建需要公有 IP 地址的 AWS 资源时：

- IPAM 会按顺序检查您的策略规则。
- 如果某条规则与该资源类型匹配，IPAM 会从指定的池中分配一个 IP。
- 如果该池为空且启用了溢出功能，则 Amazon 会提供一个 IP 地址。
- 如果没有匹配的规则，则会应用默认行为。

支持的服务和资源

您可以创建 IPAM 策略，来定义如何将 IPAM 池中的公有 IPv4 地址分配给以下 AWS 服务和资源：

- 弹性 IP 地址 (EIP)
- 应用程序负载均衡器 (ALB)
- Amazon Relational Database Service (RDS)
- 区域 NAT 网关

Important

如果您在创建 AWS 资源时选择了特定的 IPAM 池或 EIP 分配 ID，则该设置将覆盖 IPAM 策略。

先决条件

- 已启用[高级套餐](#)的委托管理员账户中的一个 [IPAM](#)
- 一个具有 IPv4 地址的[公有 IPAM 池](#)

- 用于执行 IPAM 和 EC2 操作的 [IAM 权限](#)

术语

IPAM 策略

IPAM 策略是一组规则，这些规则用于定义如何将 IPAM 池中的公有 IPv4 地址分配给 AWS 资源。每条规则都将 AWS 服务映射到该服务将用于获取 IP 地址的 IPAM 池。单个策略可以有多个规则，并且可以应用于多个 AWS 区域。如果 IPAM 池中的地址耗尽，则服务将回退到 Amazon 提供的 IP 地址。策略可以应用于 AWS Organizations 中的各个 AWS 账户或实体。策略可以应用于 AWS Organizations 中的各个 AWS 账户或实体。

分配规则

IPAM 策略中用于将 AWS 资源类型映射到特定 IPAM 池的可选配置。如果未定义任何规则，则资源类型默认为使用 Amazon 提供的 IP 地址。

Target

可向其应用 IPAM 策略的单个 AWS 账户或 AWS 组织内的实体。

第 1 步：创建 IPAM 策略

使用 AWS 控制台：

按照以下步骤操作，使用 AWS 控制台创建一个 IAM 策略：

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在左侧导航窗格中，选择 Policies (策略)。
3. 选择创建策略。
4. 为您的策略输入一个名称 (可选)。
5. 选择要关联到此策略的 IPAM。
6. (可选) 添加标签。
7. 选择创建策略。

使用 AWS CLI：

使用 [create-ipam-policy](#) 命令。

第 2 步：添加分配规则

创建策略后，您需要添加分配规则来定义如何分配 IP 地址：

使用 AWS 控制台：

按照以下步骤操作，使用 AWS 控制台添加分配规则：

1. 在左侧导航窗格中，选择 Policies (策略)。
2. 选择在上一步中创建的策略。
3. 在策略详细信息页面中，选择分配规则选项卡。
4. 选择创建分配规则。
5. 配置服务配置：
 - 区域设置：选择要应用此策略的 AWS 区域 (us-east-1) 或本地区域。
 - 资源类型：选择此策略的 AWS 服务或资源类型 (弹性 IP 地址、RDS 数据库实例、应用程序负载均衡器或区域可用性模式的 NAT 网关)。
6. 配置规则配置：
 - IPAM 池：选择将提供 IP 地址的 IPAM 池。
 - 检查池详细信息 (区域设置、公有 IP 源、可用空间和可用 CIDR 范围)。
7. (可选) 选择添加新规则以创建其他规则。
8. 选择创建分配规则。

使用 AWS CLI：

使用 [modify-ipam-policy-allocation-rules](#) 命令。

第 3 步：启用策略

指定应使用此策略的账户。

使用 AWS 控制台：

按以下步骤操作，使用 AWS 控制台启用策略：

1. 在策略详细信息页面中，选择目标选项卡。
2. 选择管理策略目标。

3. 请执行以下操作之一：

- 如果用于单个账户（IPAM 未与 AWS Organizations 集成），请选择为您的账户启用。
- 如果 IPAM 已与 AWS Organizations 集成（您是委托管理员时）：
 - 在组织结构部分中，选择要应用此策略的账户或组织单元。
 - 为每个目标选中已启用复选框。
 - 选择保存更改。
 - **重要提示：**启用此策略将取代选定账户或组织单元中任何有效的 IPAM 策略。

使用 AWS CLI：

根据您的设置使用 [enable-ipam-policy](#) 命令：

如果用于单个账户（IPAM 未与 AWS Organizations 集成）：

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

如果 IPAM 已与 AWS Organizations 集成（您是委托管理员时），请设置策略以定位 AWS 组织中的帐户：

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

如果 IPAM 已与 AWS Organizations 集成（您是委托管理员时），请设置策略以定位组织单元：

```
aws ec2 enable-ipam-policy \  
  --ipam-policy-id ipam-policy-12345678 \  
  --organization-target-id ou-123
```

Important

启用此策略将取代选定账户或组织单元中任何有效的 IPAM 策略。

第 4 步：测试策略

在其中一个目标账户中创建一个所配置类型的新资源（如 EIP）。该资源将自动使用您的 IPAM 池中的 IP 地址。

Important

如果您在创建 AWS 资源时选择了特定的 IPAM 池或 EIP 分配 ID，则该设置将覆盖 IPAM 策略。

第 5 步：监控使用情况

在控制台中检查您的 [IPAM 池](#)，以查看分配给您的资源的 IP 地址。

释放分配

如果您计划删除池，则可能需要释放池分配。分配是从一个 IPAM 池到另一个资源或 IPAM 池的 CIDR 分配。

如果池已预置 CIDR，则无法删除该池；如果 CIDR 已分配给资源，则无法取消预置该 CIDR。

Note

- 要释放手动分配，请使用此部分中的步骤或调用 [ReleaseIpamPoolAllocation API](#)。
- 要在私有范围内释放分配，您必须忽略或删除资源 CIDR。有关更多信息，请参阅 [更改 VPC CIDR 的监控状态](#)。一段时间后，Amazon VPC IPAM 会自动代表您释放分配。

Example

示例

如果您在私有范围内有 VPC CIDR，要释放分配，您必须忽略或删除 VPC CIDR。一段时间后，Amazon VPC IPAM 将自动从 IPAM 池中释放 VPC CIDR 分配。

- 要在公有范围内释放分配，您必须删除资源 CIDR。您不能忽略公有资源 CIDR。有关更多信息，请参阅 [仅使用 AWS CLI 自带公有 IPv4 CIDR 到 IPAM 中](#) 中的清理或 [仅使用 AWS CLI 自带 IPv6 CIDR 到 IPAM 中](#) 中的清理。一段时间后，Amazon VPC IPAM 会自动代表您释放分配。

要让 Amazon VPC IPAM 代表您释放分配，所有账户权限都必须正确配置为[单账户使用](#)或[多账户使用](#)。

当您释放由 IPAM 管理的 CIDR 时，Amazon VPC IPAM 会将 CIDR 回收回 IPAM 池中。如果使用高级套餐的 IPAM，CIDR 可在几分钟时间后用于未来分配。如果使用免费套餐的 IPAM，CIDR 需要 48 小时才能用于未来分配。有关池和分配的更多信息，请参阅[IPAM 的工作原理](#)。

AWS Management Console

要释放池分配

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 从内容窗格顶部的下拉菜单中，选择要使用的范围。有关范围的更多信息，请参阅[IPAM 的工作原理](#)。
4. 在内容窗格中，选择分配所在的池。
5. 选择 Allocations (分配) 选项卡。
6. 选择一个或多个分配。您可以按分配的资源类型来识别分配：
 - 自定义：自定义分配。
 - vpc：VPC 分配。
 - ipam-pool：IPAM 池分配。
 - ec2-public-ipv4-pool：公有 IPv4 池分配。
 - 子网：子网分配。
7. 选择 Actions (操作) > Release custom allocation (释放自定义分配)。
8. 选择 Deallocate CIDR (取消分配 CIDR)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令释放池分配：

1. 获取 IPAM 池 ID : [describe-ipam-pools](#)
2. 查看您在池中的当前分配 : [get-ipam-pool-allocations](#)
3. 释放分配 : [release-ipam-pool-allocation](#)
4. 查看已更新的分配 : [get-ipam-pool-allocations](#)

要添加新分配，请参阅 [从 IPAM 池中分配 CIDR](#)。要在释放分配后删除池，首先必须 [从池中取消预置 CIDR](#)。

使用 AWS RAM 共享 IPAM 池

按照此部分中的步骤适用 AWS Resource Access Manager (RAM) 共享 IPAM 池。当您与 RAM 共享 IPAM 池时，“主体”可以将池中的 CIDR 分配给来自各自账户的 AWS 资源，例如 VPC。主体是 RAM 中的一个概念，表示 AWS Organizations 中的任何 AWS 账户、IAM 角色、IAM 角色或组织部门。有关更多信息，请参阅 AWS RAM 用户指南中的 [使用共享的共享您的 AWS 资源](#)。

Note

- 如果您已将 IPAM 与 AWS Organizations 集成，您只能与 AWS RAM 共享 IPAM 池。有关更多信息，请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)。如果您是单个账户 IPAM 用户，则无法与 AWS RAM 共享 IPAM 池。
- 您必须启用在 AWS RAM 中与 AWS Organizations 共享资源。有关更多信息，请参阅 AWS RAM 用户指南中的 [在 AWS Organizations 内启用资源共享](#)。
- RAM 共享仅在您 IPAM 所在的主 AWS 区域中可用。您必须在 IPAM 所在的 AWS 区域创建共享，而不是在 IPAM 池的区域中。
- 创建和删除 IPAM 池资源共享的账户在附加到其 IAM 角色的 IAM 策略中必须具有以下权限：
 - ec2:PutResourcePolicy
 - ec2>DeleteResourcePolicy
- 您可以向 RAM 共享添加多个 IPAM 池。
- 虽然您可以与 AWS 组织外部的任何 AWS 账户共享 IPAM 池，但只有在账户所有者完成了与委派的 IPAM 管理员共享资源发现的过程后，IPAM 才会监控组织外部账户中的 IP 地址，如 [将 IPAM 与组织外部的账户集成](#) 中所述。

AWS Management Console

要使用 RAM 共享 IPAM 池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，默认的私有范围被选中。如果您不想使用默认的私有范围，请从内容窗格顶部的下拉菜单中选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 在内容窗格中，选择要共享的池，然后选择 Actions (操作) > View details (查看详细信息)。
5. 在 Resource sharing (资源共享) 下，选择 Create resource share (创建资源共享)。因此，AWS RAM 控制台将打开。您将在 AWS RAM 中创建共享池。
6. 选择 Create a Resource Group (创建资源组)。
7. 为共享资源添加 Name (名称)。
8. 在 Select resource type (选择资源类型) 下，选择 IPAM 池并选择一个或多个 IPAM 池。
9. 选择 Next (下一步)。
10. 选择资源共享的权限之一：
 - AWSRAMDefaultPermissionsIpamPool：选择此权限可允许主体查看共享 IPAM 池中的 CIDR 和分配，并在池中分配/释放 CIDR。
 - AWSRAMPermissionIpamPoolByoipCidrImport：选择此权限可允许主体将 BYOIP CIDR 导入共享 IPAM 池中。只有当您具有现有的 BYOIP CIDR 并且想要将它们导入 IPAM 并与主体共享时，才需要此权限。有关 BYOIP CIDR 到 IPAM 的其他信息，请参阅 [教程：将 BYOIP IPv4 CIDR 传输到 IPAM](#)。
11. 选择允许访问此资源的主体。如果主体要将现有的 BYOIP CIDR 导入到此共享 IPAM 池中，请将 BYOIP CIDR 所有者账户添加为主体。
12. 查看资源共享选项和要共享的委托人，然后选择 Create (创建)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。在那里，您可以找到运行命令时可以使用的选项的详细说明。

使用以下 AWS CLI 命令通过 RAM 共享 IPAM 池：

1. 获取 IPAM 的 ARN：[describe-ipam-pools](#)

2. 创建资源共享：[create-resource-share](#)
3. 查看资源共享：[get-resource-shares](#)

由于在 RAM 中创建资源共享，其他主体现在可以使用 IPAM 池将 CIDR 分配给资源。有关监控主体创建的资源的信息，请参阅 [按资源监控 CIDR 使用情况](#)。有关如何从共享 IPAM 池创建 VPC 和分配 CIDR 的更多信息，请参阅《Amazon VPC 用户指南》中的 [创建 VPC](#)。

使用资源发现

资源发现是一个 IPAM 组件，IPAM 可以通过它来管理和监控属于拥有资源发现的账户的资源。这使得 IPAM 能够维持工作负载中 IP 地址使用情况的最新清单，从而便于管理和规划 IP 地址。

默认情况下，创建 IPAM 时会创建资源发现。您也可以独立于 IPAM 创建资源发现，并将其与其他账户或组织所拥有的 IPAM 集成。如果资源发现拥有者是组织的委托管理员，IPAM 会监控该组织所有成员的资源。

Note

创建、共享和关联资源发现是将 IPAM 与组织外部账户集成的过程的一部分（请参阅 [将 IPAM 与组织外部的账户集成](#)）。如果您不想创建 IPAM 并将其与组织外部的账户集成，则无需创建、共享或关联资源发现。

请注意，本部分为一组程序，都与使用资源发现相关。

目录

- [创建资源发现以与其他 IPAM 集成](#)
- [查看资源发现详细信息](#)
- [与其他 AWS 账户共享资源发现](#)
- [将资源发现与 IPAM 关联](#)
- [取消关联资源发现](#)
- [删除资源发现](#)

创建资源发现以与其他 IPAM 集成

本部分介绍如何创建资源发现。默认情况下，创建 IPAM 时会创建资源发现。每个区域资源发现的默认限额为 1。有关 IPAM 限额的更多信息，请参阅 [IPAM 的配额](#)。

Note

创建、共享和关联资源发现是将 IPAM 与组织外部账户集成的过程的一部分（请参阅 [将 IPAM 与组织外部的账户集成](#)）。如果您不想创建 IPAM 并将其与组织外部的账户集成，则无需创建、共享或关联资源发现。

如果您想将 IPAM 与组织外部的账户集成，则此步骤必须由辅助组织管理员账户完成。有关此过程所涉及角色的更多信息，请参阅 [过程概述](#)。

AWS Management Console

创建资源发现

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择资源发现。
3. 选择创建资源发现。
4. 选择允许 Amazon VPC IP 地址管理器将数据从源账户复制到 IPAM 委托账户中。如果未选中此选项，则无法创建资源发现。
5. （可选）向资源发现添加名称标签。标签是为 AWS 资源分配的标记。每个标签都包含一个键和一个可选值。您可以使用标签来搜索和筛选您的资源或跟踪 AWS 成本。
6. （可选）添加描述。
7. 在运营区域下，选择需要发现资源的 AWS 区域。当前区域将自动设置为运营区域之一。如果您正在创建资源发现以便将其与运营区域 us-east-1 中的 IPAM 共享，请确保选择此处的 us-east-1。如果忘记选择运营区域，可以稍后返回并编辑资源发现设置。

Note

大多数情况下，资源发现应与 IPAM 位于同一运营区域，否则您只能在该区域进行资源发现。

8. （可选）为池选择任何其他标签。

9. 选择创建。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

- 创建资源发现：[create-ipam-resource-discovery](#)

查看资源发现详细信息

查看 AWS IPAM 中资源发现的详细信息可以提供有价值的见解，例如：

- 识别已导入的特定 AWS 资源及其关联的 IP 地址分配。
- 监控资源发现过程的状态和进度。
- 对 IPAM 与发现的资源之间的任何问题或差异进行问题排除。
- 分析 IP 地址利用率和趋势。

此信息可以帮助您优化 IP 地址管理，并确保 IPAM 与实际资源部署保持一致。

AWS Management Console

查看资源发现详细信息

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择资源发现。
3. 选择资源发现。
4. 在资源发现详细信息下，查看与资源发现相关的详细信息，例如“默认”，该信息表明资源发现是否为默认设置。默认资源发现是创建 IPAM 时自动创建的资源发现。
5. 在选项卡中，查看资源发现的详细信息：
 - 已发现资源–资源发现所监控的资源。IPAM 会监控以下资源类型 VPC、公有 IPv4 池、VPC 子网和弹性 IP 地址的 CIDR。
 - 名称 (资源 ID) - 资源发现 ID。
 - IP 分配情况 – 正在使用的 IP 地址空间百分比。要将十进制转换为百分比，请将十进制乘以 100。请注意以下几点：

- 对于属于 VPC 的资源，这表示 VPC 中子网 CIDR 所占用 IP 地址空间的百分比。
- 对于属于子网的资源，如果子网预置了 IPv4 CIDR，则表示子网中正在使用的 IPv4 地址空间的百分比。如果子网配置了 IPv6 CIDR，则不表示正在使用的 IPv6 地址空间的百分比。目前无法计算正在使用的 IPv6 地址空间的百分比。
- 对于属于公有 IPv4 池的资源，这表示池中分配给弹性 IP 地址 (EIP) 的 IP 地址空间的百分比。
- CIDR – 资源 CIDR。
- 区域 – 资源区域。
- 拥有者 ID – 资源拥有者 ID。
- 采样时间 – 上次成功发现资源的时间。
- 已发现账户：资源发现所监控的 AWS 账户。如果 IPAM 已与 AWS Organizations 集成，则组织中的所有账户均为已发现账户。
- 账户 ID – 账户 ID。
- 区域 – 从中返回账户信息的 AWS 区域。
- 上次尝试发现时间 – 上次尝试发现资源的时间。
- 上次成功发现时间 – 上次成功发现资源的时间。
- 状态 – 资源发现失败的原因。
- 运营区域 – 资源发现的运营区域。
- 资源共享 – 如已共享资源发现，则会列出资源共享 ARN。
- 资源共享 ARN – 资源共享 ARN。
- 状态 – 资源共享的当前状态。可能的值有：
 - 活动 – 资源共享处于活动状态并且可供使用。
 - 已删除 – 资源共享已删除并且不再可用。
 - 待处理 – 资源共享接受邀请正在等待响应。
- 创建时间 – 资源共享的创建时间。
- 标签 – 标签是您为 AWS 资源分配的标记。每一个标签都包含一个键和一个可选值。您可以使用标签来搜索和筛选您的资源或跟踪 AWS 成本。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

[查看资源发现详细信息](#)

- 查看资源发现详细信息：[describe-ipam-resource-discoveries](#)

与其他 AWS 账户共享资源发现

按照本部分中的步骤使用 AWS Resource Access Manager 共享资源发现。有关 AWS RAM 的更多信息，请参阅《AWS RAM 用户指南》中的[共享 AWS 资源](#)。

Note

创建、共享和关联资源发现是将 IPAM 与组织外部账户集成的过程的一部分（请参阅[将 IPAM 与组织外部的账户集成](#)）。如果您不想创建 IPAM 并将其与组织外部的账户集成，则无需创建、共享或关联资源发现。

创建用于监控组织外部账户的 IPAM 时，辅助组织管理员账户将使用 AWS RAM 与主组织 IPAM 账户共享其资源发现。您必须先与主组织 IPAM 账户共享资源发现，主组织 IPAM 账户才能将资源发现与其 IPAM 相关联。有关此过程所涉及角色的更多信息，请参阅[过程概述](#)。

Note

- 使用 AWS RAM 创建资源共享以共享资源发现时，您必须在主组织 IPAM 的主区域中创建资源共享。
- 要创建和删除用于资源发现的资源共享，账户的 IAM 策略中必须具有以下权限：
 - ec2:PutResourcePolicy
 - ec2>DeleteResourcePolicy
- 如果您与其他账户共享资源发现，则该账户可以看到其上的任何[OU 排除项](#)，其中包含资源发现所有者组织的组织 ID、根 ID 和组织单位 ID 等信息。

如果您想将 IPAM 与组织外部的账户集成，则此步骤必须由辅助组织管理员账户完成。

AWS Management Console

共享资源发现

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择资源发现。

3. 选择资源共享选项卡。
4. 选择创建资源共享。AWS RAM 控制台随即打开，您可以在其中创建资源共享。
5. 在 AWS RAM 控制台中，选择设置。
6. 选择允许与 AWS Organizations 共享，然后选择保存设置。
7. 选择创建资源共享。
8. 为共享资源添加名称。
9. 在选择资源类型下，选择 IPAM 资源发现，然后选择相应的资源发现。
10. 选择下一步。
11. 在关联权限下，您可以查看将为被授予此资源共享访问权限的主体启用的默认权限：
 - AWSRAMPermissionIpamResourceDiscovery
 - 此权限允许以下操作：
 - ec2:AssociateIpamResourceDiscovery
 - ec2:GetIpamDiscoveredAccounts
 - ec2:GetIpamDiscoveredPublicAddresses
 - ec2:GetIpamDiscoveredResourceCidrs
12. 指定允许访问共享资源的主体。对于主体，请选择主组织 IPAM 账户，然后选择添加。
13. 选择下一步。
14. 查看资源共享选项和要共享的主体。然后选择创建资源共享。
15. 资源发现共享后，主组织 IPAM 账户必须接受，然后将其与 IPAM 关联。有关更多信息，请参阅 [将资源发现与 IPAM 关联](#)。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

1. 创建资源共享：[create-resource-share](#)
2. 查看资源共享：[get-resource-shares](#)

将资源发现与 IPAM 关联

本部分介绍如何将资源发现与 IPAM 关联。将资源发现与 IPAM 关联后，IPAM 会监控资源发现所发现的所有资源 CIDR 和账户。创建 IPAM 时，系统会为 IPAM 创建默认资源发现并自动将其与 IPAM 关联。

资源发现关联的默认限额为 5。有关更多信息（包括如何调整限额），请参阅 [IPAM 的配额](#)。

Note

创建、共享和关联资源发现是将 IPAM 与组织外部账户集成的过程的一部分（请参阅 [将 IPAM 与组织外部的账户集成](#)）。如果您不想创建 IPAM 并将其与组织外部的账户集成，则无需创建、共享或关联资源发现。

如果您想将 IPAM 与组织外部的账户集成，则此步骤必须由主组织 IPAM 账户完成。有关此过程所涉及角色的更多信息，请参阅 [过程概述](#)。

AWS Management Console

关联资源发现

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 IPAM。
3. 选择关联发现，然后选择关联资源发现。
4. 在 IPAM 资源发现下，选择辅助组织管理员账户与您共享的资源发现。
5. 选择关联。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

- 关联资源发现：[associate-ipam-resource-discovery](#)

取消关联资源发现

本部分介绍如何将资源发现与 IPAM 取消关联。将资源发现与 IPAM 取消关联后，IPAM 不会再监控资源发现所发现的所有资源 CIDR 和账户。

Note

无法取消关联默认资源发现。默认资源发现关联是创建 IPAM 时自动创建的关联。但是，删除 IPAM 也将一并删除默认资源发现关联。

此步骤必须由主组织 IPAM 账户完成。有关此过程所涉及角色的更多信息，请参阅 [过程概述](#)。

AWS Management Console

取消关联资源发现

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 IPAM。
3. 选择关联发现，然后选择取消关联资源发现。
4. 在 IPAM 资源发现下，选择辅助组织管理员账户与您共享的资源发现。
5. 选择取消关联。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

- 取消关联资源发现：[disassociate-ipam-resource-discovery](#)

删除资源发现

本部分介绍如何删除资源发现。

Note

无法删除默认资源发现。默认资源发现是创建 IPAM 时自动创建的资源发现。但是，删除 IPAM 也将一并删除默认资源发现。

此步骤必须由辅助组织管理员账户完成。有关此过程所涉及角色的更多信息，请参阅 [过程概述](#)。

AWS Management Console

删除资源发现

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择资源发现。
3. 选择资源发现，然后选择操作>删除资源发现。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

- 删除资源发现：[delete-ipam-resource-discovery](#)

跟踪 IPAM 中的 IP 地址使用情况

Amazon VPC IP 地址管理器提供 IP 地址使用情况跟踪功能，可为任何管理复杂网络环境的人带来益处。IPAM 跨 AWS 提供对 IP 地址分配、利用率和使用趋势的可见性。这可以帮助您识别未使用或使用效率低下的 IP 地址，优化地址空间并防止发生潜在的 IP 地址耗尽。

IPAM 在 CIDR、范围和 IPAM 级别方面跟踪 IP 地址的使用情况，提供详细的报告和分析。这对于大规模部署、多账户设置和不断变化的网络要求非常有价值。

通过利用 IPAM 的使用情况跟踪，您可以作出明智的决策、改进 IP 地址管理，并确保 IP 资源的有效利用。

Note

此部分中所述的任务是可选的。如果您想完成此部分中的任务，并且已委派了 IPAM 账户，则应该由 IPAM 账户完成这些任务。

内容

- [使用 IPAM 控制面板监控 CIDR 使用情况](#)
- [按资源监控 CIDR 使用情况](#)
- [使用 Amazon CloudWatch 监控 IPAM](#)
- [查看 IP 地址历史记录](#)
- [查看公有 IP 见解](#)

使用 IPAM 控制面板监控 CIDR 使用情况

Amazon VPC IP 地址管理器中的 IPAM 控制面板可使您监控多种关键场景的 CIDR 使用情况：

- 识别未使用或未充分利用的 IP 地址空间：控制面板提供了 CIDR 利用率的可视性，使您能够识别具有可回收或重新分配的可用容量的 CIDR。
- 优化 IP 地址管理：通过密切跟踪 CIDR 的使用情况，您可以就扩展、收缩或重新分配 IP 地址块做出明智的决定，以满足不断变化的业务和基础设施需求。
- 防止 IP 地址耗尽：监控 CIDR 使用情况可帮助您预测何时可能需要获取额外的 IP 地址空间，让您能够主动规划并避免因 IP 地址耗尽而导致的服务中断。

- 确保合规性和治理能力：IPAM 控制面板可以帮助您演示 IP 地址使用模式，以满足围绕 IP 地址管理的监管要求或内部政策。
- 解决网络问题：详细的 CIDR 使用数据可以帮助识别网络连接问题或资源冲突的根本原因。

通过 IPAM 控制面板密切监控 CIDR 的使用情况，您可以提高 AWS 内部 IP 地址管理的效率、弹性和合规性。

AWS Management Console

使用 IPAM 控制面板监控 CIDR 使用情况

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择控制面板。
3. 默认情况下，当您查看控制面板时，默认的私有范围被选中。如果您不想使用默认的私有范围，请从内容窗格顶部的下拉菜单中选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 控制面板提供了某个范围内的 IPAM 池和 CIDR 的总览。您可以添加、移除、移动小组件以及调整大小，从而自定义控制面板。
 - Scope (范围)：此范围的详细信息。范围是 IPAM 中最高级别的容器。IPAM 包含两个默认范围，一个为私有范围，另一个为公有范围。每个范围代表单个网络的 IP 空间。您可以包含多个私有范围，但只能有一个公有范围。
 - Scope ID (范围 ID)：此范围的 ID。
 - Scope type (范围类型)：范围的类型。
 - IPAM ID：范围所在的 IPAM 的 ID。
 - 此范围中的 IPAM 池：范围所在的 IPAM 的 ID。
 - 查看此范围中的网络资源：您将进入 IPAM 控制台的资源部分。
 - 搜索此范围中的 IP 地址历史记录：您将进入 IPAM 控制台的搜索 IP 历史记录部分。
 - 资源 CIDR 类型：范围中的资源 CIDR 类型。
 - 子网：子网的 CIDR 数量。
 - VPC：VPC 的 CIDR 数量。
 - EIP：弹性 IP 地址的 CIDR 数量。
 - 公有 IPv4 池：公有 IPv4 池的 CIDR 数量。
 - 管理状态：CIDR 的管理状态。

- Unmanaged CIDRs (非托管 CIDR) : 此范围内非托管资源的资源 CIDR 数量。
- Ignored CIDRs (忽略的 CIDR) : 您选择的免于使用范围中的 IPAM 监控的资源 CIDR 数量。IPAM 不会评估范围内被忽略资源的重叠或合规性。选择忽略资源时, 从 IPAM 池中分配给它的任何空间都将返回到池中, 并且不会通过自动导入再次导入该资源 (如果在池中设置了自动导入分配规则) 。
- Managed CIDRs (托管 CIDR) : 从范围内的 IPAM 池分配的可管理资源 (VPC 或公有 IPv4 池) 的资源 CIDR 数量。
- 重叠的资源 CIDR : 重叠和不重叠的 CIDR 数量。重叠的 CIDR 可能会导致 VPC 中的路由不正确。
 - Overlapping CIDRs (重叠 CIDR) : 在此范围中的 IPAM 池内重叠的 CIDR 的数量。重叠的 CIDR 可能会导致 VPC 中的路由不正确。
 - 不重叠的 CIDR : 此范围中的 IPAM 池内不重叠的资源 CIDR 数量。
- 合规的资源 CIDR : 合规的资源 CIDR 数量。
 - Compliant CIDRs (合规的 CIDR) : 符合范围内 IPAM 池分配规则的资源 CIDR 数量。
 - Noncompliant CIDRs (不合规的 CIDR) : 不符合范围内 IPAM 池分配规则的资源 CIDR 数量。
- 重叠状态 : 随着时间推移重叠的 CIDR 数量。
 - 重叠的 CIDR : 此范围中的 IPAM 池内重叠的 CIDR 数量。重叠的 CIDR 可能会导致 VPC 中的路由不正确。
- 合规状态 : 随着时间推移符合以及不符合范围中 IPAM 池的分配规则的 CIDR 数量。
 - 合规的资源 CIDR : 符合分配规则的资源 CIDR 数量。
 - 不合规的资源 CIDR : 不符合分配规则的资源 CIDR 数量。
- VPC 利用率 : IP 利用率最高或最低的 VPC (IPv4 和 IPv6) 。您可以使用此信息配置 Amazon CloudWatch 告警, 以便在 IP 利用率阈值被突破时发出警报。有关更多信息, 请参阅 [IPAM 资源利用率指标](#)。
- 子网利用率 : IP 利用率最高或最低的子网 (仅限 IPv4) 。您可以使用这些信息来决定是保留还是删除未充分利用的资源。有关更多信息, 请参阅 [IPAM 资源利用率指标](#)。
- IP 分配比例最高的 VPC : 分配给子网的 IP 地址空间百分比最高的 VPC。借助此指标可以方便地了解是否需要为 VPC 预调配额外的 IP 地址空间。
- IP 分配比例最高的子网 : 分配给资源的 IP 地址空间百分比最高的子网。借助此指标可以方便地了解是否需要为子网预调配额外的 IP 地址空间。
- 池指定 : 随着时间推移在范围内指定给资源和手动分配的 IP 空间百分比。

- 池分配：随着时间推移分配给范围中其他池的池 IP 空间百分比。

Command line

控制面板中显示的信息来自 Amazon CloudWatch 中存储的指标。有关存储在 Amazon CloudWatch 中的指标的更多信息，请参阅 [使用 Amazon CloudWatch 监控 IPAM](#)。使用 [AWS CLI 参考](#)中的 Amazon CloudWatch 选项查看 IPAM 池和范围中的分配指标。

如果您发现为池预置的 CIDR 几乎已完全分配，则可能需要预置额外的 CIDR。有关更多信息，请参阅 [将 CIDR 预置到池](#)。

按资源监控 CIDR 使用情况

Amazon VPC IP 地址管理器中的资源视图可集中概述您的 AWS 资源中 IP 地址的使用情况。这使您能够快速识别哪些资源正在消耗 IP 地址，跟踪地址分配趋势，并优化 IP 地址管理，以适应不断变化的基础设施和业务需求。

在 IPAM 中，资源是分配 IP 地址或 CIDR 块的 AWS 服务实体。IPAM 管理一些资源，但只监控另一些资源，因此了解两者之间的区别很重要：

- 托管资源：托管资源具有从 IPAM 池中分配的 CIDR。IPAM 监控 CIDR 是否可能与池中其他 CIDR 的 IP 地址重叠，并监控 CIDR 是否符合池的分配规则。IPAM 支持管理以下类型的资源：
 - 弹性 IP 地址
 - 公有 IPv4 池

Note

公有 IPv4 池和 IPAM 池由 AWS 中的不同资源管理。公共 IPv4 池是单一账户资源，使您能够将公有 CIDR 转换为弹性 IP 地址。IPAM 池可用于将公有空间分配给公有 IPv4 池。

- VPC
- 监控资源：如果某个资源被 IPAM 监控，则 IPAM 已检测到该资源，您可以在将 `get-ipam-resource-cidrs` 与 AWS CLI 结合使用时或在导航窗格中查看 Resources (资源) 时查看有关资源 CIDR 的详细信息。IPAM 支持监控以下资源：
 - 弹性 IP 地址
 - 公有 IPv4 池

- VPC
- VPC 子网

AWS Management Console

按资源监控 CIDR 使用情况

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Resources (资源)。
3. 从内容窗格顶部的 IP 下拉菜单中，选择要使用的 IP 地址协议：IPv4 或 IPv6。
4. 从内容窗格顶部的范围下拉菜单中，选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
5. 使用资源 CIDR 映射来查看范围内可用、已分配和重叠的 IP 地址空间：
 - 可用：IP 地址范围可供分配。
 - 合规且不重叠：IP 地址范围已分配给由 IPAM 管理的资源。
 - 占用：IP 地址范围已分配给资源。
 - 重叠：IP 地址范围已分配给多个资源且有重叠。
 - 不合规：IP 地址范围不合规。某个使用 IP 地址范围的资源不符合为该池设置的分配规则。

在 CIDR 映射中，选择位于映射底部的 IP 地址块，来查看较小 CIDR 块中的资源。选择位于映射顶部的 IP 地址块，来查看较大 CIDR 块中的资源。

6. 在此表中，您可以查看有关该范围内的资源的以下详细信息：
 - 名称 (资源 ID)：资源的名称和资源 ID。
 - CIDR：与资源关联的 CIDR。
 - Management state (管理状态)：资源的状态。
 - Managed (托管)：该资源具有从 IPAM 池中分配的 CIDR，IPAM 正在监控该资源是否可能与 CIDR 重叠以及是否符合池分配规则。
 - Unmanaged (非托管)：该资源不具有从 IPAM 池中分配的 CIDR，IPAM 正在监控该资源是否可能存在符合池分配规则的 CIDR。对 CIDR 进行重叠监控。
 - 已忽略：已选择该资源免于监控。不会评估忽略的资源是否存在重叠或分配规则合规性。选择忽略资源时，从 IPAM 池中分配给它的任何空间都将返回到池中，并且不会通过自动导入再次导入该资源 (如果在池中设置了自动导入分配规则)。

- -：此资源不是 IPAM 可以管理的资源类型之一。
- Compliance status (合规性状态)：CIDR 的合规性状态。
- Compliant (合规)：托管资源符合 IPAM 池的分配规则。
- Noncompliant (不合规)：资源 CIDR 不符合 IPAM 池的一个或多个分配规则。

Example

如果 VPC 的 CIDR 不符合 IPAM 池的网络掩码长度参数，或者资源与 IPAM 池不在同一个 AWS 区域中，它将被标记为不合规。

- Unmanaged (非托管)：该资源不具有从 IPAM 池中分配的 CIDR，IPAM 正在监控该资源是否可能存在符合池分配规则的 CIDR。对 CIDR 进行重叠监控。
- 已忽略：已选择该资源免于监控。不会评估忽略的资源是否存在重叠或分配规则合规性。选择忽略资源时，从 IPAM 池中分配给它的任何空间都将返回到池中，并且不会通过自动导入再次导入该资源（如果在池中设置了自动导入分配规则）。
- -：此资源不是 IPAM 可以管理的资源类型之一。
- Overlap status (重叠状态)：CIDR 的重叠状态。
- Nonoverlapping (不重叠)：资源 CIDR 与同一范围内的另一个 CIDR 不重叠。
- Overlapping (重叠)：资源 CIDR 与同一范围内的另一个 CIDR 重叠。请注意，如果资源 CIDR 重叠，则可能与手动分配重叠。
- 已忽略：已选择该资源免于监控。IPAM 不会评估被忽略资源的重叠或分配规则合规性。选择忽略资源时，从 IPAM 池中分配给它的任何空间都将返回到池中，并且不会通过自动导入再次导入该资源（如果在池中设置了自动导入分配规则）。
- -：此资源不是 IPAM 可以管理的资源类型之一。
- IP 分配情况：对于属于 VPC 的资源，表示 VPC 中子网 CIDR 占用的 IP 地址空间的百分比。对于属于子网的资源，如果子网预置了 IPv4 CIDR，则表示子网中正在使用的 IPv4 地址空间的百分比。如果子网配置了 IPv6 CIDR，则不表示正在使用的 IPv6 地址空间的百分比。目前无法计算正在使用的 IPv6 地址空间的百分比。对于属于公有 IPv4 池的资源，这表示池中分配给弹性 IP 地址 (EIP) 的 IP 地址空间的百分比。
- Region (区域)：资源的 AWS 区域。
- Owner ID (拥有者 ID)：创建此资源的人员的 AWS 账户 ID。
- 资源类型：无论资源是 VPC、子网、弹性 IP 地址还是公有 IPv4 池。
- Pool ID (池 ID)：资源所在的 IPAM 池的 ID。

7. 使用筛选资源按列属性 (例如，VPC ID 或合规性状态) 筛选资源表。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

请使用以下 AWS CLI 命令按资源监控 CIDR 使用情况：

1. 获取范围 ID：[describe-ipam-scopes](#)
2. 请求资源信息：[get-ipam-resource-cidrs](#)

使用 Amazon CloudWatch 监控 IPAM

IPAM 会自动在您 IPAM 所在主区域的 AWS/IPAM [Amazon CloudWatch 命名空间](#) 中存储与 IP 地址使用情况（例如，IPAM 池中可用的 IP 地址空间以及符合分配规则的资源 CIDR 数量）和资源利用率相关的指标。

将 IPAM 与 CloudWatch 集成可增强您监控、分析和优化 AWS 内的 IP 地址管理的能力。

使用案例包括：

- 跟踪 IP 地址利用率趋势：CloudWatch 可以监控 CIDR 池使用情况、范围分配和其他 IPAM 指标，以帮助您主动识别潜在的 IP 地址耗尽风险。
- 设置基于利用率的警报：您可以配置 CloudWatch 警报，使其在 CIDR 利用率达到预定阈值时通知您，从而实现及时干预和优化。
- 监控 IPAM 事件：CloudWatch 可以捕获和分析与 IPAM 相关的事件，例如 CIDR 分配、取消分配和范围修改，从而提供对 IP 地址管理活动的可见性。
- 生成自定义控制面板：通过将 IPAM 数据与其他 AWS 指标相结合，您可以创建全面的控制面板，以可视化和分析您的 IP 地址场景以及相关的基础设施和性能指标。

目录

- [通过 IPAM 控制台管理警报](#)
- [IPAM 指标](#)
- [IPAM 资源利用率指标](#)

通过 IPAM 控制台管理警报

您可以直接从 IPAM 控制台创建和管理 Amazon CloudWatch 警报。处于 INSUFFICIENT_DATA 或 ALARM 状态的 [IPAM 指标](#) 或 [IPAM 资源利用率指标](#) 警报将在控制台顶部显示为警告栏，并在监控旁边的左侧导航栏中显示为视觉指示器。

要管理特定资源的警报，请选择资源，然后选择 VPC、子网或池。资源详细信息页面打开后，选择警报选项卡。

警报选项卡显示与所选资源关联的所有 CloudWatch 警报。在此选项卡中，您可以查看警报详细信息、监控当前状态和访问警报配置选项。该选项卡显示 AWS/IPAM 命名空间中与您正在查看的资源相关的警报。

以下屏幕截图展示了 IPAM 控制台中的警报管理界面：

The screenshot displays the Amazon VPC IP Address Manager console. On the left is a navigation sidebar with sections for Monitoring (43 alerts, 25 OK, 14 pending), Planning, and Announcements (1). The main area shows the 'subnet-0' resource page with tabs for CIDRs, Monitoring, Compliancy, ENIs, Alarms (selected), and Tags. The 'Summary' section lists: Subnet ID (subnet-0), Scope ID (ipam-scope-0), IPAM ID (ipam-0), Region (us-west-1), Availability zone ID (usw1-az1), and VPC ID (vpc-0). The 'Alarms (1)' section shows a table with one alarm named 'nowalarm' in an 'ALARM' state, monitoring the 'SubnetIPUsage' metric for resource 'subnet-0'. The last update was on 7/23/2025 at 1:32:05 PM, and actions are enabled.

警报选项卡提供了 IPAM 所在区域的 Amazon CloudWatch 命名空间中的 AWS/IPAM CloudWatch 警报的详细摘要：

- 警报名称：CloudWatch 警报的用户定义名称。
- 状态：CloudWatch 警报的当前状态：
 - 警报：指标在规定的阈值范围外。
 - 正常：指标在规定的阈值范围内。
 - INSUFFICIENT_DATA：数据不足，无法确定警报状态。
- 指标：警报正在监控的特定 CloudWatch 指标。
- 资源 ID：警报正在监控的 AWS 资源的唯一标识符。

- 上次更新时间：上次更改或评估警报状态的日期和时间。
- 已启用操作：表示是否为警报启用 CloudWatch 操作：
 - 是：满足条件时，警报可以触发配置的操作。
 - 否：警报正在监控，但不执行操作。

此外，如果您在监控选项卡上查看 VPC、子网或池的利用率图表，则可以选择为资源利用率创建警报的选项。然后，您将被重定向到 CloudWatch 控制台，其中预先填充了资源和指标详细信息。您可以在配置警报阈值，例如在利用率达到特定百分比时收到通知。

IPAM 指标

IPAM 会将有关您的 IPAM、池和范围的数据发布到 Amazon CloudWatch。您可以使用这些指标为 IPAM 池创建告警，以通知您地址池是否即将耗尽，或者资源是否未能遵守池上设置的分配规则。使用 Amazon CloudWatch 创建告警和设置通知不在本节的范围内。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的[使用 Amazon CloudWatch 警报](#)。

下面列出了 IPAM 发送到 Amazon CloudWatch 的指标和维度。

IPAM 指标

AWS/IPAM 命名空间包括以下 IPAM 指标。

指标名称	描述
TotalActiveIpCount	<p>总活跃 IP 数是如果您从免费套餐切换到高级套餐则您的 IPAM 中需要向您收费的活跃 IP 地址数量。活动 IP 地址定义为与附加到 EC2 实例等资源的弹性网络接口 (ENI) 关联的 IP 地址或前缀。</p> <ul style="list-style-type: none"> • 此指标仅适用于免费套餐的客户。 • 如果您的 IPAM 与 AWS Organizations 集成，则活动 IP 计数将涵盖所有组织账户。 • 您无法按 IP 类型 (公有/私有) 或类别 (IPv4/IPv6) 查看活动 IP 数的明细。 • IPAM 仅计入受监控账户拥有的 ENI 的 IP。共享子网的计数可能不准确。如果子网所有者或 ENI 所有者不在 IPAM 覆盖范围内，则不包括其 IP 地址。

IPAM 池指标

AWS/IPAM 命名空间包括 IPAM 的以下池指标。

指标名称	描述
CompliantResourceCidrs	符合 IPAM 池分配规则的托管式资源 CIDR 数量。有关分配规则的更多信息，请参阅 创建顶级 IPv4 池 。
NoncompliantResourceCidrs	不符合 IPAM 池分配规则的托管式资源 CIDR 数量。有关分配规则的更多信息，请参阅 创建顶级 IPv4 池 。
PercentAllocated	已分配给其他池的池 IP 空间的百分比。
PercentAssigned	已分配给资源（包括手动分配）的池 IP 空间的百分比。
PercentAvailable	尚未分配给其他池或资源的池 IP 空间的百分比。

IPAM 范围指标

AWS/IPAM 命名空间包括 IPAM 的以下范围指标。

指标名称	描述
CompliantResourceCidrs	符合范围内 IPAM 池分配规则的资源 CIDR 数量。
ManagedResourceCidrs	从范围内的 IPAM 池分配的可管理资源（VPC 或公有 IPv4 池）的资源 CIDR 数量。
NoncompliantResourceCidrs	不符合范围内 IPAM 池分配规则的资源 CIDR 数量。
OverlappingResourceCidrs	范围重叠的资源 CIDR 的数量。
UnmanagedResourceCidrs	范围内当前与可管理资源关联但未由 IPAM 管理的资源 CIDR 的数量。

IPAM 公有 IP 指标

AWS/IPAM 命名空间包括 IPAM 的以下公有 IP 指标。

指标名称	描述
AmazonOwnedContigIPs	预调配给 IPAM 拥有的 Amazon 提供的连续公有 IPv4 池的 CIDR 中的 IP 地址数量。
AllocatedAmazonOwnedContigIPs	从 Amazon 提供的连续公有 IPv4 池 CIDR 块中分配的 IP 地址数量。
UnallocatedAmazonOwnedContigIPs	IPAM 拥有的 Amazon 提供的连续公有 IPv4 池的 CIDR 块中的 IP 地址数量。
AssociatedAmazonOwnedContigIPs	从 Amazon 提供的连续公有 IPv4 池 CIDR 块中分配的与弹性网络接口相关的弹性 IP 地址数量。
UnassociatedAmazonOwnedContigIPs	从 Amazon 提供的连续公有 IPv4 池 CIDR 块中分配的与弹性网络接口不相关的弹性 IP 地址数量。

IPAM 前缀列表解析器指标

建议您针对故障指标设置 CloudWatch 警报，因为您可能需要重新评估和调整 [IPAM 前缀列表解析器规则](#)，以保持在本版本和前缀列表大小的限制范围内。

指标名称	描述
IpamPrefixListResolverSyncFailure	前缀列表解析器与目标同步失败。如果超过“每个前缀列表解析器版本的 CIDR 条目数”等配额、找不到目标前缀列表或目标托管前缀列表上的同步被禁用，则可能会发生这种情况。
IpamPrefixListResolverSyncSuccess	前缀列表解析器已成功与目标同步。
IpamPrefixListResolverVersionCreationSuccess	版本创建成功。
IpamPrefixListResolverVersionCreationFailure	版本创建失败。如果已达到“每个前缀列表解析器版本的 CIDR 条目数”配额，则可能会发生这种情况。

指标维度

要筛选 IPAM 指标，请使用以下维度。

维度	描述
AddressFamily	资源 CIDR (IPv4 或 IPv6) 的 IP 地址系列。
Locale	IPAM 池可用于分配的 AWS 区域。
PoolID	池的 ID。
ScopeID	范围的 ID。

有关使用 Amazon CloudWatch 监控 VPC 的信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的 [VPC 的 CloudWatch 指标](#)。

IPAM 资源利用率指标

IPAM 会将 IPAM 监控的资源的 IP 利用率指标发布到 Amazon CloudWatch。这些资源包括：

- VPC (IPv4 和 IPv6)
- 子网 (IPv4)
- 公有 IPv4 池

IPAM 按 IP 地址系列 (IPv4 或 IPv6) 分别计算和发布 IP 利用率指标。资源的 IP 利用率是针对同一地址系列的所有 CIDR 进行计算的。

对于每种资源类型和地址系列组合，IPAM 使用三条规则来确定要发布的指标：

- 多达 50 个具有最高 IP 利用率的资源。您可以使用此信息配置警报，以便在 IP 利用率阈值被突破时发出警报。
- 多达 50 个具有最低 IP 利用率的资源。您可以使用这些信息来决定是保留还是删除未充分利用的资源。
- 多达 50 个其他资源。您可以使用此信息来一致地跟踪可能未在高利用率组或低利用率组中捕获的资源的 IP 利用率。
 - 最多 50 个包含从 IPAM 池分配的 CIDR 的 VPC (按 CIDR 块的总大小划分优先级)。

- 最多 50 个其 VPC 包含从 IPAM 池分配的 CIDR 的子网（按 CIDR 块的总大小划分优先级）。
- 最多 50 个包含从 IPAM 池分配的 CIDR 的公有 IPv4 池（按 CIDR 块的总大小划分优先级）。

在应用每个规则之后，指标会聚合并在每种资源类型的相同指标名称下发布。有关指标名称及其维度的详细信息，请参见下文。

Important

每个资源类型、地址系列和规则组合都有一个唯一限制。每个限制的默认值为 50。您可以通过联系 AWS 支持中心来调整这些限制，如《AWS 一般参考》中的 [AWS 服务配额](#) 所述。

Example 示例

假设您的 IPAM 监控 2,500 个 VPN 和 10,000 个子网，所有这些都具有 IPv4 和 IPv6 CIDR。IPAM 发布以下 IP 利用率指标：

- 最多 150 个 VPC IPv4 IP 利用率，包括：
 - IPv4 IP 利用率最高的 50 个 VPC
 - IPv4 利用率最低的 50 个 VPC
 - 最多 50 个包含从 IPAM 池分配的 IPv4 CIDR 的 VPC
- 最多 150 个 VPC IPv6 IP 利用率，包括：
 - IPv6 IP 利用率最高的 50 个 VPC
 - IPv6 利用率最低的 50 个 VPC
 - 最多 50 个包含从 IPAM 池分配的 IPv6 CIDR 的 VPC
- 最多 150 个子网 IPv4 利用率指标，包括：
 - IPv4 IP 利用率最高的 50 个子网
 - IPv4 IP 利用率最低的 50 个子网
 - 最多 50 个其 VPC 包含从 IPAM 池分配的 IPv4 CIDR 的子网

VPC 指标

下面列出了 VPC 指标名称和描述。

指标名称	描述
VpcIPUsage	VPC 子网中 CIDR 涵盖的 IP 总数除以 VPC 中 CIDR 涵盖的 IP 总数。这是针对相同 IPAM 范围内的所有 VPC CIDR 计算的，并分别针对 IPv4 和 IPv6 CIDR 计算。

下面列出了可用于筛选 VPC 指标的维度。

维度	描述
AddressFamily	资源 CIDR (IPv4 或 IPv6) 的 IP 地址系列。
OwnerID	VPC 所有者的 ID。
Region	VPC 所在的 AWS 区域。
ScopeID	VPC 所属的 IPAM 范围的 ID。
VpcID	VPC 的 ID。

子网指标

下面列出了子网指标名称和描述。

指标名称	描述
SubnetIPUsage	活跃 IP 的数量除以子网 IPv4 CIDR 中的 IP 总数。

下面列出了可用于筛选子网指标的维度。

维度	描述
AddressFamily	资源 CIDR (仅限 IPv4) 的 IP 地址系列。
OwnerID	子网所有者的 ID。

维度	描述
Region	子网所在的 AWS 区域。
ScopeID	子网所属的 IPAM 范围的 ID。
SubnetID	子网的 ID。
VpcID	子网所属的 VPC 的 ID。

公有 IPv4 池指标

下面列出了公有 IPv4 池指标名称和描述。

指标名称	描述
PublicIPv4PoolIPUsage	来自公有 IPv4 池的 EIP 数量除以池中的 IP 总数。

下面列出了可用于筛选公有 IPv4 池指标的维度。

维度	描述
OwnerID	公有 IPv4 池所有者的 ID。
PublicIPv4PoolID	公有 IPv4 池的 ID。
Region	公有 IPv4 池所在的 AWS 区域。
ScopeID	公有 IPv4 池所属的 IPAM 范围的 ID。

公有 IP 洞察指标

下面列出了[公共 IP 洞察功能](#)指标的名称和描述。

指标名称	描述
AmazonOwnedElasticIPs	您已为您的 AWS 账户中的资源预配置或分配的 Amazon 拥有的弹性 IP 地址的数量。
AssociatedAmazonOwnedElasticIPs	您已将您的 AWS 账户中的资源与之关联的 Amazon 拥有的弹性 IP 地址的数量。
AssociatedBringYourOwnIPs	您使用自带 IP 地址 (BYOIP) 带到 AWS, 并与您的 AWS 账户中的资源关联的公有 IPv4 地址的数量。
BringYourOwnIPs	您使用自带 IP 地址 (BYOIP) 带到 AWS 的公有 IPv4 地址的数量。
EC2PublicIPs	当实例启动到默认子网或配置为自动分配公有 IPv4 地址的子网时, 分配给 EC2 实例的公有 IPv4 地址的数量。
ServiceManagedBringYourOwnIPs	您使用 AWS 服务预配置和管理的自带 IP 地址 (BYOIP) 带到 AWS 的公有 IPv4 地址的数量。
ServiceManagedIPs	由 AWS 服务预配置和管理的公有 IPv4 地址的数量。
UnassociatedAmazonOwnedElasticIPs	您尚未将您的 AWS 账户中的资源与之关联的 Amazon 拥有的弹性 IP 地址的数量。
UnassociatedBringYourOwnIPs	您使用自带 IP 地址 (BYOIP) 带到 AWS, 但尚未将其与您的 AWS 账户中的任何资源关联的公有 IPv4 地址的数量。

下面列出了可用于筛选公共 IP 洞察指标的维度。

维度	描述
IpamId	IP 地址所属的 IPAM 的 ID。
Region	公有 IP 地址所在的 AWS 区域。

创建警报的快速提示

要为 IP 地址利用率高的资源快速创建 Amazon CloudWatch 警报，请打开 CloudWatch 控制台，选择指标、所有指标，选择查询选项卡，选择命名空间 AWS/IPAM > VPC IP Usage Metrics、AWS/IPAM > Subnet IP Usage Metrics 或 AWS/IPAM > Public IPv4 Pool IP Usage Metrics，选择指标名称 MAX(VpcIPUsage)、MAX(SubnetIPUsage) 或 MAX(PublicIPv4PoolIPUsage)，然后选择创建告警。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的 [为 Metrics Insights 查询创建告警](#)。

查看 IP 地址历史记录

按照本部分中的步骤查看 IPAM 范围内 IP 地址或 CIDR 的历史记录。您可以使用历史数据来分析和审核网络安全和路由策略。IPAM 会自动将 IP 地址监控数据保留长达三年。

您可以使用 IP 历史数据搜索以下类型资源的 IP 地址或 CIDR 的状态更改：

- VPC
- VPC 子网
- 弹性 IP 地址
- EC2 实例
- 连接到实例的 EC2 网络接口

Important

尽管 IPAM 不会监控 Amazon EC2 实例或挂载到实例的 EC2 网络接口，但您可以使用搜索 IP 历史记录功能，来搜索 EC2 实例和网络接口 CIDR 上的历史数据。

Note

- 如果将资源从一个 IPAM 范围移动到另一个范围，之前的历史记录将结束，并会在新范围下创建新的历史记录。有关更多信息，请参阅 [在范围之间移动 VPC CIDR](#)。
- 如果您删除资源或将资源转移到不受 IPAM 监控的 AWS 账户，则与该资源相关的任何新历史记录都将不可见，IPAM 也不会监控该资源。但该资源的 IP 地址仍可搜索。

- 如果您 [将 IPAM 与组织外部的账户集成](#)，IPAM 所有者可以查看这些账户拥有的所有资源 CIDR 的 IP 地址历史记录。

AWS Management Console

要查看 CIDR 的历史记录

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择搜索 IP 历史记录。
3. 输入 IPv4 或 IPv6 IP 地址或 CIDR。它必须是资源的特定 CIDR。
4. 选择 IPAM 范围 ID。
5. 选择日期/时间范围。
6. 如果要按 VPC 筛选结果，请输入 VPC ID。如果 CIDR 出现在多个 VPC 中，请使用此选项。
7. 选择搜索。

Command line

本节中的命令链接到《AWS CLI 命令参考》。本文档提供了运行命令时可以使用的选项的详细说明。

- 查看 CIDR 的历史记录：[get-ipam-address-history](#)

要查看如何使用 AWS CLI 分析和审计 IP 地址使用情况的示例，请参阅[教程：使用 AWS CLI 查看 IP 地址历史记录](#)。

搜索结果分为以下列：

- Sampled end time (结束时间采样)：IPAM 范围内资源到 CIDR 关联的结束时间采样。在定期快照中获取更改，因此结束时间可能发生在此特定时间之前。
- Sampled start time (开始时间采样)：IPAM 范围内资源到 CIDR 关联的开始时间采样。在定期快照中获取更改，因此开始时间可能发生在此特定时间之前。

Example

为了帮助解释您在开始时间采样和结束时间采样下看到的时间，我们来看一个示例使用案例：

下午 2:00，创建了一个具有 CIDR 10.0.0.0/16 的 VPC。下午 3:00，创建了一个具有 CIDR 10.0.0.0/8 的 IPAM 和 IPAM 池，然后选择自动导入选项以允许 IPAM 发现和导入属于 10.0.0.0/8 IP 地址范围内的任何 CIDR。由于 IPAM 会在定期快照中获取对 CIDR 的更改，因此到下午 3:05 分才会发现现有的 VPC CIDR。当您使用搜索 IP 历史记录功能搜索此 VPC 的 ID 时，VPC 的采样开始时间为下午 3:05，即 IPAM 发现它的时间，而不是下午 2:00（创建 VPC 的时间）。现在，假设您决定在下午 5:00 删除 VPC。删除 VPC 后，将分配给 VPC 的 CIDR 10.0.0.0/16 回收回 IPAM 池。IPAM 在下午 5:05 拍摄定期快照并获取更改。当您在搜索 IP 历史记录功能中搜索此 VPC 的 ID 时，VPC CIDR 的采样结束时间将为下午 5:05，而不是下午 5:00（删除 VPC 的时间）。

- Resource ID（资源 ID）：资源与 CIDR 关联时生成的 ID。
- Name（名称）：资源的名称（如果适用）。
- Compliance status（合规性状态）：CIDR 的合规性状态。
 - Compliant（合规）：托管资源符合 IPAM 池的分配规则。
 - Noncompliant（不合规）：资源 CIDR 不符合 IPAM 池的一个或多个分配规则。

Example

如果 VPC 的 CIDR 不符合 IPAM 池的网络掩码长度参数，或者资源与 IPAM 池不在同一个 AWS 区域中，它将被标记为不合规。

- Unmanaged（非托管）：该资源不具有从 IPAM 池中分配的 CIDR，IPAM 正在监控该资源是否存在符合池分配规则的 CIDR。对 CIDR 进行重叠监控。
- Ignored（已忽略）：已选择该托管资源免于监控。不会评估忽略的资源是否存在重叠或分配规则合规性。选择忽略资源时，从 IPAM 池中分配给它的任何空间都将返回到池中，并且不会通过自动导入再次导入该资源（如果在池中设置了自动导入分配规则）。
- -：此资源不是 IPAM 可以监控或管理的资源类型之一。
- Overlap status（重叠状态）：CIDR 的重叠状态。
 - Nonoverlapping（不重叠）：资源 CIDR 与同一范围内的另一个 CIDR 不重叠。
 - Overlapping（重叠）：资源 CIDR 与同一范围内的另一个 CIDR 重叠。请注意，如果资源 CIDR 重叠，则可能与手动分配重叠。
 - Ignored（已忽略）：已选择该托管资源免于监控。IPAM 不会评估被忽略资源的重叠或分配规则合规性。选择忽略资源时，从 IPAM 池中分配给它的任何空间都将返回到池中，并且不会通过自动导入再次导入该资源（如果在池中设置了自动导入分配规则）。
 - -：此资源不是 IPAM 可以监控或管理的资源类型之一。
- 资源类型

- vpc : CIDR 与 VPC 关联。
- subnet (子网) : CIDR 与 VPC 子网相关联。
- eip : CIDR 与弹性 IP 地址相关联。
- instance (实例) : CIDR 与 EC2 实例相关联。
- network-interface : CIDR 与网络接口相关联。
- VPC ID : 此资源所属的 VPC 的 ID (如果适用)。
- Region (区域) : 此资源的 AWS 区域。
- Owner ID (所有者 ID) : 创建此资源的用户的 AWS 账户 ID (如果适用)。

查看公有 IP 见解

您可以使用公共 IP 洞察功能来查看以下内容：

- 如果您的 IPAM 已[与 AWS 组织中的多个账户集成](#)，则可以查看整个 AWS 组织中所有 AWS 区域的服务使用的所有公有 IPv4 地址。
- 如果您的 IPAM 已[与单个账户集成](#)，则可以查看你的账户所有 AWS 区域的服务使用的所有公有 IPv4 地址。

公有 IPv4 地址是指可从互联网路由的 IPv4 地址。公有 IPv4 地址是通过 IPv4 从互联网直接访问资源所必需的。

Note

AWS 将对所有公有 IPv4 地址收费，包括与运行的实例相关联的公有 IPv4 地址和弹性 IP 地址。有关更多信息，请参阅 [Amazon VPC 定价页面](#) 中的公有 IPv4 地址定价选项卡。

您可以查看对以下公有 IPv4 地址类型的洞察：

- 弹性 IP 地址 (EIP) : Amazon 提供的静态公有 IPv4 地址，您可以将其与 EC2 实例、弹性网络接口或 AWS 资源相关联。
- EC2 公有 IPv4 地址 : Amazon 分配给 EC2 实例的公有 IPv4 地址 (如果 EC2 实例在默认子网中启动，或者该实例在已配置为自动分配公有 IPv4 地址的子网中启动)。
- BYOIPv4 地址 : 您使用[自带 IP 地址 \(BYOIP\)](#)带到 AWS 的 IPv4 地址范围内的公有 IPv4 地址。

- 服务管理的 IPv4 地址：在 AWS 资源上自动预配置并由 AWS 服务管理的公有 IPv4 地址。例如，Amazon ECS、Amazon RDS 或 Amazon WorkSpaces 上的公有 IPv4 地址。

公共 IP 洞察功能会向您显示您的账户中跨区域使用的服务的所有公有 IPv4 地址。您可以使用这些见解来确定公有 IPv4 地址的使用情况，并查看释放未使用的弹性 IP 地址的建议。

- 公有 IP 类型：按类型组织的公有 IPv4 地址的数量。
 - Amazon 拥有的 EIP：您已为您的 AWS 账户中的资源预配置或分配的弹性 IP 地址。
 - EC2 公有地址：当实例启动到默认子网或配置为自动分配公有 IPv4 地址的子网时，分配给 EC2 实例的公有 IPv4 地址。
 - BYOIP：您使用自带 IP 地址 (BYOIP) 带到 AWS 的公有 IPv4 地址。
 - 服务托管 IP：由 AWS 服务预配置和管理的公有 IPv4 地址。
 - 服务托管 BYOIP：带给 AWS 并由 AWS 服务管理的公有 IPv4 地址。
 - Amazon 拥有的连续 EIP：从 Amazon 提供的连续公有 IPv4 IPAM 池中分配的弹性 IP 地址。
- EIP 使用情况：按使用方式组织的弹性 IP 地址的数量。
 - Amazon 拥有的关联 EIP：您在 AWS 账户中预配置且已将其与 EC2 实例、网络接口或 AWS 资源关联的弹性 IP 地址。
 - 关联的 BYOIP：您使用 BYOIP 带到 AWS 且已将其与网络接口关联的公有 IPv4 地址。
 - Amazon 拥有的未关联 EIP：您在 AWS 帐户中预配置但尚未将其与网络接口关联的弹性 IP 地址。
 - 未关联的 BYOIP：您使用 BYOIP 带到 AWS 但未将其与网络接口关联的公有 IPv4 地址。
 - Amazon 拥有的关联的连续 EIP：从 Amazon 提供的连续公有 IPv4 IPAM 池中分配的并与资源关联的弹性 IP 地址。
 - Amazon 拥有的未关联的连续 EIP：从 Amazon 提供的连续公有 IPv4 IPAM 池中分配的并未与资源关联的弹性 IP 地址。
- Amazon 拥有的 IPv4 连续 IP 使用情况：该表显示了一段时间内连续的公有 IPv4 地址使用情况以及 Amazon 拥有的相关的 IPv4 IPAM 池。
- 公有 IP 地址：公有 IPv4 地址及其属性的表。
 - IP 地址：公有 IPv4 地址。
 - 关联：该地址是否与 EC2 实例、网络接口或 AWS 资源相关联。
 - 关联：公有 IPv4 地址与 EC2 实例、网络接口或 AWS 资源相关联。
 - 未关联：公有 IPv4 地址未与任何资源相关联且在 AWS 账户中处于空闲状态。

- 地址类型：IP 地址类型。
 - Amazon 拥有的 EIP：公有 IPv4 地址是弹性 IP 地址。
 - BYOIP：公有 IPv4 地址已使用 BYOIP 带到 AWS。
 - EC2 公有 IP：公有 IPv4 地址已自动分配给 EC2 实例。
 - 服务管理 BYOIP：公有 IPv4 地址已使用自带 IP (BYOIP) 带入 AWS。
 - 服务托管 IP：公有 IPv4 地址已预配置并由 AWS 服务管理。
- 服务：与 IP 地址关联的服务。
 - AGA：AWS Global Accelerator。如果使用[自定义路由加速器](#)，则不会列出其公有 IP。要查看这些公有 IP，请参阅[查看您的自定义路由加速器](#)。
 - 数据库迁移服务：AWS Database Migration Service (DMS) 复制实例。
 - Redshift：Amazon Redshift 集群。
 - RDS：Amazon Relational Database Service (RDS) 实例。
 - 负载均衡器 (EC2)：应用程序负载均衡器或网络负载均衡器。
 - NAT 网关 (VPC)：Amazon VPC 公有 NAT 网关。
 - Site-to-Site VPN：AWS Site-to-Site VPN 虚拟私有网关。
 - 其他：其他当前无法识别的服务。
- 名称 (EIP ID)：如果此公有 IPv4 地址是弹性 IP 地址分配，则这是 EIP 分配的名称和 ID。
- 网络接口 ID：如果此公有 IPv4 地址与网络接口关联，则这是网络接口的 ID。
- 实例 ID：如果此公有 IPv4 地址与 EC2 实例关联，则这是实例 ID。
- 安全组：如果此公有 IPv4 地址与 EC2 实例关联，则这是分配给实例的安全组的名称和 ID。
- 公有 IPv4 池：如果这是来自 Amazon 拥有和管理的 IP 地址池的弹性 IP 地址，则值为“-”。如果您是拥有并带给 Amazon (使用 BYOIP) 的 IP 地址范围内的弹性 IP 地址，则值为公有 IPv4 池 ID。
- 网络边界组：如果广告了 IP 地址，则这是广告 IP 地址的 AWS 区域。
- 所有者 ID：资源所有者的 AWS 账号。
- 采样时间：上次成功发现资源的时间。
- 资源发现 ID：发现此公有 IPv4 地址的资源发现的 ID。
- 服务资源：资源 ARN 或 ID。

如果向您的账户分配了弹性 IP 地址，但该地址未与网络接口关联，则会出现一条横幅，告知您的账户中有未关联的 EIP，应将其释放。

Important

公共 IP 洞察功能最近已更新。如果您看到与无权调用 `getIpamDiscoveredPublicAddresses` 相关的错误，则需要更新与您共享的资源发现所附加的托管权限。联系创建资源发现的人员，要求他们将托管权限 `AWSRAMPermissionIpamResourceDiscovery` 更新为默认版本。有关更多信息，请参阅《AWS RAM 用户指南》中的[更新资源共享](#)。

AWS Management Console

查看公有 IP 地址洞察

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择公有 IP 地址见解。
3. 如需查看公有 IP 地址的详细信息，请单击 IP 地址来选择该地址。
4. 查看 IP 地址相关的以下信息：
 - 详细信息：与“公有 IP 见解”主窗格的列中可见的信息相同，例如地址类型和服务。
 - 入站安全组规则：如果此 IP 地址与 EC2 实例关联，则这些是控制实例入站流量的安全组规则。
 - 出站安全组规则：如果此 IP 地址与 EC2 实例关联，则这些是控制来自实例的出站流量的安全组规则。
 - 标签：充当元数据的键和值对，用于组织 AWS 资源。

Command line

使用以下命令获取 IPAM 发现的公有 IP 地址：[get-ipam-discovered-public-addresses](#)

Amazon VPC IP 地址管理器教程

以下教程为您演示如何使用 AWS CLI 执行常见 IPAM 任务。要获取 AWS CLI，请参阅 [访问 IPAM](#)。有关这些教程中提到的 IPAM 概念的更多信息，请参阅 [IPAM 的工作原理](#)。

内容

- [开始通过 AWS CLI 使用 IPAM](#)
- [教程：使用控制台创建 IPAM 和池](#)
- [教程：使用 AWS CLI 创建 IPAM 和池](#)
- [教程：使用 AWS CLI 查看 IP 地址历史记录](#)
- [教程：自带 ASN 到 IPAM 中](#)
- [教程：将 IP 地址带入 IPAM](#)
- [教程：将 BYOIP IPv4 CIDR 传输到 IPAM](#)
- [教程：为子网 IP 分配规划 VPC IP 地址空间](#)
- [从 IPAM 池中分配连续弹性 IP 地址](#)

开始通过 AWS CLI 使用 IPAM

本教程将指导您完成使用单个 AWS 账户在 AWS CLI 中设置和使用 Amazon VPC IP 地址管理器 (IPAM) 的过程。到本教程结束时，您将已经创建 IPAM 和 IP 地址池层次结构，并将 CIDR 分配给了 VPC。

先决条件

在开始本教程之前，请确保您具有：

- 有权创建和管理 IPAM 资源的 AWS 账户。
- 已安装 AWS CLI 并配置了相应的凭证。有关安装 AWS CLI 的信息，请参阅 [安装或更新最新版本的 AWS CLI](#)。有关配置 AWS CLI 的信息，请参阅 [基本配置](#)。
- 有关 IP 寻址和 CIDR 表示法的基础知识。
- 有关 Amazon VPC 概念的基础知识。
- 完成本教程大约需要 30 分钟。

创建 IPAM

第一步是根据运营区域创建 IPAM。您可以使用 IPAM 来计划、跟踪和监控 AWS 工作负载的 IP 地址。

创建 IPAM，其运营区域为 us-east-1 和 us-west-2：

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

此命令会创建 IPAM 并使其能够管理指定区域中的 IP 地址。运营区域是允许 IPAM 在其中管理 IP 地址 CIDR 的 AWS 区域。

验证 IPAM 是否已创建：

```
aws ec2 describe-ipams
```

记下输出中的 IPAM ID，您将在后续步骤中用到它。

等待 IPAM 创建完毕并可用（约 20 秒）：

```
sleep 20
```

获取 IPAM 范围 ID

创建 IPAM 时，AWS 将自动创建一个私有范围和一个公有范围。在本教程中，我们将使用私有范围。

检索 IPAM 详细信息并提取私有范围 ID：

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

将 ipam-0abcd1234 替换为实际的 IPAM ID。

在输出中，找到 PrivateDefaultScopeId 字段中的私有范围 ID 并记下来。该条目看起来类似于 ipam-scope-0abcd1234。

创建顶级 IPv4 池

现在，我们在私有范围中创建一个顶级池。该池将作为层次结构中所有其他池的父池。

创建顶级 IPv4 池：

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

将 `ipam-scope-0abcd1234` 替换为实际的私有范围 ID。

等待池创建完毕并可用：

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

将 `ipam-pool-0abcd1234` 替换为实际的顶级池 ID。应等待状态显示 `create-complete` 之后，再继续操作。

池可用后，向池预置 CIDR 块：

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

等待 CIDR 预置完毕：

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

应等待状态显示 `provisioned` 之后，再继续操作。

创建区域 IPv4 池

接下来，在顶级池中创建区域池。该池特定于某个特别的 AWS 区域。

创建区域 IPv4 池：

```
aws ec2 create-ipam-pool \  
  --ipam-scope-id ipam-scope-0abcd1234 \  
  --source-ipam-pool-id ipam-pool-0abcd1234 \  
  --region us-east-1
```

```
--locale us-east-1 \  
--address-family ipv4 \  
--description "Regional pool in us-east-1"
```

将 `ipam-scope-0abcd1234` 替换为实际的私有范围 ID，将 `ipam-pool-0abcd1234` 替换为顶级池 ID。

等待区域池创建完毕并可用：

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

将 `ipam-pool-1abcd1234` 替换为实际的区域池 ID。应等待状态显示 `create-complete` 之后，再继续操作。

池可用后，向池预置 CIDR 块：

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

等待 CIDR 预置完毕：

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

应等待状态显示 `provisioned` 之后，再继续操作。

创建开发 IPv4 池

现在，在区域池中创建开发池。该池将用于开发环境。

创建开发 IPv4 池：

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

```

```
--description "Development pool"
```

将 `ipam-scope-0abcd1234` 替换为实际的私有范围 ID，将 `ipam-pool-1abcd1234` 替换为区域池 ID。

注意：务必添加 `--locale` 参数，以便与父池的区域一致。

等待开发池创建完毕并可用：

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

将 `ipam-pool-2abcd1234` 替换为实际的开发池 ID。应等待状态显示 `create-complete` 之后，再继续操作。

池可用后，向池预置 CIDR 块：

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

等待 CIDR 预置完毕：

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

应等待状态显示 `provisioned` 之后，再继续操作。

创建使用 IPAM 池 CIDR 的 VPC

最后，创建使用 IPAM 池中 CIDR 的 VPC。此处演示了如何使用 IPAM 为 AWS 资源分配 IP 地址空间。

创建使用 IPAM 池 CIDR 的 VPC：

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

将 `ipam-pool-2abcd1234` 替换为实际的开发池 ID。

`--ipv4-netmask-length 26` 参数指定了您希望从池中分配 /26 CIDR 块 (64 个 IP 地址)。选择此网络掩码长度是为了确保它小于池的 CIDR 块 (/24)。

验证 VPC 是否已创建：

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

验证 IPAM 池的分配情况

检查 CIDR 是否已从 IPAM 池中分配：

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

将 `ipam-pool-2abcd1234` 替换为实际的开发池 ID。

此命令显示了来自指定 IPAM 池的所有分配，包括您刚刚创建的 VPC。

故障排除

以下是在使用 IPAM 时可能会遇到的一些常见问题：

- **权限错误**：请确保 IAM 用户或角色具有创建和管理 IPAM 资源所需的权限。您可能需要 `ec2:CreateIpam`、`ec2:CreateIpamPool` 和其他相关权限。
- **超出资源限制**：默认情况下，只能为每个账户创建一个 IPAM。如果已经有一个 IPAM，则需要先将其删除，然后再创建新的 IPAM，或者使用现有的 IPAM。
- **CIDR 分配失败**：向池预置 CIDR 时，请确保要预置的 CIDR 不会与其他池中的现有分配重叠。
- **API 请求超时**：如果您遇到“RequestExpired”错误，这可能是由于网络延迟或时间同步问题所致。请尝试再次运行命令。
- **“状态错误”报错**：如果您收到“IncorrectState”错误，这可能是由于您尝试对其执行操作的资源未处于正确状态。请等待资源创建或预置完毕再继续。
- **分配大小错误**：如果您收到有关分配大小的“InvalidParameterValue”错误，请确保您请求的网络掩码长度适合池大小。例如，您不能从 /24 池中分配 /25 CIDR。
- **依赖项冲突**：清理资源时，您可能会遇到“DependencyViolation”错误。这是因为资源之间存在依赖关系。在删除池之前，请确保按照与创建时相反的顺序删除资源，并取消预置 CIDR。

清理资源

完成本教程后，应清除您创建的资源，以免产生不必要的费用。

1. 删除 VPC：

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

2. 从开发池中取消预置 CIDR：

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

3. 删除开发池：

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

4. 从区域池中取消预置 CIDR：

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

5. 删除区域池：

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

6. 从顶级池中取消预置 CIDR：

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

7. 删除顶级池：

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

8. 删除 IPAM：

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

将所有 ID 替换为实际的资源 ID。

Note

前后两个操作的间隔时间应稍微延长一些，以确保资源完全删除，然后再继续下一步操作。如果您遇到依赖项冲突的问题，请等待几秒，然后重试。

后续步骤

现在，您已经学会了如何通过 AWS CLI 创建和使用 IPAM，您可能需要探索更多高级功能：

- [计划 IP 地址预置](#)：了解如何有效规划 IP 地址空间
- [按资源监控 CIDR 使用情况](#)：了解如何监控 IP 地址使用情况
- [使用 AWS RAM 共享 IPAM 池](#)：了解如何跨 AWS 账户共享 IPAM 池
- [将 IPAM 与 AWS Organization 中的账户集成](#)：了解如何在整个组织中使用 IPAM

教程：使用控制台创建 IPAM 和池

在本教程中，您将创建 IPAM、与 AWS Organizations 集成、创建 IP 地址池，并使用 IPAM 池中的 CIDR 创建 VPC。

本教程将向您展示如何根据不同的开发需求使用 IPAM 来组织 IP 地址空间。完成本教程后，您将拥有一个用于预生产资源的 IP 地址池。然后，您可以根据路由和安全需求创建其他池，例如用于生产资源的池。

尽管您可以作为单个用户使用 IPAM，但如果与 AWS Organizations 集成，您将能够在组织中跨账户管理 IP 地址。本教程将介绍如何将 IPAM 与组织中的账户集成，不包括如何 [将 IPAM 与组织外部的账户集成](#)。

Note

本教程中的说明将向您介绍如何以特定方式命名 IPAM 资源、在特定区域中创建 IPAM 资源，以及为池使用特定的 IP 地址 CIDR 范围。此举旨在简化 IPAM 中的可用选择，便于您快速开始使用 IPAM。完成本教程后，您可能会决定创建一个新的 IPAM 并对其进行不同的配置。

内容

- [前提条件](#)
- [AWS Organizations 如何与 IPAM 集成](#)
- [步骤 1：委派 IPAM 管理员](#)
- [步骤 2：创建 IPAM](#)
- [步骤 3：创建顶级 IPAM 池](#)
- [步骤 4：创建区域 IPAM 池](#)
- [步骤 5：创建预生产开发池](#)
- [步骤 6：共享 IPAM 池](#)
- [步骤 7：创建一个 VPC，其具有从 IPAM 池分配的 CIDR](#)
- [步骤 8：清除](#)

前提条件

开始之前，必须设置具有至少一个成员账户的 AWS Organizations 账户。有关更多信息，请参阅《AWS Organizations 用户指南》中的[创建并管理组织](#)。

AWS Organizations 如何与 IPAM 集成

本部分显示了您在本教程中使用的 AWS Organizations 账户的示例。在本教程中，与 IPAM 集成时，您将使用组织中的三个账户：

- 用于登录 IPAM 控制台并委派 IPAM 管理员的管理账户（下图中称为 example-management-account）。您不能将组织的管理账户作为 IPAM 管理员。
- 作为 IPAM 管理员账户的成员账户（下图中称为 example-member-account-1）。IPAM 管理员账户负责创建 IPAM 并使用它来管理和监控整个组织的 IP 地址使用情况。您可以将组织中的任何成员账户委派为 IPAM 管理员。
- 作为开发者账户的成员账户（上文中称为 example-member-account-2）。此账户会创建一个 VPC，其具有一个从 IPAM 池分配的 CIDR。

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 the title is a search bar and a 'Hierarchy' button. The main content is a table showing the organizational structure:

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 855210303341 example-management-account@amazon.com	Joined 2022/12/28

除账户外，您还需要组织单位（包含将其用作开发者账户的成员账户，上图中的 `ou-fssg-q5brfv9c`）的 ID。您需要使用此 ID，以便在后面的步骤中共享 IPAM 池时可以与该 OU 共享。

Note

有关管理账户和成员账户等 AWS Organizations 账户类型的更多信息，请参阅 [AWS Organizations 术语和概念](#)。

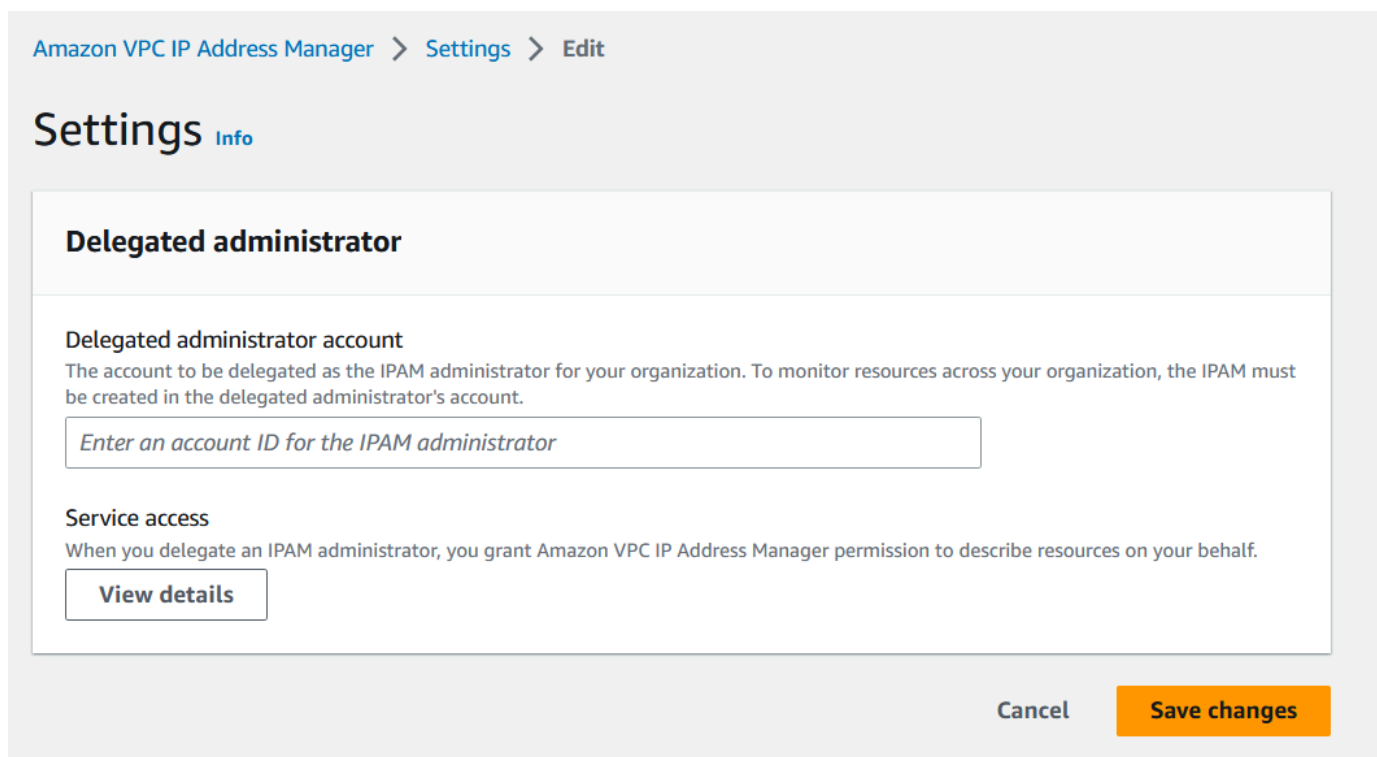
步骤 1：委派 IPAM 管理员

在此步骤中，您将委派 AWS Organizations 成员账户作为 IPAM 管理员。当您委派 IPAM 管理员时，每个 AWS Organizations 成员账户中都会自动创建一个 [服务相关角色](#)。IPAM 通过在每个成员账户中担任服务相关角色，来监控这些账户中的 IP 地址使用情况。然后，无论其组织单位如何，它都可以发现资源及其 CIDR。

您必须拥有所需的 AWS Identity and Access Management (IAM) 权限，才能完成此步骤。有关更多信息，请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)。

委派 IPAM 管理员账户

1. 使用 AWS Organizations 管理账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在 AWS 管理控制台中，选择您要在其中与 IPAM 合作的 AWS 区域。
3. 在导航面板中选择组织设置。
4. 选择 Delegate (委派)。仅当您以 AWS Organizations 管理账户身份登录控制台时，委派选项才可用。
5. 输入组织成员账户的 AWS 账户 ID。IPAM 管理员必须是 AWS Organizations 成员账户，而不是管理账户。



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 Info'. Below this, there is a section titled 'Delegated administrator'. Underneath, it says 'Delegated administrator account' and provides 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.' There is a text input field with the placeholder text 'Enter an account ID for the IPAM administrator'. Below that, there is a section titled 'Service access' with the text: 'When you delegate an IPAM administrator, you grant Amazon VPC IP Address Manager permission to describe resources on your behalf.' There is a 'View details' button. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

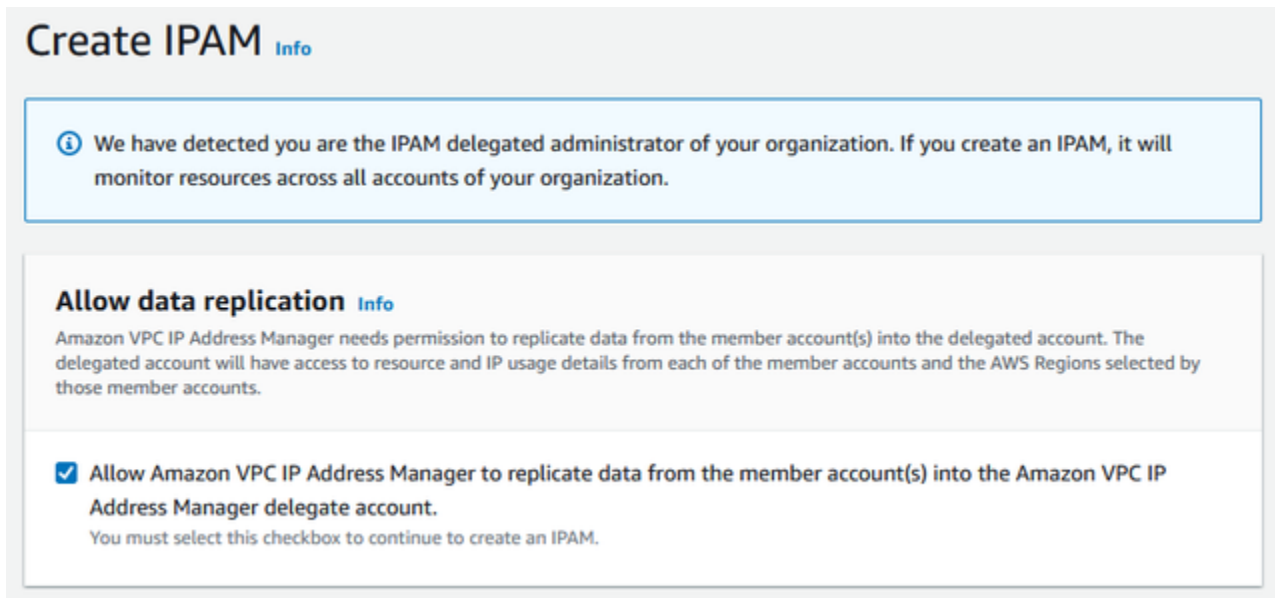
6. 选择保存更改。使用与成员账户相关的详细信息填充委派管理员信息。

步骤 2：创建 IPAM

在本步骤中，您将创建一个 IPAM。创建 IPAM 时，IPAM 会自动为 IPAM 创建两个作用域：用于所有私有空间的私有作用域和用于所有公有空间的公有作用域。范围以及池和分配是 IPAM 的关键组成部分。有关更多信息，请参阅 [IPAM 的工作原理](#)。

创建 IPAM

1. 使用 [上一步](#) 中委派作为 IPAM 管理员的 AWS Organizations 成员账户，打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在 AWS 管理控制台中，选择您要在其中创建 IPAM 的 AWS 区域。在主操作区域创建 IPAM。
3. 在服务主页上，选择创建 IPAM。
4. 选择 Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (允许 Amazon VPC IP 地址管理器将数据从源账户复制到 IPAM 委托账户中)。如果未选中此选项，则无法创建 IPAM。



5. 在运营区域下，选择此 IPAM 可以在其中管理和发现资源的 AWS 区域。您要在其中创建 IPAM 的 AWS 区域将自动被选为运营区域之一。在本教程中，IPAM 的主区域是 us-east-1，因此我们将选择 us-west-1 和 us-west-2 作为其他运营区域。如果忘记了运营区域，可以稍后编辑 IPAM 设置并添加或删除区域。

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. 选择创建 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

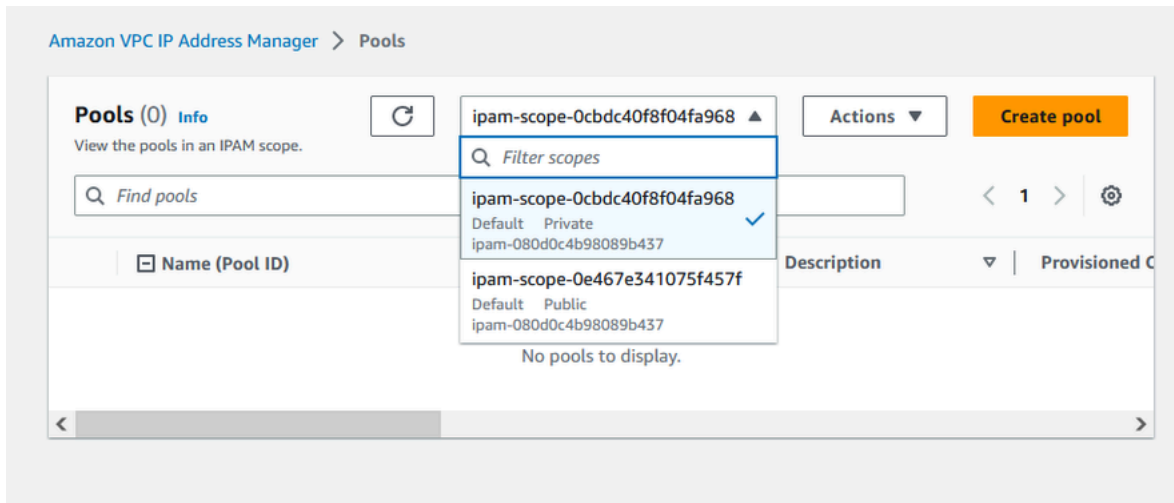
步骤 3：创建顶级 IPAM 池

在本教程中，您将从顶层 IPAM 池开始创建池层次结构。在后续步骤中，您将创建一对区域池和其中一个区域池中的预生产开发池。

有关可以使用 IPAM 构建的池层次结构的更多信息，请参阅 [示例 IPAM 池计划](#)。

创建顶层池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 选择私有作用域。



4. 选择创建池。
5. 在 IPAM 范围下，确保选中私有范围。
6. （可选）添加池的名称标签和对池的描述，如“Global pool”。
7. 在源下，选择 IPAM 范围。这是我们的顶层池，它没有源池。
8. 在地址系列下，选择 IPv4。
9. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
10. 对于区域设置，选择无。区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。您将在本教程的下一部分中为您创建的区域池设置区域设置。

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. 选择要为池预置的 CIDR。在此示例中，预置的是 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

12. 将配置此池的分配规则设置保留为禁用状态。这是我们的顶层池，您无法直接从该池中将 CIDR 分配给 VPC。相反，您将从从该池创建的子池中进行分配。

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

13. 选择创建池。池已创建，且 CIDR 处于等待预置状态：

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. 请等待状态切换为已预置，然后再执行下一步操作。

✔ 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/ipam-pool-06fb4cace4bc1e551	Owner ID 320805250157	Compliance status -	Overlap status -

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

CIDRs (1) Info

Deprovision CIDRs | Provision CIDR

< 1 > ⚙

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

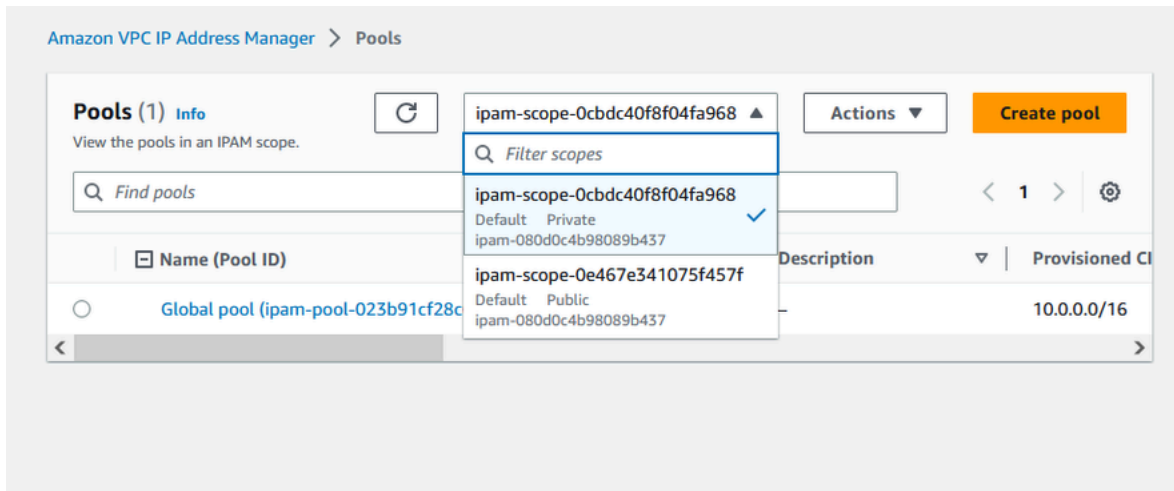
现在，您已创建顶层池，将在 us-west-1 和 us-west-2 中创建区域池。

步骤 4：创建区域 IPAM 池

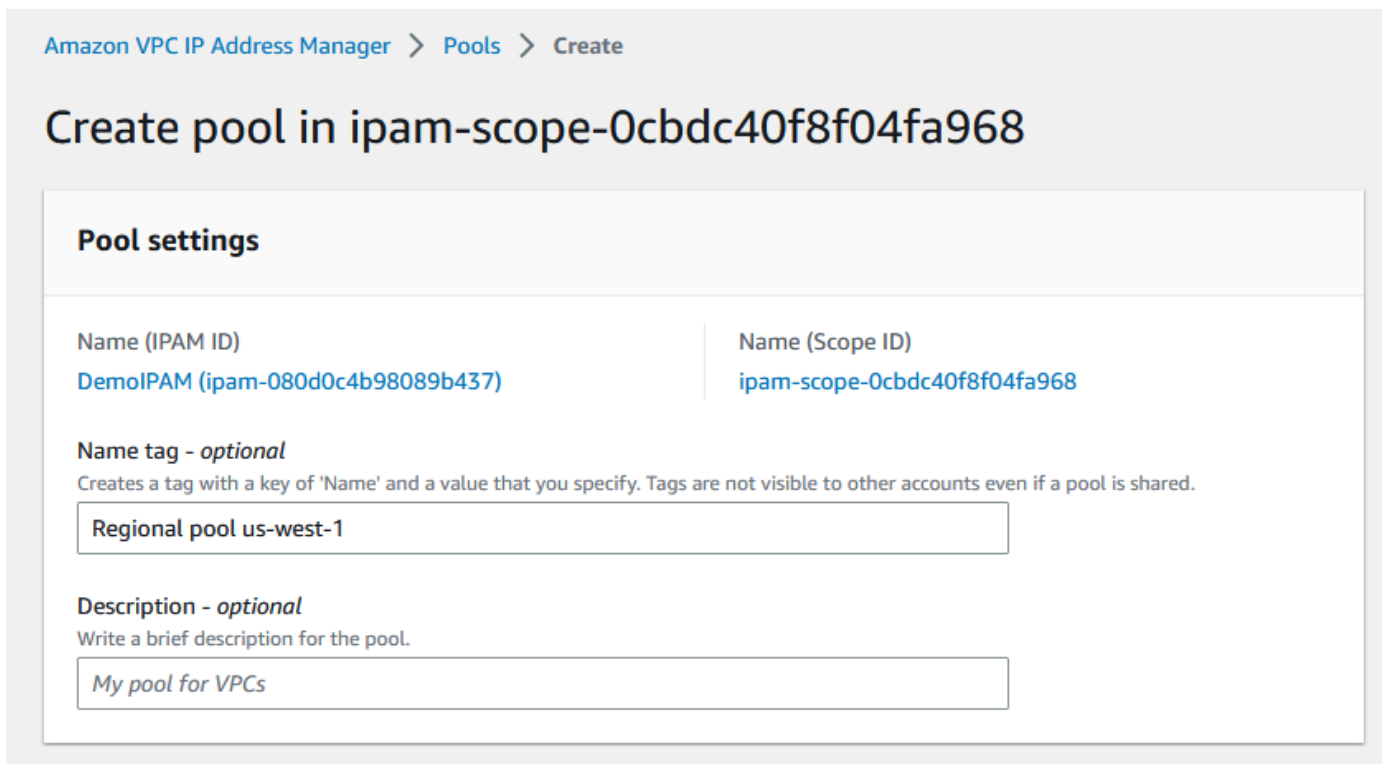
本部分将介绍如何使用两个区域池组织 IP 地址。在本教程中，我们将遵循其中一个[示例 IPAM 池计划](#)，并创建两个区域池，供您组织中的成员账户用于向其 VPC 分配 CIDR。

创建区域池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 选择私有作用域。



4. 选择创建池。
5. 在 IPAM 范围下，确保选中私有范围。
6. (可选) 添加池的名称标签和池的描述，例如区域池 us-west-1。



7. 在源下，选择 IPAM 池，然后选择您在 [步骤 3：创建顶级 IPAM 池](#) 中创建的顶层池（“全局池”）。然后，在区域设置下，选择 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.

- 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
- 在要预置的 CIDR 下，输入 10.0.0.0/18，这将为该池提供大约 16,000 个可用 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

10. 将配置此池的分配规则设置保留为禁用状态。您无法直接从该池中将 CIDR 分配给 VPC。相反，您将从从该池创建的子池中进行分配。

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

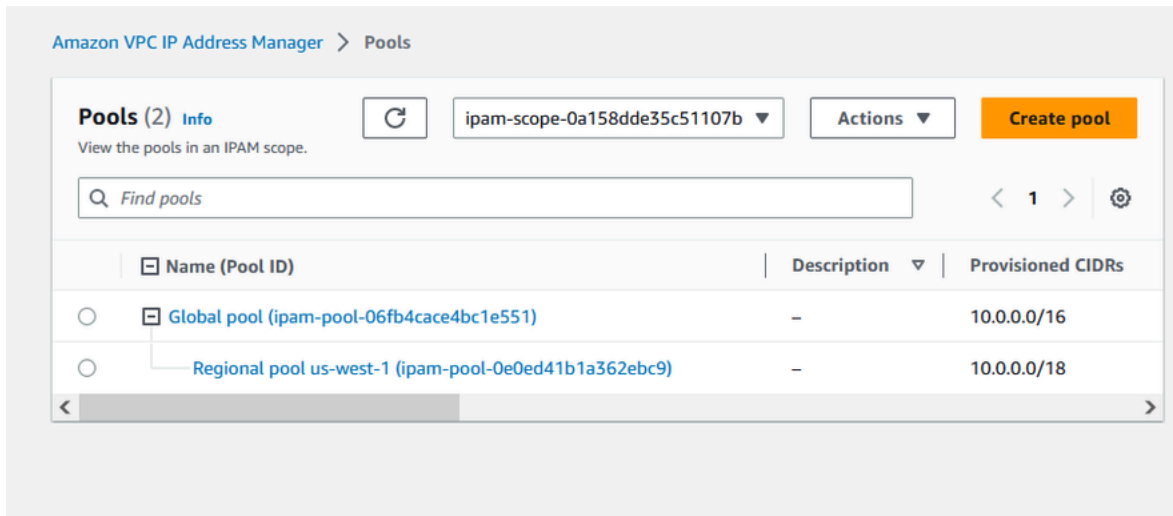


AWS best practice

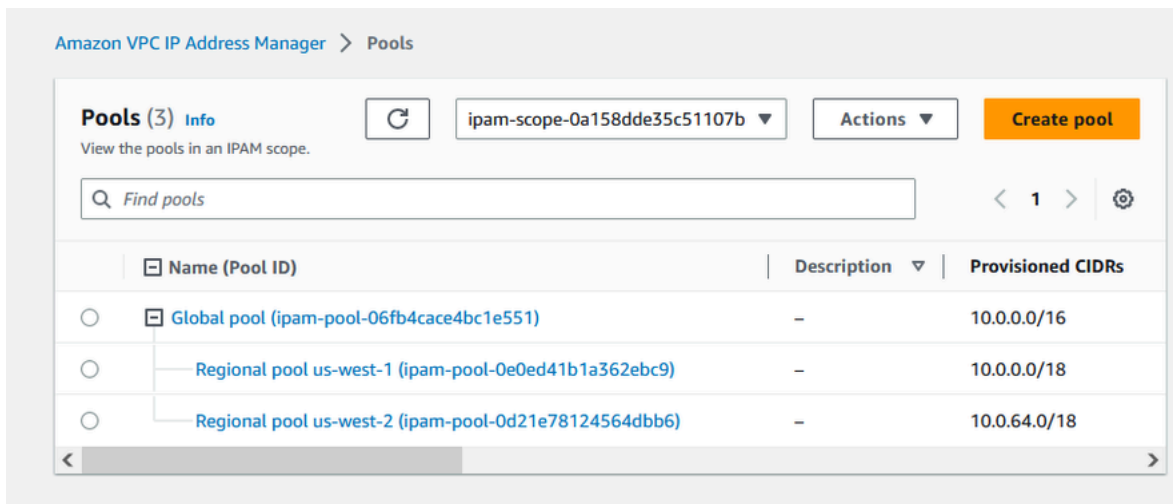
We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize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

Configure this pool's allocation rule settings

11. 选择创建池。
12. 返回到池视图查看您创建的 IPAM 池的层次结构。



13. 重复本节中的步骤，在 us-west-2 区域设置中创建第二个区域池，并为其预置 CIDR 10.0.64.0/18。完成该过程后，您将在与此层次结构类似的层次结构中拥有三个池：



步骤 5：创建预生产开发池

按照本部分中的步骤，在其中一个区域池中创建用于预生产资源的开发池。

创建预生产开发池

1. 采用上一部分中的相同方式，使用 IPAM 管理员账户创建一个名为 Pre-prod 池的池，但这次使用区域池 us-west-1 作为源池。

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 10.0.0.0/20 的 CIDR 进行预置，这将为该池提供大约 4,000 个 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. 切换配置此池的分配规则设置选项。执行以下操作：

1. 在 CIDR 管理下，对于自动导入已发现的资源，将默认的不允许选项保留为选中状态。此选项将使 IPAM 自动导入其在池的区域设置中发现的资源 CIDR。本教程不提供此选项的详细说明，但您可以在 [创建顶级 IPv4 池](#) 中阅读有关该选项的更多信息。
2. 在网络掩码合规性下，为网络掩码长度最小值、默认值和最大值选择 /24。本教程不提供此选项的详细说明，但您可以在 [创建顶级 IPv4 池](#) 中阅读有关该选项的更多信息。需要注意的是，您稍后使用该池中的 CIDR 创建的 VPC 将根据此处设置限制为 /24。
3. 在标签合规性下，输入 environment/pre-prod。VPC 需要此标签才能从池中分配空间。稍后我们将演示其工作原理。

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



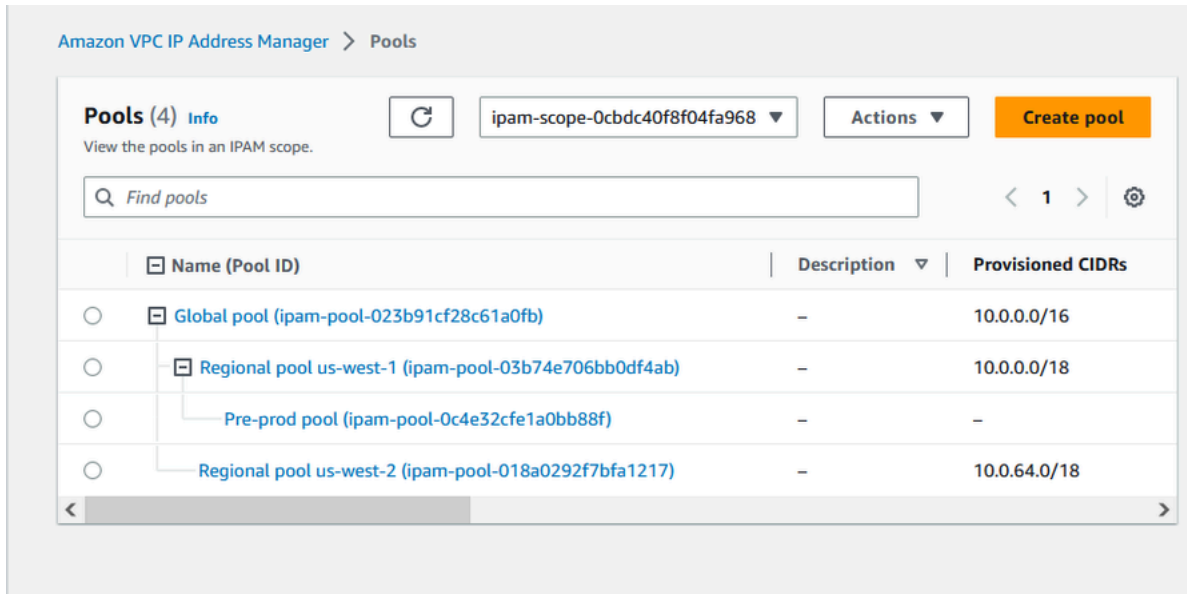
Remove

Add new required tag

You can add up to 49 more tags.

4. 选择创建池。

5. 现在，池层次结构在区域池 us-west-1 下添加了一个额外的子池：



现在，您已准备好与组织中的另一个成员账户共享 IPAM 池，并允许该账户从池中分配 CIDR 来创建 VPC。

步骤 6：共享 IPAM 池

按照本部分中的步骤使用 AWS Resource Access Manager (RAM) 共享预生产的 IPAM 池。

本部分包含两个子部分：

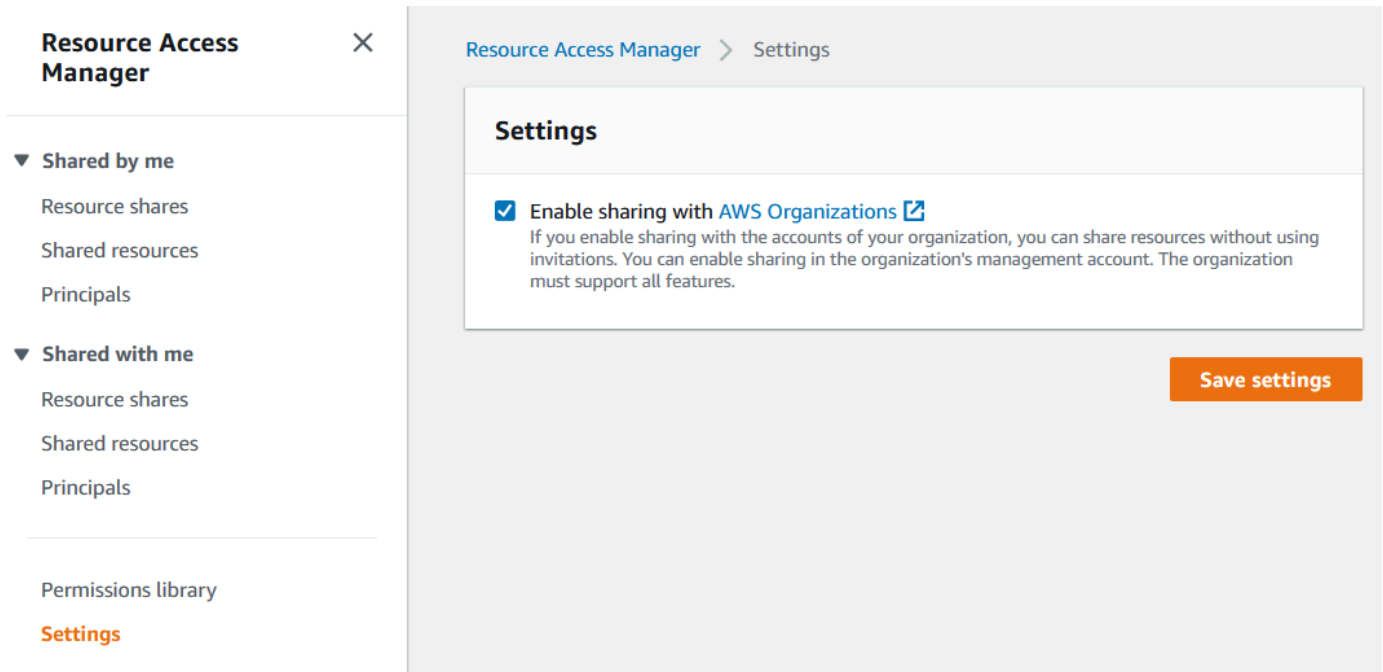
- [步骤 6.1. 在 AWS RAM 中启用资源共享](#)：此步骤必须由 AWS Organizations 管理账户完成。
- [步骤 6.2. 使用 AWS RAM 共享 IPAM 池](#)：此步骤必须由 IPAM 管理员完成。

步骤 6.1. 在 AWS RAM 中启用资源共享

创建 IPAM 后，您需要与组织中的其他账户共享 IP 地址池。在共享 IPAM 池之前，请先完成本部分中的步骤，启用与 AWS RAM 的资源共享。

启用资源共享

1. 使用 AWS Organizations 管理账户打开 AWS RAM 控制台，地址：<https://console.aws.amazon.com/ram/>。
2. 在左侧导航窗格中，依次选择设置、启用与 AWS Organizations 共享、保存设置。



您现在可以与组织的其他成员共享 IPAM 池。

步骤 6.2. 使用 AWS RAM 共享 IPAM 池

在本部分中，您将与其他 AWS Organizations 成员账户共享预生产开发池。有关共享 IPAM 池的完整说明，例如所需 IAM 权限的相关信息，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。

使用 AWS RAM 共享 IPAM 池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 选择私有作用域，选择预生产 IPAM 池，然后选择操作 > 查看详细信息。
4. 在资源共享下，选择创建资源共享。AWS RAM 控制台将打开。您将使用 AWS RAM 共享该池。
5. 选择创建资源共享。

Sent request to provision 10.0.0/20

Amazon VPC IP Address Manager > Pools > ipam-pool-07bdd12d7c94e4693

Pre-prod pool (ipam-pool-07bdd12d7c94e4693)

Pool summary

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

Pool details | Monitoring | IP space visualization | CIDRs | Allocations | Resources | Compliance | **Resource sharing** | Tags

Resource sharing Info

Filter resource shares

Resource share ARN | Status | Created at

No shares
This resource is not part of any resource share.

Create resource share

AWS RAM 控制台将打开。

- 在 AWS RAM 控制台中，再次选择创建资源共享。
- 为共享资源添加名称。
- 在选择资源类型下，选择 IPAM 池，然后选择预生产开发池的 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

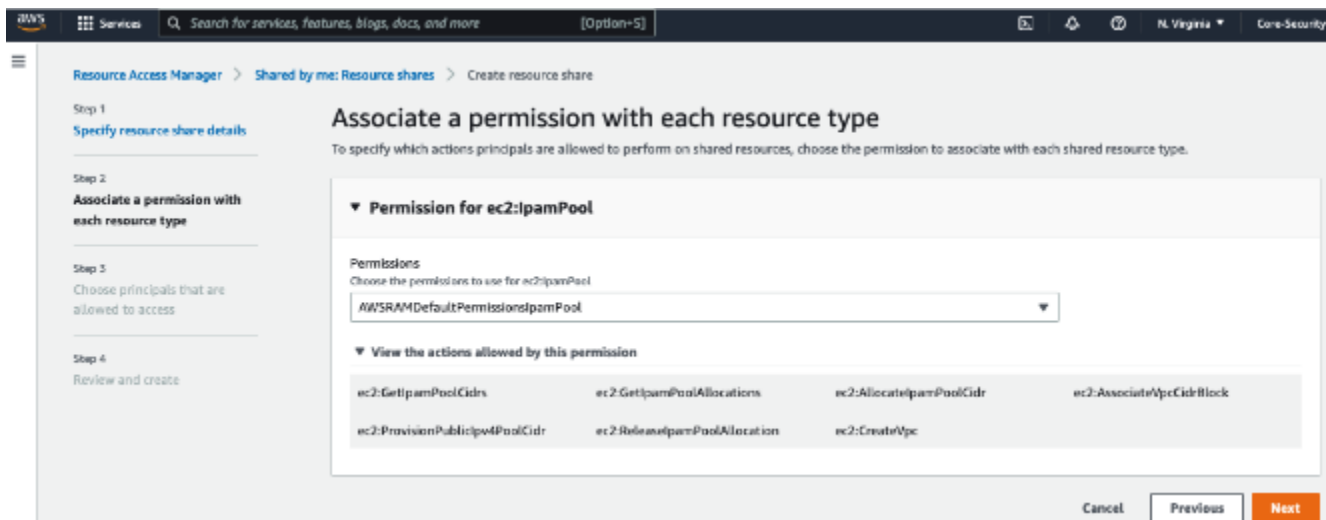
Selected resources (1)

Deselect

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

9. 选择下一步。

10. 将默认的 `AWSRAMDefaultPermissionsIpamPool` 权限保留为选中状态。本教程不提供权限选项的详细信息，但您可以在 [使用 AWS RAM 共享 IPAM 池](#) 中查看有关这些选项的更多信息。



11. 选择下一步。
12. 在主体下，选择仅允许在组织内共享。输入 AWS Organizations 组织单位 ID (如 [AWS Organizations 如何与 IPAM 集成](#) 中所述，然后选择添加)。

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

<input type="checkbox"/>	Principal ID	Type
--------------------------	--------------	------

No selected principals.

Cancel

Previous

Next

13. 选择下一步。

14. 查看资源共享选项和要共享的主体，然后选择创建。

现在池已共享，请转到下一步以创建 VPC，并向其分配 IPAM 池中的 CIDR。

步骤 7：创建一个 VPC，其具有从 IPAM 池分配的 CIDR

按照本部分中的步骤，创建一个具有从预生产池分配的 CIDR 的 VPC。此步骤应由上一部分中与之共享 IPAM 池的 OU 中的成员账户（在 [AWS Organizations 如何与 IPAM 集成](#) 中名为 example-member-account-2）完成。有关创建 VPC 所需的 IAM 权限的更多信息，请参阅《Amazon VPC 用户指南》中的 [Amazon VPC 策略示例](#)。

创建一个 VPC，其具有从 IPAM 池分配的 CIDR

1. 使用成员账户，作为您将用作开发者账户的成员账户打开 VPC 控制台，地址 <https://console.aws.amazon.com/vpc/>。
2. 选择创建 VPC。
3. 执行以下操作：
 1. 输入名称，例如 Example VPC。
 2. 选择 IPAM 分配的 IPv4 CIDR 块。
 3. 在 IPv4 IPAM 池下，选择预生产池的 ID。
 4. 选择网络掩码长度。由于您将此池的可用网络掩码长度限制为 /24 (在 [步骤 5：创建预生产开发池](#) 中)，因此唯一可用的网络掩码选项是 /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.

Example VPC

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

IPv4 IPAM pool

ipam-pool-0c4e32cfe1a0bb88f
us-west-1

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

Netmask

/24 (allowed maximum) 256 IPs

4. 为方便演示，此时请勿在标签下添加任何其他标签。创建预生产池（在[步骤 5：创建预生产开发池](#)中完成）时，您添加了一个分配规则，要求使用该池中的 CIDR 创建的任何 VPC 都必须具有环境/预生产标签。暂时将环境/预生产标签保留为关闭状态，以便您能够看到出现的错误，告知您没有添加所需的标签。
5. 选择创建 VPC。
6. 出现一个错误，告知您没有添加所需的标签。出现该错误是因为您在创建预生产池（在[步骤 5：创建预生产开发池](#)中）时设置了分配规则。分配规则要求使用此池中的 CIDR 创建的任何 VPC 都具有环境/预生产标签。

⊗ **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. 现在，在标签下，添加环境/预生产标签，然后再次选择创建 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 X

Q environment X

Add new tag

You can add 48 more tags.

Value - *optional*

Q Example VPC X

Q pre-prod X

Remove

Remove

8. VPC 创建成功，并且 VPC 符合预生产池上的标签规则：




✔ 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 控制台的资源窗格中，IPAM 管理员将能够查看和管理 VPC 及其分配的 CIDR。请注意，VPC 需要一些时间才能在资源窗格中显示。

步骤 8：清除

在本教程中，您通过委派管理员创建了 IPAM，也创建了多个池，还允许组织中的成员账户从池中分配 VPC CIDR。

按照本部分中的步骤清除您在本教程中创建的资源。

清除在本教程中创建的资源

1. 使用创建示例 VPC 的成员账户，删除 VPC。有关详细说明，请参阅《Amazon Virtual Private Cloud 用户指南》中的[删除 VPC](#)。
2. 使用 IPAM 管理员账户删除 AWS RAM 控制台中的示例资源共享。有关详细说明，请参阅《AWS Resource Access Manager 用户指南》中的[删除 AWS RAM 中的资源共享](#)。

3. 使用 IPAM 管理员账户登录 RAM 控制台并禁用您在 [步骤 6.1. 在 AWS RAM 中启用资源共享](#) 中启用的与 AWS Organizations 共享。
4. 使用 IPAM 管理员账户，在 IPAM 控制台中选择 IPAM，然后选择操作 > 删除，来删除示例 IPAM。有关详细说明，请参阅 [删除 IPAM](#)。
5. 当系统提示您删除 IPAM 时，选择级联删除。这将在删除 IPAM 之前，删除 IPAM 中的所有作用域和池。

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. 输入删除并选择删除。
7. 使用 AWS Organizations 管理账户登录 IPAM 控制台，选择设置，然后删除委派的管理员账户。
8. （可选）将 IPAM 与 AWS Organizations 集成时，[IPAM 会自动在每个成员账户中创建一个服务相关角色](#)。使用每个 AWS Organizations 成员账户，登录 IAM 并删除每个成员账户中的 AWSServiceRoleForIPAM 服务相关角色。
9. 清理已完成。

教程：使用 AWS CLI 创建 IPAM 和池

按照本教程中的步骤使用 AWS CLI 创建 IPAM、创建 IP 地址池并使用 IPAM 池中的 CIDR 分配 VPC。

以下示例显示了池结构的层次结构，您可以通过遵照本部分中的步骤来创建这些结构：

- IPAM 在 AWS 区域 1、AWS 区域 2 中运营

- 私有范围
 - 顶级池
 - AWS 区域 2 中的区域池
 - 开发池
 - VPC 的分配

Note

在本部分中，您将创建一个 IPAM。默认情况下，您只能创建一个 IPAM。有关更多信息，请参阅 [IPAM 的配额](#)。如果您已委派了 IPAM 账户并创建了 IPAM，则可以跳过步骤 1 和步骤 2。

内容

- [步骤 1：在企业中启用 IPAM](#)
- [步骤 2：创建 IPAM](#)
- [步骤 3：创建 IPv4 地址池](#)
- [步骤 4：向顶级池预置 CIDR](#)
- [步骤 5。使用来自顶级池的 CIDR 创建区域池](#)
- [步骤 6：向区域池预置 CIDR](#)
- [第 7 步。创建 RAM 共享以启用跨账户的 IP 分配](#)
- [步骤 8：创建 VPC](#)
- [第 9 步。清理](#)

步骤 1：在企业中启用 IPAM

此为可选步骤。完成此步骤以在企业中启用 IPAM，然后使用 AWS CLI 配置委派的 IPAM。有关 IPAM 账户角色的更多信息，请参阅 [将 IPAM 与 AWS Organization 中的账户集成](#)。

此请求必须来自 AWS Organizations 管理账户。运行以下命令时，请确保您使用的角色具有允许执行以下操作的 IAM policy：

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

- `iam:CreateServiceLinkedRole`

```
aws ec2 enable-ipam-organization-admin-account --region us-east-1 --delegated-admin-account-id 111111111111
```

您应看到以下输出，它表明启用成功。

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

步骤 2：创建 IPAM

按照本部分中的步骤创建 IPAM 并查看有关创建范围的其他信息。在后面的步骤中创建池并为这些池预置 IP 地址范围时，您将使用此 IPAM。

Note

允许区域选项确定了 IPAM 池可用于的哪些 AWS 区域。有关这些运营区域的更多信息，请参阅 [创建 IPAM](#)。

要使用 AWS CLI 创建 IPAM

1. 运行以下命令以创建 IPAM 实例。

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

创建 IPAM 时，AWS 自动执行以下操作：

- 为 IPAM 返回全局唯一的资源 ID (IpamId)。
- 创建默认的公有范围 (PublicDefaultScopeId) 和默认的私有范围 (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. 运行以下命令以查看与范围相关的其他信息。公有范围适用于将通过公共互联网访问的 IP 地址。私有范围适用于不通过公共互联网访问的 IP 地址。

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

在输出中，您将看到可用的范围。您将在下一步中使用私有范围 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
    }
]
}

```

步骤 3：创建 IPv4 地址池

按照本部分中的步骤创建 IPv4 地址池。

Important

您不会在这个顶级池上使用 `--locale` 选项。稍后您将在区域池中设置区域设置选项。区域设置是您希望有一个池可用于 CIDR 分配的区域。由于未在顶级池上设置区域设置，该区域设置将为原定设置 `None`。如果池的区域设置为 `None`，则任何 AWS 区域的 VPC 资源都无法使用该池。您只能在池中手动分配 IP 地址空间以预订空间。

使用 AWS CLI 为您的所有 AWS 资源创建 IPv4 地址池

1. 运行以下命令以创建 IPv4 地址池。请使用您在上一步中创建的 IPAM 的私有范围的 ID。

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

在输出中，您将看到池的 `create-in-progress` 的状态。

```

{
  "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. 运行以下命令，直到您在输出中看到 `create-complete` 的状态。

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

下面的示例输出显示正确的状态。

```
{
  "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"
    }
  ]
}
```

步骤 4：向顶级池预置 CIDR

按照本部分中的步骤向顶级池预置 CIDR，然后验证是否已预置 CIDR。有关更多信息，请参阅 [将 CIDR 预置到池](#)。

使用 AWS CLI 向池预置 CIDR 块

1. 请运行以下命令以预置 CIDR。

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

在输出中，您可以验证预置的状态。

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

2. 运行以下命令，直到您在输出中看到 `provisioned` 的状态。

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

下面的示例输出显示正确的状态。

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

步骤 5。使用来自顶级池的 CIDR 创建区域池

创建 IPAM 池时，该池默认情况下属于 IPAM 的 AWS 区域。创建 VPC 时，VPC 从中进行提取的池必须与 VPC 位于同一个区域中。创建池时，您可以使用 `--locale` 选项使池可用于 IPAM 的区域之外的区域中的服务。按照本部分中的步骤在另一个区域设置中创建区域池。

要使用 AWS CLI 通过来自上一个池的 CIDR 创建池

1. 运行以下命令以创建池并插入带有前一个池中已知可用 CIDR 的空间。

```
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
```

在输出中，您将看到创建的池的 ID。在下一步骤中，您需要用到此 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. 运行以下命令，直到您在输出中看到 create-complete 的状态。

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

在输出中，您可以看到您在 IPAM 中拥有的池。在本教程中，我们创建了一个顶级池和一个区域池，所以您会看到这两个池。

```
{  
  "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"
    }
]
}

```

步骤 6：向区域池预置 CIDR

按照本部分中的步骤向池分配 CIDR 块，并验证它是否已成功预置。

要使用 AWS CLI 将 CIDR 块分配到区域池

1. 请运行以下命令以预置 CIDR。

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

在输出中，您将看到池的状态。

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

2. 运行以下命令，直到您在输出中看到 `provisioned` 的状态。

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

下面的示例输出显示正确的状态。

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

3. 运行以下命令查询顶级池以查看分配。区域池被看作是顶级池中的分配。

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

在输出中，您将区域池看作是顶级池中的分配。

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

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

第 7 步。创建 RAM 共享以启用跨账户的 IP 分配

此为可选步骤。只有完成 [将 IPAM 与 AWS Organization 中的账户集成](#) 后，您才能完成此步骤。

当您创建 IPAM 池 AWS RAM 共享时，它将支持跨账户分配 IP。RAM 共享仅在主 AWS 区域中可用。请注意，您可以在与 IPAM 相同的区域中创建此共享，而不能在池的本地区域中。IPAM 资源上的所有管理操作都是通过您 IPAM 所在的主区域进行的。本教程中的示例为单个池创建单个共享，但是您可以将多个池添加到单个共享中。有关更多信息，包括必须输入的选项的说明，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。

使用以下命令创建资源共享。

```
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
```

输出表明，该池已创建。

```
{
  "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
  }
}
```

步骤 8：创建 VPC

运行以下命令以创建 VPC 并将 CIDR 块从新创建的 IPAM 中的池分配给 VPC。

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

输出表明，VPC 已创建。

```
{
  "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
  }
}
```

第 9 步。清理

按照本部分中的步骤删除您在本教程中创建的 IPAM 资源。

1. 删除 VPC。

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

2. 删除 IPAM 池 RAM 共享。

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

3. 从区域池中取消预置池 CIDR。

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

4. 从顶级池中取消预置池 CIDR。

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

5. 删除 IPAM

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

教程：使用 AWS CLI 查看 IP 地址历史记录

本部分中的场景将向您展示如何使用 AWS CLI 分析和审计 IP 地址使用情况。有关使用 AWS CLI 的一般信息，请参阅 AWS 命令行界面用户指南中的[使用 AWS CLI](#)。

内容

- [概述](#)
- [场景](#)

概述

IPAM 会自动将您的 IP 地址监控数据最多保留三年。您可以使用历史数据来分析和审核网络安全和路由策略。您可以为以下类型的资源搜索历史见解：

- VPC
- VPC 子网
- 弹性 IP 地址
- 正在运行的 EC2 实例
- 连接到实例的 EC2 网络接口

⚠ Important

尽管 IPAM 不会监控 Amazon EC2 实例或挂载到实例的 EC2 网络接口，但您可以使用搜索 IP 历史记录功能，来搜索 EC2 实例和网络接口 CIDR 上的历史数据。

📘 Note

- 本教程中的命令必须使用拥有 IPAM 的账户和托管 IPAM 的 AWS 区域运行。
- CIDR 更改的记录会在定期快照中拾取，这意味着记录出现或更新可能需要一些时间，SampledStartTime 和 SampledEndTime 的值可能与实际发生时间不同。

场景

本部分中的场景将向您展示如何使用 AWS CLI 分析和审计 IP 地址使用情况。有关本教程中提到的采样结束时间和开始时间等值的更多信息，请参阅 [查看 IP 地址历史记录](#)。

场景 1：2021 年 12 月 27 日上午 1:00 和晚上 9:00 (UTC) 之间有哪些资源与 **10.2.1.155/32** 关联？

1. 运行如下命令：

```
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. 查看分析结果。在下面的示例中，CIDR 在一段时间内分配给网络接口和 EC2 实例。请注意，没有 SampledEndTime 值表示记录仍处于活动状态。有关以下输出中显示的值的更多信息，请参阅 [查看 IP 地址历史记录](#)。

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

```

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

```

如果网络接口连接到的实例的拥有者 ID 与网络接口的所有者 ID 不同（如 NAT 网关、VPC 中的 Lambda 网络接口和其他 AWS 服务的情况），则 ResourceOwnerId 为 amazon-aws，而不是网络接口拥有者的账户 ID。以下示例显示了与 NAT 网关关联的 CIDR 的记录：

```

{
  "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"
    }
  ]
}

```

场景 2：2021 年 12 月 1 日至 2021 年 12 月 27 日 (UTC) 有哪些资源与 **10.2.1.0/24** 关联？

1. 运行如下命令：

```
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. 查看分析结果。在下面的示例中，CIDR 在一段时间内分配给子网和 VPC。请注意，没有 `SampledEndTime` 值表示记录仍处于活动状态。有关以下输出中显示的值的更多信息，请参阅 [查看 IP 地址历史记录](#)。

```
{  
  "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"  
    }  
  ]  
}
```

场景 3：2021 年 12 月 1 日至 2021 年 12 月 27 日 (UTC) 有哪些资源与 **2605:9cc0:409::/56** 关联？

1. 运行以下命令，其中 `--region` 是指 IPAM 主区域：

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

2. 查看分析结果。在下面的示例中，在 IPAM 主区域以外的区域，CIDR 在一段时间内分配给两个不同的 VPC。请注意，没有 `SampledEndTime` 值表示记录仍处于活动状态。有关以下输出中显示的值的更多信息，请参阅 [查看 IP 地址历史记录](#)。

```
{
  "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"
    }
  ]
}
```

场景 4：在过去的 24 小时内，有哪些资源与 **10.0.0.0/24** 关联（假设当前时间是 2021 年 12 月 27 日午夜 (UTC)）？

1. 运行如下命令：

```
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. 查看分析结果。在下面的示例中，CIDR 已在一段时间内分配给多个子网和 VPC。请注意，没有 `SampledEndTime` 值表示记录仍处于活动状态。有关以下输出中显示的值的更多信息，请参阅 [查看 IP 地址历史记录](#)。

```
{
  "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"
    }
]
}

```

场景 5：当前有哪些资源与 **10.2.1.155/32** 关联？

1. 运行如下命令：

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

2. 查看分析结果。在下面的示例中，CIDR 在一段时间内分配给网络接口和 EC2 实例。请注意，没有 `SampledEndTime` 值表示记录仍处于活动状态。有关以下输出中显示的值的更多信息，请参阅 [查看 IP 地址历史记录](#)。

```

{
  "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"
    }
  ]
}

```

场景 6：当前有哪些资源与 **10.2.1.0/24** 关联？

1. 运行如下命令：

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

- 查看分析结果。在下面的示例中，CIDR 在一段时间内分配给 VPC 和子网。只返回与此 /24 CIDR 完全匹配的结果，而不是 /24 CIDR 中的所有 /32。请注意，没有 SampledEndTime 值表示记录仍处于活动状态。有关以下输出中显示的值的更多信息，请参阅 [查看 IP 地址历史记录](#)。

```

{
  "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"
    }
  ]
}
```

场景 7：当前有哪些资源与 **54.0.0.9/32** 关联？

在此示例中，54.0.0.9/32 将分配给不属于与 IPAM 集成的 AWS 企业的弹性 IP 地址。

1. 运行如下命令：

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

2. 由于 54.0.0.9/32 分配给不属于此示例中与 IPAM 集成的 AWS 企业的弹性 IP 地址，因此不会返回任何记录。

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

教程：自带 ASN 到 IPAM 中

如果您的应用程序使用的是合作伙伴或客户允许在其网络中列出的可信 IP 地址和自治系统号 (ASN)，则无需合作伙伴或客户更改允许列表，即可在 AWS 中运行这些应用程序。

自治系统编号 (ASN) 是一个全球唯一的号码，允许通过互联网识别一组网络，并使用[边界网关协议](#)与其他网络动态交换路由数据。例如，互联网服务提供商 (ISP) 使用 ASN 来识别网络流量来源。并非所有组织都自己购买 ASN，但对于购买了 ASN 的组织，它们可以将自己的 ASN 带到 AWS。

通过自带自治系统编号 (BYOASN)，您能够使用自己的公有 ASN (而不是 AWS ASN) 来公开发布自己引入 AWS 的 IPv4 或 IPv6 地址。当您使用 BYOASN 时，来自您的 IP 地址的流量会携带您的 ASN (而不是 AWS ASN)，并且根据您的 IP 地址和 ASN 允许列出的流量的客户或合作伙伴可以访问您的工作负载。

Important

- 使用您的 IPAM 主区域的 IPAM 管理员账户完成本教程。

- 本教程假定您拥有想要带入 IPAM 的公共 ASN，并且您已经将 BYOIP CIDR 带入 AWS 并配置到公有范围内的池中。您可以随时将 ASN 带入 IPAM，但要使用该 ASN，您必须关联已带入 AWS 账户的 CIDR。本教程假定您已完成这一操作。有关更多信息，请参阅 [教程：将 IP 地址带入 IPAM](#)。
- 您可以即时在广告自己的 ASN 或 AWS ASN 之间切换，但每小时只能从 AWS ASN 更改为自己的 ASN 一次。
- 如果您的 BYOIP CIDR 当前已广告，则无需将其从广告中撤回即可与您的 ASN 关联。

ASN 的载入先决条件

要完成本教程，您需要做以下准备：

- 您的 2 字节或 4 字节的公有 ASN。
- 如果您已经通过 [教程：将 IP 地址带入 IPAM](#) 将一个 IP 地址范围带到 AWS，那么您需要该 IP 地址的 CIDR 范围。您还需要一个私有密钥。您可以使用在将 IP 地址 CIDR 范围带到 AWS 时创建的私有密钥，也可以按照《Amazon EC2 用户指南》的 [创建私有密钥并生成 X.509 证书](#) 中所述创建新的私有密钥。
- 当您通过 [教程：将 IP 地址带入 IPAM](#) 将 IPv4 或 IPv6 地址范围引入 AWS 时，可以 [创建 X.509 证书](#)，然后将 [X.509 证书上传到 RIR 中的 RDAP 记录](#)。您必须将创建的同一证书上传到 ASN 的 RIR 中的 RDAP 记录中。请务必在编码部分前后包含 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE----- 字符串。所有这些内容必须都在单个长线上。更新 RDAP 的过程取决于您的 RIR：
 - 对于 ARIN，使用 [客户经理门户](#)，通过“修改 ASN”选项在代表您的 ASN 的“网络信息”对象的“公共注释”部分中添加证书。请勿将其添加到您组织的注释部分。
 - 对于 RIPE，将证书作为新的“descr”字段添加到代表您的 ASN 的“aut-num”对象。通常可在 [RIPE 数据库门户](#) 的“我的资源”部分中了解到相关信息。请勿将其添加到您所在组织的注释部分或“aut-num”对象的“备注”字段中。
 - 对于 APNIC，通过电子邮件将证书发送到 helpdesk@apnic.net，以手动将其添加到您的 ASN 的“备注”字段中。请以 ASN 的 APNIC 授权联系人身份发送电子邮件。
- 将 IP 地址范围带入 IPAM 时，可创建一个 ROA 来验证自己是否控制了带入 IPAM 的 IP 地址空间。除了该 ROA 之外，您的 RIR 中还必须有第二个 ROA，其中包含要带入 IPAM 的 ASN。如果 RIR 中没有 ASN 的第二个 ROA，请完成 [3. 在 RIR 中创建 ROA 对象](#)。忽略其他步骤。

教程步骤

使用 AWS 管理控制台或 AWS CLI，完成以下步骤。

AWS Management Console

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在左侧导航窗格中，选择 IPAM。
3. 选择您的 IPAM。
4. 选择 BYOASN 选项卡，然后选择预置 BYOASN。
5. 输入 ASN。接下来，消息字段会自动填充您在下一步中需要登录的消息。
 - 消息的格式如下，其中 ACCOUNT 是您的 AWS 账号，ASN 是您带到 IPAM 的 ASN，YYYYMMDD 是消息的到期日期（默认为下个月的最后一天）。示例：

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

6. 复制该信息，并根据需要使用您自己的值替换到期日期。
7. 使用私有密钥对消息进行签名。示例：

```
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. 在签名下，输入签名。
9. （可选）要预置另一个 ASN，请选择预置其他 ASN。您最多可以预置 5 个 ASN。要增加此配额，请参阅[IPAM 的配额](#)。
10. 选择预置。
11. 在 BYOASN 选项卡中查看预置过程。等待状态从待预置更改为已预置。处于预置失败状态的 BYOASN 将在 7 天后自动删除。成功预置 ASN 后，您可以将其与 BYOIP CIDR 关联。
12. 在左侧导航窗格中，选择池。
13. 选择您的公有范围。有关范围的更多信息，请参阅[IPAM 的工作原理](#)。
14. 选择已为其预置 BYOIP CIDR 的区域池。该池必须将服务设置为 EC2，并且必须选择一个区域设置。
15. 选择 CIDR 选项卡，然后选择一个 BYOIP CIDR。
16. 选择操作 > 管理 BYOASN 关联。

17. 在已关联的 BYOASN 下，选择您带入 AWS 的 ASN。如果您有多个 ASN，则可以将多个 ASN 关联到 BYOIP CIDR。您可以将尽可能多的 ASN 关联到 IPAM。请注意，默认情况下，您最多可以将 5 个 ASN 带入 IPAM。有关更多信息，请参阅 [IPAM 的配额](#)。
18. 选择关联。
19. 等待 ASN 关联完成。在 ASN 成功与 BYOIP CIDR 关联后，您可以再次广告 BYOIP CIDR。
20. 选择池 CIDR 选项卡。
21. 选择 BYOIP CIDR，然后选择操作 > 广告。接下来，系统会显示您的 ASN 选项：Amazon ASN 和您带入 IPAM 的所有 ASN。
22. 选择您带入 IPAM 的 ASN，然后选择广告 CIDR。这样一来，将广告 BYOIP CIDR，并且广告列中的值将从“已撤回”变为“已刊登广告”。自治系统编号列显示与 CIDR 关联的 ASN。
23. （可选）如果您决定要将 ASN 关联更改回 Amazon ASN，选择 BYOIP CIDR，然后再次选择操作 > 广告。这一次我们选择 Amazon ASN。您可以随时换回 Amazon ASN，但每小时只能更改为自定义 ASN 一次。

本教程已完成。

清理

1. 解除 ASN 与 BYOIP CIDR 的关联
 - 要从广告中撤回 BYOIP CIDR，在公有范围的池中，选择 BYOIP CIDR，然后选择操作 > 撤消广告。
 - 要解除 ASN 与 CIDR 的关联，请选择操作 > 管理 BYOASN 关联。
2. 取消预置 ASN
 - 要取消预置 ASN，在“BYOASN”选项卡中，选择 ASN，然后选择取消预置 ASN。接下来，ASN 将被取消预置。处于已取消预置状态的 BYOASN 将在 7 天后自动删除。

清理完成。

Command line

1. 通过包含您的 ASN 和授权消息来预置您的 ASN。签名是用您的私有密钥签署的消息。

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

2. 描述您的 ASN 以跟踪预置过程。如果请求成功，您应该会在几分钟后看到预置状态被设置为已预置。

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

3. 将您的 ASN 与 BYOIP CIDR 关联。您希望从中广告的任何自定义 ASN 都必须先与您的 CIDR 关联。

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

4. 描述您的 CIDR 以跟踪关联流程。

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

5. 使用您的 ASN 广告您的 CIDR。如果 CIDR 已广告，则会将源于 Amazon 的 ASN 换成您的 ASN。

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

6. 描述您的 CIDR 以查看 ASN 状态从已关联更改为已刊登广告。

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

本教程已完成。

清理

1. 请执行以下操作之一：

- 要仅撤回您的 ASN 广告并重新使用 Amazon ASN，同时保留已广告的 CIDR，您必须使用 `asn` 参数的特殊 AWS 值调用 `advertise-byoip-cidr`。您可以随时换回 Amazon ASN，但每小时只能更改为自定义 ASN 一次。

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

- 要同时撤回您的 CIDR 和 ASN 广告，你可以调用 `withdraw-byoip-cidr`。

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

2. 要清理您的 ASN，您必须先取消其与 BYOIP CIDR 的关联。

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

- 您的 ASN 与已关联的所有 BYOIP CIDR 取消关联后，就可以取消其预置。

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

- 删除所有 ASN 关联后，也可以取消预置 BYOIP CIDR。

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

- 确认取消预置。

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

清理已完成。

教程：将 IP 地址带入 IPAM

本部分中的教程将引导您完成将公有 IP 地址空间带到 AWS，并使用 IPAM 管理空间的过程。

使用 IPAM 管理公有 IP 地址空间具有以下益处：

- 提高整个企业的公有 IP 地址利用率：您可以使用 IPAM 跨 AWS 账户共享 IP 地址空间。如果不使用 IPAM，您将无法跨 AWS Organizations 账户共享您的公有 IP 空间。
- 简化将公有 IP 空间带到 AWS 的过程：您可以使用 IPAM 一次性载入公有 IP 地址空间，然后使用 IPAM 将公有 IP 跨区域分配到 EC2 实例和[应用程序负载均衡器](#)等资源。如果没有 IPAM，您必须为每个 AWS 区域登记您的公有 IP。

内容

- [验证域控制权](#)
- [使用 AWS 管理控制台和 AWS CLI 自带 IP 到 IPAM 中](#)
- [仅使用 AWS CLI 自带 IP CIDR 到 IPAM 中](#)
- [使用 IPAM 自带 IP 到 CloudFront](#)

验证域控制权

在将 IP 地址范围引入 AWS 之前，您必须使用本节中所述的一个选项来验证自己是否控制了 IP 地址空间。之后，如果将 IP 地址范围引入 AWS，AWS 会验证您是否控制了 IP 地址范围。该验证可确保客户无法使用属于他人的 IP 范围，防止出现路由和安全问题。

您可以通过两种方法来验证自己是否控制了相应范围：

- X.509 证书：如果 IP 地址范围是在支持 RDAP 的互联网注册机构（例如 ARIN、RIPE 和 APNIC）注册，您可以使用 X.509 证书验证域的所有权。
- DNS TXT 记录：无论互联网注册机构是否支持 RDAP，您都可以使用验证令牌和 DNS TXT 记录来验证域的所有权。

内容

- [使用 X.509 证书验证域](#)
- [使用 DNS TXT 记录验证域](#)

使用 X.509 证书验证域

本节旨在介绍在将 IP 地址范围引入 IPAM 之前，如何使用 X.509 证书验证域。

使用 X.509 证书验证域

1. 完成《Amazon EC2 用户指南》中的 [Amazon EC2 中 BYOIP 的先决条件](#) 中的三个步骤。

Note

创建 ROA 时，对于 IPv4 CIDR，您必须将 IP 地址前缀的最大长度设置为 /24。对于 IPv6 CIDR，如果要将它们添加到可传播池中，IP 地址前缀的最大长度必须为 /48。这可以确保您有充分的灵活性来跨 AWS 区域划分您的公有 IP 地址。IPAM 强制执行您设置的最大长度。最大长度是您对此路由允许的最小前缀长度公告。例如，如果您通过将最大长度设置为 /20 将 AWS CIDR 块带入 /24 中，您可以根据自己喜欢的方式划分较大的块（例如 /21、/22 或 /24）并将这些较小的 CIDR 块分发到任何区域。如果您要将最大长度设置为 /23，您将无法划分和传播来自较大块的 /24。另请注意，/24 是最小的 IPv4 块，/48 是您可以从区域向互联网广告的最小 IPv6 块。

2. 仅完成《Amazon EC2 用户指南》中在 [AWS 中预置公开发布的地址范围](#) 下的步骤 1 和 2，先不预置地址范围（步骤 3）。保存 text_message 和 signed_message。本过程后面部分需要使用它们。

完成上述步骤后，继续[使用 AWS 管理控制台和 AWS CLI 自带 IP 到 IPAM 中](#)或[仅使用 AWS CLI 自带 IP CIDR 到 IPAM 中](#)。

使用 DNS TXT 记录验证域

在将 IP 地址范围引入 IPAM 之前，请先完成本节中的步骤，使用 DNS TXT 记录验证自己的域。

您可以使用 DNS TXT 记录来验证自己是否控制了公有 IP 地址范围。DNS TXT 记录是一种包含域名信息的 DNS 记录。该功能让您能够使用在任何互联网注册机构（例如 JPNIC、LACNIC 和 AFRINIC）注册的 IP 地址，而不仅仅是那些支持基于 RDAP（注册数据访问协议）记录的（例如 ARIN、RIPE 和 APNIC）的注册机构。

Important

要想继续操作，必须先免费或高级套餐中创建了 IPAM。如果没有 IPAM，请先完成[创建 IPAM](#)。

内容

- [步骤 1：创建 ROA（若没有）](#)
- [步骤 2：创建验证令牌](#)
- [步骤 3：设置 DNS 区域和 TXT 记录](#)

步骤 1：创建 ROA（若没有）

必须在区域互联网注册机构（RIR）中为自己要公开发布的 IP 地址范围创建路由来源授权（ROA）。如果 RIR 中没有 ROA，请先完成 [《Amazon EC2 用户指南》中的 3. 在 RIR 中创建 ROA 对象](#)。忽略其他步骤。

您可以引入的最具体 IPv4 地址范围是 /24。对于公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /48；对于不公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /60。

步骤 2：创建验证令牌

验证令牌是 AWS 生成的随机值，可用于证明对外部资源的控制权。例如，当您将 IP 地址范围引入 AWS (BYOIP) 时，可以使用验证令牌来验证自己是否控制了公有 IP 地址范围。

完成本节中的步骤，创建好验证令牌；在本教程的后续步骤中，您需要使用该令牌才能将自己的 IP 地址范围引入 IPAM。请按照以下说明，在 AWS 控制台或 AWS CLI 中继续操作。

AWS Management Console

创建验证令牌

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在 AWS 管理控制台中，选择要在其中创建 IPAM 的 AWS 区域。
3. 在左侧导航窗格中，选择 IPAM。
4. 选择 IPAM，然后选择验证令牌选项卡。
5. 选择创建验证令牌。
6. 创建令牌后，让该浏览器选项卡保持打开状态。下一步会用到令牌值和令牌名称，而后续步骤会用到令牌 ID。

请注意以下几点：

- 创建验证令牌后，您可以在 72 小时内将该令牌重复用于从 IPAM 预置的多个 BYOIP CIDR。若想在 72 小时后预置更多 CIDR，必须创建新令牌。
- 最多可创建 100 个令牌。如果令牌数达到上限，请删除过期令牌。

Command line

- 请求 IPAM 使用 [create-ipam-external-resource-verification-token](#) 创建一个可用于配置 DNS 的验证令牌：

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

该指令会返回一个 IpamExternalResourceVerificationTokenId 和带有 TokenName 和 TokenValue 的令牌，以及该令牌的到期时间 (NotAfter)。

```
{
```

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

请注意以下几点：

- 创建验证令牌后，您可以在 72 小时内将该令牌重复用于从 IPAM 预置的多个 BYOIP CIDR。若想在 72 小时后预置更多 CIDR，必须创建新令牌。
- 使用 [describe-ipam-external-resource-verification-tokens](#) 可以查看令牌。
- 最多可创建 100 个令牌。如果令牌数达到上限，则可以使用 [delete-ipam-external-resource-verification-token](#) 删除过期令牌。

步骤 3：设置 DNS 区域和 TXT 记录

完成本部分中的步骤，设置好 DNS 域和 TXT 记录。如果未使用 Route53 作为 DNS，则按照 DNS 提供商提供的文档设置好 DNS 区域并添加 TXT 记录。

如果使用的是 Route53，请注意以下几点：

- 要在 AWS 控制台中创建反向查找区域，请参阅《Amazon Route 53 Developer Guide》中的 [Creating a public hosted zone](#) 或使用 AWS CLI 命令 [create-hosted-zone](#)。
- 要在 AWS 控制台的反向查找区域中创建记录，请参阅《Amazon Route 53 Developer Guide》中的 [Creating records by using the Amazon Route 53 console](#) 或使用 AWS CLI 命令 [change-resource-record-sets](#)。
- 创建好托管区后，将托管区从 RIR 委托给 Route53 提供的域名服务器（例如 [LACNIC](#) 或 [APNIC](#)）。

无论使用的是 Route53 还是其他 DNS 提供商，在设置 TXT 记录时，都需要注意以下几点：

- 记录名称应为令牌名称。

- 记录类型应为 TXT。
- ResourceRecord 值应为令牌值。

示例：

- 名称：86950620.113.0.203.in-addr.arpa
- 类型：TXT
- ResourceRecords 值：a34597c3-5317-4238-9ce7-50da5b6e6dc8

其中：

- 86950620 为验证令牌名称。
- 113.0.203.in-addr.arpa 为反向查找区域的名称。
- TXT 为记录类型。
- a34597c3-5317-4238-9ce7-50da5b6e6dc8 为验证令牌值。

Note

根据要通过 BYOIP 引入 IPAM 的前缀大小，必须在 DNS 中创建一条或多条身份验证记录。这些身份验证记录的记录类型为 TXT，且必须放置在前缀本身或其父前缀的反向区域中。

- 对于 IPv4，身份验证记录需要与构成前缀的八位字节边界的范围保持一致。
 - 示例
 - 对于 198.18.123.0/24（已按八位字节边界对齐），您需要创建一条身份验证记录：
 - `token-name.123.18.198.in-addr.arpa. IN TXT "token-value"`
 - 对于 198.18.12.0/22（本身未按八位字节边界对齐），您需要创建四条身份验证记录。这些记录必须涵盖子网 198.18.12.0/24、198.18.13.0/24、198.18.14.0/24 和 198.18.15.0/24（这些子网均按八位字节边界对齐）。相应的 DNS 条目必须是：
 - `token-name.12.18.198.in-addr.arpa. IN TXT "token-value"`
 - `token-name.13.18.198.in-addr.arpa. IN TXT "token-value"`
 - `token-name.14.18.198.in-addr.arpa. IN TXT "token-value"`
 - `token-name.15.18.198.in-addr.arpa. IN TXT "token-value"`
 - 对于 198.18.0.0/16（已按八位字节边界对齐），您需要创建一条身份验证记录：

- `token-name.18.198.in-addr.arpa. IN TXT "token-value"`
- 对于 IPv6，身份验证记录需要与构成前缀的半字节边界的范围保持一致。有效的半字节数值包括 32、36、40、44、48、52、56 和 60。
- 示例
 - 对于 2001:0db8::/40 (已按半字节边界对齐)，您需要创建一条身份验证记录：
 - `token-name.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "token-value"`
 - 对于 2001:0db8:80::/42 (本身未按半字节边界对齐)，您需要创建四条身份验证记录。这些记录必须涵盖子网 2001:db8:80::/44、2001:db8:90::/44、2001:db8:a0::/44 和 2001:db8:b0::/44 (这些子网均按半字节边界对齐)。相应的 DNS 条目必须是：
 - `token-name.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "token-value"`
 - `token-name.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "token-value"`
 - `token-name.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
 - `token-name.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
 - 对于非公开发布范围 2001:db8:0:1000::/54 (该范围本身未按半字节边界对齐)，您需要创建四条身份验证记录。这些记录必须涵盖子网 2001:db8:0:1000::/56、2001:db8:0:1100::/56、2001:db8:0:1200::/56 和 2001:db8:0:1300::/56 (这些子网均按半字节边界对齐)。相应的 DNS 条目必须是：
 - `token-name.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
 - `token-name.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
 - `token-name.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
 - `token-name.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
- 要验证 token-name 和 ip6.arpa 字符串之间十六进制数字的正确数量，请将该数量乘以四。结果应与前缀长度一致。例如，对于 /56 前缀，应有 14 个十六进制数字。

完成上述步骤后，继续[使用 AWS 管理控制台和 AWS CLI 自带 IP 到 IPAM 中](#)或[仅使用 AWS CLI 自带 IP CIDR 到 IPAM 中](#)。

使用 AWS 管理控制台和 AWS CLI 自带 IP 到 IPAM 中

自带 IP (BYOIP) 到 IPAM 允许您在 AWS 中使用组织现有的 IPv4 和 IPv6 地址范围。这使您能够在自己的 IP 地址空间下将本地和云环境统一，从而保持一致的品牌形象、提高网络性能、增强安全性并简化管理。

按照以下步骤，使用 AWS 管理控制台和 AWS CLI 将 IPv4 或 IPv6 CIDR 带入 IPAM 中。

Note

开始操作之前，必须先[验证域控制权](#)。

将 IPv4 地址范围设置为 AWS 后，您可以使用该范围内的所有 IP 地址，包括第一个地址（网络地址）和最后一个地址（广播地址）。

内容

- [使用 AWS 管理控制台和 AWS CLI 自带 IPv4 CIDR 到 IPAM 中](#)
- [使用 AWS 管理控制台自带 IPv6 CIDR 到 IPAM 中](#)

使用 AWS 管理控制台和 AWS CLI 自带 IPv4 CIDR 到 IPAM 中

按照以下步骤将 IPv4 CIDR 带入 IPAM 中，然后使用 AWS 管理控制台和 AWS CLI 分配弹性 IP 地址 (EIP)。

Important

- 本教程假定您已完成以下部分中的步骤：
 - [将 IPAM 与 AWS Organization 中的账户集成](#).
 - [创建 IPAM](#).
- 本教程的每个步骤都必须由以下三个 AWS Organizations 账户之一完成：
 - 管理账户。
 - [将 IPAM 与 AWS Organization 中的账户集成](#) 中配置为 IPAM 管理员的成员账户。在本教程中，此账户将被称为 IPAM 账户。
 - 将从 IPAM 池中分配 CIDR 的企业中的成员账户。在本教程中，此账户将被称为成员账户。

内容

- [第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色](#)
- [步骤 2：创建顶级 IPAM 池](#)
- [步骤 3：在顶级池中创建区域池](#)
- [步骤 4：传播 CIDR](#)
- [步骤 5。共享区域池](#)
- [步骤 6：从池中分配弹性 IP 地址](#)
- [步骤 7：将弹性 IP 地址与 EC2 实例相关联](#)
- [步骤 8：清除](#)
- [步骤 6 的替代方案](#)

第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色

要以单个 AWS 用户的身份完成本教程，您可以使用 AWS CLI 命名配置文件在 IAM 角色之间切换。[命名配置文件](#)是您在将 `--profile` 选项与 AWS CLI 结合使用时引用的设置和凭证集合。有关如何为 AWS 账户创建 IAM 角色和命名配置文件的更多信息，请参阅[在 AWS CLI 中使用 IAM 角色](#)。

为您将在本教程中使用的三个 AWS 账户分别创建一个角色和一个命名配置文件：

- 为 AWS Organizations 管理账户创建名为 `management-account` 的配置文件。
- 为配置为 IPAM 管理员的 AWS Organizations 成员账户创建名为 `ipam-account` 的配置文件。
- 为将从 IPAM 池中分配 CIDR 的企业中的 AWS Organizations 成员账户创建名为 `member-account` 的配置文件。

创建 IAM 角色和命名配置文件后，请返回本页面并转至下一步。在本教程的其余部分中，您将注意到示例 AWS CLI 命令会将 `--profile` 选项与其中一个命名配置文件一起使用，以指示哪个账户必须运行该命令。

步骤 2：创建顶级 IPAM 池

完成本部分中的步骤创建顶级 IPAM 池。


此步骤必须由 IPAM 账户完成。

如需创建池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。

2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，创建池时，默认的私有范围被选中。选择公有范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 选择创建池。
5. (可选) 添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 范围。
7. 在地址系列下，选择 IPv4。
8. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
9. 在区域设置下，选择无。

IPAM 与 BYOIP 集成要求在将用于 BYOIP CIDR 的任何一个池上设置区域设置。由于我们将创建一个其中包含一个区域池的顶级 IPAM 池，并且我们将为区域池中的弹性 IP 地址分配空间，因此您将在区域池中设置区域设置，而不是在顶级池中。在后面的步骤中创建区域池时，您将区域设置添加到区域池中。

 Note

如果您只创建单个池而不是其中包含区域池的顶级池，则需要为此池选择一个区域设置，以便该池可用于分配。

10. 在公有 IP 来源下，选择 BYOIP。
11. 在要预置的 CIDR 下，执行下列某项操作：
 - 如果 [使用 X.509 证书验证域控制权](#)，则必须包含 CIDR 和 BYOIP 消息以及在该步骤中创建的证书签名，以便我们验证您是否控制了公共空间。
 - 如果 [使用 DNS TXT 记录验证域控制权](#)，则必须包含 CIDR 和 IPAM 消息以及在该步骤中创建的验证令牌，以便我们验证您是否控制了公共空间。

请注意，将 IPv4 CIDR 预置到顶级池中的资源池时，您可以预置的最低 IPv4 CIDR 为 /24；不允许使用更具体的 CIDR (例如 /25)。

⚠ Important

虽然大多数预配置将在两小时内完成，但对于公开发布的范围，完成预配置过程可能需要长达一周的时间。

12. 将配置此池的分配规则设置保持未选中状态。
13. (可选) 为池选择 Tags (标签) 。
14. 选择创建池。

在继续之前，请确保已预置此 CIDR。您可以在池详细信息页面的 CIDR 选项卡中查看资源调配状态。

步骤 3：在顶级池中创建区域池

在顶级池中创建区域池。IPAM 与 BYOIP 集成要求在将用于 BYOIP CIDR 的任何一个池上设置区域设置。在本部分中创建区域池时，您将区域设置添加到区域池中。Locale 必须是创建 IPAM 时配置的其中一个操作区域的一部分。例如，区域设置为 us-east-1 意味着 us-east-1 必须是 IPAM 的操作区域。区域设置为 us-east-1-scl-1 (用于本地区域的网络边界组) 意味着 IPAM 的操作区域必须为 us-east-1。

此步骤必须由 IPAM 账户完成。

要在顶级池中创建区域池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池) 。
3. 默认情况下，创建池时，默认的私有范围被选中。如果您不想使用默认的私有范围，请从内容窗格顶部的下拉菜单中选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 选择创建池。
5. (可选) 添加池的名称标签和池的描述。
6. 在源池下，选择您在上一部分中创建的顶级池。
7. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
8. 在 Locale (区域设置) 下，选择池的区域设置。在本教程中，我们将使用 us-east-2 作为区域池的区域设置。可用的选项来自您在创建 IPAM 时选择的运营区域。

池的区域设置应为以下选项之一：

- 您希望此 IPAM 池可用于分配的 AWS 区域。
- 您希望此 IPAM 池可用于分配的 AWS 本地区域的网络边界组 ([支持的本地区域](#))。此选项仅适用于公共范围内的 IPAM IPv4 池。
- [AWS 专用本地区域](#)。要在 AWS 专用本地区域内创建池，请在选择器输入中输入 AWS 专用本地区域。
- 当您要在全球范围内跨所有 AWS 区域 (例如 CloudFront 地点) 使用 IP 地址时，为 Global。Global 区域设置仅适用于公有 IPv4 池。

例如，您只能从与 VPC 的区域共享区域设置的 IPAM 池中为 VPC 分配 CIDR。请注意，当您为池选择了区域设置后，无法对其进行修改。如果 IPAM 的主区域由于中断而不可用，并且池的区域设置与 IPAM 的主区域不同，则该池仍可用于分配 IP 地址。

选择区域设置可确保池与从中分配的资源之间没有跨区域依赖关系。

9. 在服务下，选择 EC2 (EIP/VPC)。您选择的服务将决定可传播 CIDR 的 AWS 服务。目前，唯一的选择是 EC2 (EIP/VPC)，这意味着从此池中分配的 CIDR 在 Amazon EC2 服务 (适用于弹性 IP 地址) 和 Amazon VPC 服务 (适用于与 VPC 关联的 CIDR) 中是可传播的。
10. 在要预置的 CIDR 下，选择要为池预置的 CIDR。

Note

将 CIDR 预置到顶级池中的区域池时，您可以预置的最具体的 IPv4 CIDR 为 /24；不允许使用更具体的 CIDR (例如 /25)。创建区域池后，您可以在该区域池内创建较小的池 (例如 /25)。请注意，如果您共享该区域池内的一个或多个区域池，则这些池只能在该区域池上设置的区域中使用。

11. 启用配置此池的分配规则设置。这里的分配规则选项与创建顶级池时的选项相同。请参阅 [创建顶级 IPv4 池](#) 以了解创建池时可用的选项。区域池的分配规则不是从顶级池继承来的。如果您不在此应用任何规则，则不会为池设置分配规则。
12. (可选) 为池选择 Tags (标签)。
13. 配置完池后，选择创建池。

在继续之前，请确保已预置此 CIDR。您可以在池详细信息页面的 CIDR 选项卡中查看资源调配状态。

步骤 4：传播 CIDR

本部分中的步骤必须由 IPAM 账户完成。将弹性 IP 地址 (EIP) 与实例或 Elastic Load Balancer 关联后，您就可以开启传播您带到处于已配置了 Service EC2 (EIP/VPC) (服务 EC2 (EIP/VPC)) 的池中的 AWS 的 CIDR。在本教程中，这就是您的区域池。默认情况下，CIDR 不会被传播，这意味着它不能通过互联网公开访问。

此步骤必须由 IPAM 账户完成。

Note

传播状态不会限制您分配弹性 IP 地址的能力。即使您的 BYOIPv4 CIDR 未传播，您仍然可以从 IPAM 池中创建 EIP。

要传播 CIDR

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，创建池时，默认的私有范围被选中。选择公有范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 选择您在本教程中创建的区域池。
5. 选择 CIDR 选项卡。
6. 选择 BYOIP CIDR，然后选择操作 > 广告。
7. 选择广告 CIDR。

这样一来，将广告 BYOIP CIDR，并且广告列中的值将从已撤回变为已刊登广告。

步骤 5。共享区域池

按照本部分中的步骤使用 AWS Resource Access Manager (RAM) 共享 IPAM 池。

在 AWS RAM 中启用资源共享

创建 IPAM 后，您需要与组织中的其他账户共享区域池。在共享 IPAM 池之前，请先完成本部分中的步骤，启用与 AWS RAM 的资源共享。如果要使用 AWS CLI 启用资源共享，请使用 `--profile management-account` 选项。

启用资源共享

1. 使用 AWS Organizations 管理账户打开 AWS RAM 控制台，地址：<https://console.aws.amazon.com/ram/>。
2. 在左侧导航窗格中，依次选择设置、启用与 AWS Organizations 共享、保存设置。

您现在可以与组织的其他成员共享 IPAM 池。

使用 AWS RAM 共享 IPAM 池

在这一部分，您将与其他 AWS Organizations 成员账户共享区域池。有关共享 IPAM 池的完整说明，例如所需 IAM 权限的相关信息，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。如果要使用 AWS CLI 启用资源共享，请使用 `--profile ipam-account` 选项。

使用 AWS RAM 共享 IPAM 池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 依次选择私有范围、IPAM 池以及操作 > 查看详细信息。
4. 在资源共享下，选择创建资源共享。AWS RAM 控制台将打开。您将使用 AWS RAM 来共享该池。
5. 选择创建资源共享。
6. 在 AWS RAM 控制台中，再次选择创建资源共享。
7. 为共享资源添加名称。
8. 在选择资源类型下，选择 IPAM 池，然后选择要共享的池的 ARN。
9. 选择下一步。
10. 选择 `AWSRAMPermissionIpamPoolByoipCidrImport` 权限。本教程不提供权限选项的详细信息，但您可以在 [使用 AWS RAM 共享 IPAM 池](#) 中查看有关这些选项的更多信息。
11. 选择下一步。
12. 在委托人 > 选择主体类型下，选择 AWS 账户，输入要为 IPAM 提供 IP 地址范围的账户的账户 ID，然后选择添加。
13. 选择下一步。
14. 查看资源共享选项和要共享的主体，然后选择创建。
15. 要允许 `member-account` 账户从 IPAM 池中分配 IP 地址 CIDRS，请使用 `AWSRAMDefaultPermissionsIpamPool` 创建第二个资源共享。`--resource-arns` 的值是

您在上一部分中创建的 IPAM 池的 ARN。--principals 的值是 **member-account** 的账户 ID。--permission-arns 的值是 AWSRAMDefaultPermissionsIpamPool 权限的 ARN。

步骤 6：从池中分配弹性 IP 地址

完成本部分中的步骤，以从池中分配弹性 IP 地址。请注意，如果您使用公有 IPv4 池来分配弹性 IP 地址，则可以使用 [步骤 6 的替代方案](#) 中的替代步骤而不是本部分中的步骤。

Important

如果您看到与无权调用 `ec2:AllocateAddress` 相关的错误，则需要更新当前分配给与您共享的 IPAM 池的托管权限。联系创建资源共享的人员，要求他们将托管权限 `AWSRAMPermissionIpamResourceDiscovery` 更新为默认版本。有关更多信息，请参阅《AWS RAM 用户指南》中的[更新资源共享](#)。

AWS Management Console

按照《Amazon EC2 用户指南》中的[分配弹性 IP 地址](#)中的步骤分配地址，但请注意以下几点：

- 此步骤必须由成员账户完成。
- 确保您的 EC2 控制台所在的 AWS 区域与您在创建区域池时选择的区域设置选项相匹配。
- 选择地址池时，选择使用 IPv4 IPAM 池分配选项，然后选择您创建的区域池。

Command line

使用 [allocate-address](#) 命令从池中分配一个地址。您使用的 --region 必须与您在步骤 2 中创建池时选择的 -locale 选项相匹配。包括您在 --ipam-pool-id 中在步骤 2 中创建的 IPAM 池的 ID。或者，您也可以使用 --address 选项在 IPAM 池中选择特定的 /32。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce
```

示例响应：

```
{  
  "PublicIp": "18.97.0.41",  
  "AllocationId": "eipalloc-056cdd6019c0f4b46",
```

```
"PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",  
"NetworkBorderGroup": "us-east-1",  
"Domain": "vpc"  
}
```

有关更多信息，请参阅《Amazon EC2 用户指南》中的[分配弹性 IP 地址](#)。

步骤 7：将弹性 IP 地址与 EC2 实例相关联

完成本部分中的步骤将弹性 IP 地址与 EC2 实例相关联。

AWS Management Console

按照《Amazon EC2 用户指南》中的[关联弹性 IP 地址](#)中的步骤从 IPAM 池中分配弹性 IP 地址，但请注意以下几点：使用 AWS 管理控制台选项时，您关联弹性 IP 地址所在的 AWS 区域必须与您在创建区域池时选择的区域设置选项相匹配。

此步骤必须由成员账户完成。

Command line

此步骤必须由成员账户完成。使用 `--profile member-account` 选项。

使用 `associate-address` 命令将弹性 IP 地址与实例相关联。您关联弹性 IP 地址所在的 `--region` 区域必须与您创建区域池时选择的 `--locale` 选项匹配。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --  
public-ip 18.97.0.41
```

示例响应：

```
{  
  "AssociationId": "eipassoc-06aa85073d3936e0e"  
}
```

有关更多信息，请参阅《Amazon EC2 用户指南》中的[将弹性 IP 地址与实例或网络接口相关联](#)。

步骤 8：清除

按照本部分中的步骤清除您在本教程中预置和创建的资源。

步骤 1：从传播中撤回 CIDR

此步骤必须由 IPAM 账户完成。

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，创建池时，默认的私有范围被选中。选择公有范围。
4. 选择您在本教程中创建的区域池。
5. 选择 CIDR 选项卡。
6. 选择 BYOIP CIDR，然后选择操作>撤回广告。
7. 选择撤回 CIDR。

此时将不再广告 BYOIP CIDR，广告栏中的值将从已刊登广告变为已撤回。

步骤 2：解除弹性 IP 地址的关联

此步骤必须由成员账户完成。如果要使用 AWS CLI，请使用 `--profile member-account` 选项。

- 完成《Amazon EC2 用户指南》中的[解除弹性 IP 地址的关联](#)的步骤，以解除 EIP 的关联。在 AWS 管理控制台中打开 EC2 时，解除 EIP 关联的 AWS 区域必须与您在创建将用于 BYOIP CIDR 的池时选择的 Locale 选项匹配。在本教程中，该池就是区域池。

步骤 3：释放弹性 IP 地址

此步骤必须由成员账户完成。如果要使用 AWS CLI，请使用 `--profile member-account` 选项。

- 完成《Amazon EC2 用户指南》中的[释放弹性 IP 地址](#)的步骤，从公有 IPv4 池释放弹性 IP 地址 (EIP)。在 AWS 管理控制台中打开 EC2 时，分配 EIP 的 AWS 区域必须与您在创建将用于 BYOIP CIDR 的池时选择的 Locale 选项匹配。

步骤 4：删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成

此步骤必须分别由 IPAM 账户和管理账户完成。要使用 AWS CLI 删除 RAM 共享并禁用 RAM 集成，请使用 `--profile ipam-account` 和 `--profile management-account` 选项。

- 完成《AWS RAM 用户指南》中[删除 AWS RAM 中的资源共享](#)和[禁用与 AWS Organizations 的资源共享](#)所述的步骤，删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成。

步骤 5：从区域池和顶级池中取消预调配 CIDR

此步骤必须由 IPAM 账户完成。如果要使用 AWS CLI 共享该池，请使用 `--profile ipam-account` 选项。

- 按顺序完成 [从池中取消预置 CIDR](#) 中的步骤，从区域池中取消预置 CIDR，然后从顶级池中取消预置 CIDR。

步骤 6：删除区域池和顶级池

此步骤必须由 IPAM 账户完成。如果要使用 AWS CLI 共享该池，请使用 `--profile ipam-account` 选项。

- 按顺序完成 [删除池](#) 中的步骤，删除区域池，然后删除顶级池。

步骤 6 的替代方案

如果您使用公有 IPv4 池来分配弹性 IP 地址，则可以本部分中的步骤，而不是 [步骤 6：从池中分配弹性 IP 地址](#) 中的步骤。

内容

- [步骤 1：创建公有 IPv4 池](#)
- [步骤 2：将公有 IPv4 CIDR 预调配到您的公有 IPv4 池](#)
- [步骤 3：从公有 IPv4 池分配弹性 IP 地址](#)
- [步骤 6 清理的替代方案](#)

步骤 1：创建公有 IPv4 池

此步骤应该由预置弹性 IP 地址的成员账户完成。

Note

- 此步骤必须由成员账户使用 AWS CLI 完成。
- 公有 IPv4 池和 IPAM 池由 AWS 中的不同资源管理。公共 IPv4 池是单一账户资源，使您能够将公有 CIDR 转换为弹性 IP 地址。IPAM 池可用于将公有空间分配给公有 IPv4 池。

要使用 AWS CLI 创建公有 IPv4 池

- 请运行以下命令以预置 CIDR。运行本部分中的命令时，`--region` 的值必须与您在创建将用于 BYOIP CIDR 的池时选择的 `Locale` 选项匹配。

```
aws ec2 create-public-ipv4-pool --region us-east-2 --profile member-account
```

在输出中，您将看到公有 IPv4 池 ID。在下一步骤中，您需要用到此 ID。

```
{
  "PoolId": "ipv4pool-ec2-09037ce61cf068f9a"
}
```

步骤 2：将公有 IPv4 CIDR 预调配到您的公有 IPv4 池

将公有 IPv4 CIDR 预置到您的公有 IPv4 池。`--region` 的值为必须与您在创建将用于 BYOIP CIDR 的池时选择的 `Locale` 值匹配。`--netmask-length` 是指您想添加到公共池的 IPAM 池空间量。该值不能大于 IPAM 池的网络掩码长度。您可以定义的最不具体的 `--netmask-length` 是 24。

Note

- 如果您将 /24 CIDR 范围引入 IPAM 以便在 AWS 组织内共享，则可以为多个 IPAM 池预置较小的前缀，例如 /27（使用 `-- netmask-length 27`），而不是像本教程中所示预置整个 /24 CIDR（使用 `-- netmask-length 24`）。
- 此步骤必须由成员账户使用 AWS CLI 完成。

要使用 AWS CLI 创建公有 IPv4 池

1. 请运行以下命令以预置 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
```

在输出中，您将看到预置的 CIDR。

```
{
```

```
"PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
"PoolAddressRange": {
  "FirstAddress": "130.137.245.0",
  "LastAddress": "130.137.245.255",
  "AddressCount": 256,
  "AvailableAddressCount": 256
}
}
```

2. 运行以下命令，以查看公有 IPv4 池中预置的 CIDR。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --max-results 10 --
profile member-account
```

在输出中，您将看到预置的 CIDR。默认情况下，CIDR 不会被传播，这意味着它不能通过互联网公开访问。在本教程的最后一步中，您将有机会将此 CIDR 设置为进行传播。

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

创建公有 IPv4 池后，要查看在 IPAM 区域池中分配的公有 IPv4 池，请打开 IPAM 控制台，并在分配或资源下查看区域池中的分配。

步骤 3：从公有 IPv4 池分配弹性 IP 地址

完成《Amazon EC2 用户指南》中的[分配弹性 IP 地址](#)的步骤，从公有 IPv4 池分配 EIP。在 AWS 管理控制台中打开 EC2 时，分配 EIP 的 AWS 区域必须与您在创建将用于 BYOIP CIDR 的池时选择的 Locale 选项匹配。

此步骤必须由成员账户完成。如果要使用 AWS CLI，请使用 `--profile member-account` 选项。

完成这三个步骤后，请返回 [步骤 7：将弹性 IP 地址与 EC2 实例相关联](#) 并继续操作，直到完成本教程。

步骤 6 清理的替代方案

完成以下步骤，以清理使用步骤 9 的替代方法创建的公有 IPv4 池。在 [步骤 8：清除](#) 中的标准清理过程中，您应在释放弹性 IP 地址后完成这些步骤。

步骤 1：从您的公有 IPv4 池中取消预调配公有 IPv4 CIDR

Important

此步骤必须由成员账户使用 AWS CLI 完成。

1. 查看您的 BYOIP CIDR。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

在输出中，您将看到 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. 运行以下命令，从公有 IPv4 池中释放 CIDR。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-2 --pool-id ipv4pool-ec2-09037ce61cf068f9a --cidr 130.137.245.0/24 --profile member-account
```

3. 再次查看您的 BYOIP CIDR，并确保没有更多的预置地址。运行本部分中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

在输出中，您将看到公有 IPv4 池中的 IP 地址计数。

```
{
  "PublicIpv4Pools": [
    {
      "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
      "Description": "",
      "PoolAddressRanges": [],
      "TotalAddressCount": 0,
      "TotalAvailableAddressCount": 0,
      "NetworkBorderGroup": "us-east-2",
      "Tags": []
    }
  ]
}
```

Note

IPAM 可能需要一些时间才能发现公有 IPv4 池分配已被删除。在看到已从 IPAM 中删除分配之前，您无法继续清理和取消预置 IPAM 池 CIDR。

步骤 2：删除公有 IPv4 池

此步骤必须由成员账户完成。

- 运行以下命令，以从 CIDR 中删除公有 IPv4 池。运行本部分中的命令时，`--region` 的值必须与您在创建将用于 BYOIP CIDR 的池时选择的 Locale 选项匹配。在本教程中，该池就是区域池。必须使用 AWS CLI 完成此步骤。

```
aws ec2 delete-public-ipv4-pool --region us-east-2 --pool-id ipv4pool-ec2-09037ce61cf068f9a --profile member-account
```

在输出中，您将看到返回值真。

```
{
  "ReturnValue": true
}
```

删除该池后，要查看未由 IPAM 管理的分配，请打开 IPAM 控制台，并在分配下查看区域池的详细信息。

使用 AWS 管理控制台自带 IPv6 CIDR 到 IPAM 中

按照本教程中的步骤将 IPv6 CIDR 带入 IPAM，并使用 AWS 管理控制台和 AWS CLI 分配带有 CIDR 的 VPC。

如果不需要通过互联网公开发布 IPv6 地址，则可向 IPAM 预置私有 GUA IPv6 地址。有关更多信息，请参阅 [启用预置私有 IPv6 GUA CIDR](#)。

Important

- 本教程假定您已完成以下部分中的步骤：
 - [将 IPAM 与 AWS Organization 中的账户集成](#).
 - [创建 IPAM](#).
- 本教程的每个步骤都必须由以下三个 AWS Organizations 账户之一完成：
 - 管理账户。
 - [将 IPAM 与 AWS Organization 中的账户集成](#) 中配置为 IPAM 管理员的成员账户。在本教程中，此账户将被称为 IPAM 账户。

- 将从 IPAM 池中分配 CIDR 的企业中的成员账户。在本教程中，此账户将被称为成员账户。

内容

- [步骤 1：创建顶级 IPAM 池](#)
- [步骤 2：在顶级池中创建区域池](#)
- [步骤 3：共享区域池](#)
- [第 4 步：创建 VPC](#)
- [第 5 步：传播 CIDR](#)
- [第 6 步：清除](#)

步骤 1：创建顶级 IPAM 池


由于您将创建一个其中包含一个区域池的顶级 IPAM 池，并且我们将为区域池中的资源分配空间，因此您将在区域池中设置区域设置，而不是在顶级池中。在后面的步骤中创建区域池时，您将区域设置添加到区域池中。IPAM 与 BYOIP 集成要求在将用于 BYOIP CIDR 的任何一个池上设置区域设置。

此步骤必须由 IPAM 账户完成。

如需创建池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，创建池时，默认的私有范围被选中。选择公有范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 选择创建池。
5. (可选) 添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 范围。
7. 在地址系列下，选择 IPv6。
8. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
9. 在区域设置下，选择无。您将在区域池中设置区域设置。

区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。例如，您只能从与 VPC 的区域共享区域设置的 IPAM 池中为 VPC 分配 CIDR。请注意，当您为池选择了区域设置后，无法对其进行修改。如果 IPAM 的主区域由于中断而不可用，并且池的区域设置与 IPAM 的主区域不同，则该池仍可用于分配 IP 地址。

 Note

如果您只创建单个池而不是其中包含区域池的顶级池，则需要为此池选择一个区域设置，以便该池可用于分配。

10. 在公有 IP 源下，BYOIP 默认处于选中状态。

11. 在要预置的 CIDR 下，执行下列某项操作：

- 如果[使用 X.509 证书验证域控制权](#)，则必须包含 CIDR 和 BYOIP 消息以及在该步骤中创建的证书签名，以便我们验证您是否控制了公共空间。
- 如果[使用 DNS TXT 记录验证域控制权](#)，则必须包含 CIDR 和 IPAM 消息以及在该步骤中创建的验证令牌，以便我们验证您是否控制了公共空间。

请注意，在将 IPv6 CIDR 预置到顶级池中的池时，对于公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /48；对于不公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /60。

 Important

虽然大多数预配置将在两小时内完成，但对于公开发布的范围，完成预配置过程可能需要长达一周的时间。

12. 将配置此池的分配规则设置保持未选中状态。

13. (可选) 为池选择 Tags (标签) 。

14. 选择创建池。

在继续之前，请确保已预置此 CIDR。您可以在池详细信息页面的 CIDR 选项卡中查看资源调配状态。

步骤 2：在顶级池中创建区域池

在顶级池中创建区域池。区域设置在池上是必需的，它必须是您在创建 IPAM 时配置的运营区域之一。

此步骤必须由 IPAM 账户完成。

要在顶级池中创建区域池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，创建池时，默认的私有范围被选中。如果您不想使用默认的私有范围，请从内容窗格顶部的下拉菜单中选择要使用的范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 选择创建池。
5. (可选) 添加池的名称标签和池的描述。
6. 在源池下，选择您在上一部分中创建的顶级池。
7. 在资源规划下，保持选中在范围内规划 IP 空间。有关使用此选项规划 VPC 内的子网 IP 空间的更多信息，请参阅 [教程：为子网 IP 分配规划 VPC IP 地址空间](#)。
8. 选择池的区域设置。选择区域设置可确保池与从中分配的资源之间没有跨区域依赖关系。可用的选项来自您在创建 IPAM 时选择的运营区域。在本教程中，我们将使用 us-east-2 作为区域池的区域设置。

区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。例如，您只能从与 VPC 的区域共享区域设置的 IPAM 池中为 VPC 分配 CIDR。请注意，当您为池选择了区域设置后，无法对其进行修改。如果 IPAM 的主区域由于中断而不可用，并且池的区域设置与 IPAM 的主区域不同，则该池仍可用于分配 IP 地址。

9. 在服务下，选择 EC2 (EIP/VPC)。您选择的服务将决定可传播 CIDR 的 AWS 服务。目前，唯一的选择是 EC2 (EIP/VPC) ，这意味着从此池中分配的 CIDR 在 Amazon EC2 服务和 Amazon VPC 服务 (适用于与 VPC 关联的 CIDR) 中是可传播的。
10. 在要预置的 CIDR 下，选择要为池预置的 CIDR。请注意，在将 IPv6 CIDR 预置到顶级池中的池时，对于公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /48；对于不公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /60。
11. 启用配置此池的分配规则设置，并为此池选择可选分配规则：
 - 自动导入发现的资源：如果区域设置被设置为无，则此选项不可用。如果选中此选项，IPAM 将持续查找此池的 CIDR 范围内的资源，并将其作为分配自动导入到 IPAM 中。请注意以下几点：
 - 为了成功导入，不得将分配给这些资源的 CIDR 分配给其他资源。
 - 无论 IPAM 是否符合池的分配规则，都将导入 CIDR，因此可能会导入资源且随后会将资源标记为不合规。
 - 如果 IPAM 发现多个重叠的 CIDR，IPAM 将仅导入最大的 CIDR。
 - 如果 IPAM 发现多个具有匹配 CIDR 的 CIDR，IPAM 将只随机导入其中一个。

- 最短网络掩码长度：此 IPAM 池中的 CIDR 分配所需的符合要求的最小网络掩码长度以及可以从池中分配的最大大小的 CIDR 块。最短网络掩码长度必须小于最大网络掩码长度。IPv4 地址的可能网络掩码长度为 0 - 32。IPv6 地址的可能网络掩码长度为 0 - 128。
- 默认网络掩码长度：添加到此池的分配的默认网络掩码长度。
- 最大网络掩码长度：此池中的 CIDR 分配所需的最大网络掩码长度。此值表示可以从池中分配的最小大小的 CIDR 块。确保此值为最小 /48 值。
- 标记要求：资源分配池中的空间所需的标签。如果资源在分配空间后更改了标签，或者如果池中的分配标记规则发生了更改，则该资源可能会被标记为不合规。
- 区域设置：使用此池中的 CIDR 的资源所需的区域设置。自动导入的没有此区域设置的资源将被标记为不合规。不会自动导入到池中的资源将不允许从池中分配空间，除非它们位于此区域设置。

12. (可选) 为池选择标签。

13. 配置完池后，选择创建池。

在继续之前，请确保已预置此 CIDR。您可以在池详细信息页面的 CIDR 选项卡中查看资源调配状态。

步骤 3：共享区域池

按照本部分中的步骤使用 AWS Resource Access Manager (RAM) 共享 IPAM 池。

在 AWS RAM 中启用资源共享

创建 IPAM 后，您需要与组织中的其他账户共享区域池。在共享 IPAM 池之前，请先完成本部分中的步骤，启用与 AWS RAM 的资源共享。如果要使用 AWS CLI 启用资源共享，请使用 `--profile management-account` 选项。

启用资源共享

1. 使用 AWS Organizations 管理账户打开 AWS RAM 控制台，地址：<https://console.aws.amazon.com/ram/>。
2. 在左侧导航窗格中，依次选择设置、启用与 AWS Organizations 共享、保存设置。

您现在可以与组织的其他成员共享 IPAM 池。

使用 AWS RAM 共享 IPAM 池

在这一部分，您将与其他 AWS Organizations 成员账户共享区域池。有关共享 IPAM 池的完整说明，例如所需 IAM 权限的相关信息，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。如果要使用 AWS CLI 启用资源共享，请使用 `--profile ipam-account` 选项。

使用 AWS RAM 共享 IPAM 池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 依次选择私有范围、IPAM 池以及操作 > 查看详细信息。
4. 在资源共享下，选择创建资源共享。AWS RAM 控制台将打开。您将使用 AWS RAM 来共享该池。
5. 选择创建资源共享。
6. 在 AWS RAM 控制台中，再次选择创建资源共享。
7. 为共享资源添加名称。
8. 在选择资源类型下，选择 IPAM 池，然后选择要共享的池的 ARN。
9. 选择下一步。
10. 选择 `AWSRAMPermissionIpamPoolByoipCidrImport` 权限。本教程不提供权限选项的详细信息，但您可以在 [使用 AWS RAM 共享 IPAM 池](#) 中查看有关这些选项的更多信息。
11. 选择下一步。
12. 在委托人 > 选择主体类型下，选择 AWS 账户，输入要为 IPAM 提供 IP 地址范围的账户的账户 ID，然后选择添加。
13. 选择下一步。
14. 查看资源共享选项和要共享的主体，然后选择创建。
15. 要允许 `member-account` 账户从 IPAM 池中分配 IP 地址 CIDRS，请使用 `AWSRAMDefaultPermissionsIpamPool` 创建第二个资源共享。`--resource-arns` 的值是您在上一部分中创建的 IPAM 池的 ARN。`--principals` 的值是 `member-account` 的账户 ID。`--permission-arns` 的值是 `AWSRAMDefaultPermissionsIpamPool` 权限的 ARN。

第 4 步：创建 VPC

完成《Amazon VPC 用户指南》中的 [创建 VPC](#) 中的步骤。

此步骤必须由成员账户完成。

Note

- 在 AWS 管理控制台中打开 VPC 时，创建 VPC 的 AWS 区域必须与您在创建将用于 BYOIP CIDR 的池时选择的 Local 选项匹配。
- 当您到达为 VPC 选择 CIDR 的步骤时，您可以选择使用 IPAM 池中的 CIDR。选择您在本教程中创建的区域池。

创建 VPC 时，AWS 会将 IPAM 池中的 CIDR 分配给 VPC。您可以通过在 IPAM 控制台的内容窗格中选择池并查看池的分配选项卡来查看 IPAM 中的分配。

第 5 步：传播 CIDR

本部分中的步骤必须由 IPAM 账户完成。一旦您创建了 VPC，就可以开启传播您带入位于配置了 Service EC2 (EIP/VPC) 的池中的 AWS 的 CIDR。在本教程中，这就是您的区域池。默认情况下，CIDR 不会被传播，这意味着它不能通过互联网公开访问。

此步骤必须由 IPAM 账户完成。

要传播 CIDR

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，创建池时，默认的私有范围被选中。选择公有范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 选择您在本教程中创建的区域池。
5. 选择 CIDR 选项卡。
6. 选择 BYOIP CIDR，然后选择操作 > 广告。
7. 选择广告 CIDR。

这样一来，将广告 BYOIP CIDR，并且广告列中的值将从已撤回变为已刊登广告。

第 6 步：清除

按照本部分中的步骤清除您在本教程中预置和创建的资源。

步骤 1：从传播中撤回 CIDR

此步骤必须由 IPAM 账户完成。

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择 Pools (池)。
3. 默认情况下，创建池时，默认的私有范围被选中。选择公有范围。
4. 选择您在本教程中创建的区域池。
5. 选择 CIDR 选项卡。
6. 选择 BYOIP CIDR，然后选择操作>撤回广告。
7. 选择撤回 CIDR。

此时将不再传播 BYOIP CIDR，Advertising (传播) 栏中的值将从 Advertised (已传播) 变为 Withdrawn (已撤回)。

步骤 2：删除 VPC

此步骤必须由成员账户完成。

- 完成《Amazon VPC 用户指南》中的[删除 VPC](#)中的步骤以删除 VPC。在 AWS 管理控制台中打开 VPC 时，从中删除 VPC 的 AWS 区域必须与您在创建将用于 BYOIP CIDR 的池时选择的 Locale 选项匹配。在本教程中，该池就是区域池。

删除 VPC 时，IPAM 需要时间来发现资源已被删除并解除分配给 VPC 的 CIDR。除非在池详细信息分配选项卡中看到 IPAM 已从池中删除分配，否则无法继续执行清除中的下一步骤。

第 3 步：删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成

此步骤必须分别由 IPAM 账户和管理账户完成。

- 完成《AWS RAM 用户指南》中[删除 AWS RAM 中的资源共享](#)和[禁用与 AWS Organizations 的资源共享](#)所述的步骤，删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成。

步骤 4：从区域池和顶级池中取消预置 CIDR

此步骤必须由 IPAM 账户完成。

- 按顺序完成 [从池中取消预置 CIDR](#) 中的步骤，从区域池中取消预置 CIDR，然后从顶级池中取消预置 CIDR。

步骤 5：删除区域池和顶级池

此步骤必须由 IPAM 账户完成。

- 按顺序完成 [删除池](#) 中的步骤，删除区域池，然后删除顶级池。

仅使用 AWS CLI 自带 IP CIDR 到 IPAM 中

自带 IP (BYOIP) 到 IPAM 允许您在 AWS 中使用组织现有的 IPv4 和 IPv6 地址范围。这使您能够在自己的 IP 地址空间下将本地和云环境统一，从而保持一致的品牌形象、提高网络性能、增强安全性并简化管理。

按照以下步骤，仅使用 AWS CLI 将 IPv4 或 IPv6 CIDR 带入 IPAM 中。

Note

开始操作之前，必须先[验证域控制权](#)。

将 IPv4 地址范围设置为 AWS 后，您可以使用该范围内的所有 IP 地址，包括第一个地址（网络地址）和最后一个地址（广播地址）。

内容

- [仅使用 AWS CLI 自带公有 IPv4 CIDR 到 IPAM 中](#)
- [仅使用 AWS CLI 自带 IPv6 CIDR 到 IPAM 中](#)

仅使用 AWS CLI 自带公有 IPv4 CIDR 到 IPAM 中

按照以下步骤将 IPv4 CIDR 带入 IPAM 中，然后仅使用 AWS CLI 使用 CIDR 分配弹性 IP 地址 (EIP)。

Important

- 本教程假定您已完成以下部分中的步骤：
 - [将 IPAM 与 AWS Organization 中的账户集成](#)。

- [创建 IPAM](#).
- 本教程的每个步骤都必须由以下三个 AWS Organizations 账户之一完成：
 - 管理账户。
 - [将 IPAM 与 AWS Organization 中的账户集成](#) 中配置为 IPAM 管理员的成员账户。在本教程中，此账户将被称为 IPAM 账户。
 - 将从 IPAM 池中分配 CIDR 的企业中的成员账户。在本教程中，此账户将被称为成员账户。

内容

- [第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色](#)
- [步骤 2：创建 IPAM](#)
- [步骤 3：创建顶级 IPAM 池](#)
- [步骤 4：向顶级池预置 CIDR](#)
- [步骤 5：在顶级池中创建区域池](#)
- [步骤 6：向区域池预置 CIDR](#)
- [步骤 7：传播 CIDR](#)
- [步骤 8：共享区域池](#)
- [步骤 9：从池中分配弹性 IP 地址](#)
- [步骤 10：将弹性 IP 地址与 EC2 实例相关联](#)
- [步骤 11：清除](#)
- [步骤 9 的替代方案](#)

第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色

要以单个 AWS 用户的身份完成本教程，您可以使用 AWS CLI 命名配置文件在 IAM 角色之间切换。[命名配置文件](#) 是您在将 `--profile` 选项与 AWS CLI 结合使用时引用的设置和凭证集合。有关如何为 AWS 账户创建 IAM 角色和命名配置文件的更多信息，请参阅[在 AWS CLI 中使用 IAM 角色](#)。

为您将在本教程中使用的三个 AWS 账户分别创建一个角色和一个命名配置文件：

- 为 AWS Organizations 管理账户创建名为 `management-account` 的配置文件。
- 为配置为 IPAM 管理员的 AWS Organizations 成员账户创建名为 `ipam-account` 的配置文件。

- 为将从 IPAM 池中分配 CIDR 的企业中的 AWS Organizations 成员账户创建名为 `member-account` 的配置文件。

创建 IAM 角色和命名配置文件后，请返回本页面并转至下一步。在本教程的其余部分中，您将注意到示例 AWS CLI 命令会将 `--profile` 选项与其中一个命名配置文件一起使用，以指示哪个账户必须运行该命令。

步骤 2：创建 IPAM

此为可选步骤。如果您已在创建了 `us-east-1` 和 `us-west-2` 的运营区域的情况下创建了 IPAM，您可以跳过此步骤。创建 IPAM 并指定 `us-east-1` 和 `us-west-2` 的运营区域。您必须选择一个运营区域，以便在创建 IPAM 池时可以使用区域设置选项。IPAM 与 BYOIP 集成要求在将用于 BYOIP CIDR 的任何一个池上设置区域设置。

此步骤必须由 IPAM 账户完成。

运行如下命令：

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

在输出中，您将看到您创建的 IPAM。记下 `PublicDefaultScopeId` 值。在下一步中，您将需要使用公有范围 ID。您使用公有范围是因为 BYOIP CIDR 是公有 IP 地址，这就是公有范围的用途。

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

步骤 3：创建顶级 IPAM 池

完成本部分中的步骤创建顶级 IPAM 池。

此步骤必须由 IPAM 账户完成。

使用 AWS CLI 为您的所有 AWS 资源创建 IPv4 地址池

1. 运行以下命令以创建 IPAM 池。请使用您在上一步中创建的 IPAM 的公有范围的 ID。

此步骤必须由 IPAM 账户完成。

```
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
```

在输出中，您将会看到 `create-in-progress`，这表明池的创建正在进行中。

```
{
  "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. 运行以下命令，直到您在输出中看到 `create-complete` 的状态。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

下面的示例输出显示池的状态。

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

步骤 4：向顶级池预置 CIDR

向顶级池预置 CIDR 块。请注意，将 IPv4 CIDR 预置到顶级池中的资源池时，您可以预置的最低 IPv4 CIDR 为 /24；不允许使用更具体的 CIDR（例如 /25）。

Note

- 如果[使用 X.509 证书验证域控制权](#)，则必须包含 CIDR 和 BYOIP 消息以及在该步骤中创建的证书签名，以便我们验证您是否控制了公共空间。
- 如果[使用 DNS TXT 记录验证域控制权](#)，则必须包含 CIDR 和 IPAM 消息以及在该步骤中创建的验证令牌，以便我们验证您是否控制了公共空间。

在向顶级池预置 BYOIP CIDR 时，您只需要验证域控制权。对于顶级池中的区域池，您可以省略域所有权验证选项。

此步骤必须由 IPAM 账户完成。

Important

在向顶级池预置 BYOIP CIDR 时，您只需要验证域控制权。对于顶级池中的区域池，您可以省略域控制权选项。一旦您将自己的 BYOIP 登录到 IPAM，在跨区域和账户划分 BYOIP 时，您无需执行所有权验证。

使用 AWS CLI 向池预置 CIDR 块

1. 要为 CIDR 预置证书信息，请使用以下示例命令。除了根据需要替换示例中的值外，务必还要将 Message 和 Signature 值替换为在 [使用 X.509 证书验证域](#) 中获得的 text_message 和 signed_message 值。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --verification-method remarks-x509 --cidr-authorization-context Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsmAU0P7EN07VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7dhApR89Kt6GxRY0dRaNx8yt-uoZWzxt2yIhWngy-du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXE1T5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-oS9AZ1lafBbrFxrjFWRCTJhc7Cg3ASbR0-VWNci-C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

要为 CIDR 预置验证令牌信息，请使用以下示例命令。除了根据需要替换示例中的值外，务必还要将 ipam-ext-res-ver-token-0309ce7f67a768cf0 替换为在 [使用 DNS TXT 记录验证域](#) 中获得的 IpamExternalResourceVerificationTokenId 令牌 ID。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --verification-method dns-token --ipam-external-resource-verification-token-id ipam-ext-res-ver-token-0309ce7f67a768cf0 --profile ipam-account
```

在输出中，您将看到 CIDR 待定预置。

```
{
```

```
"IpamPoolCidr": {  
    "Cidr": "130.137.245.0/24",  
    "State": "pending-provision"  
}  
}
```

2. 在继续之前，请确保已预置此 CIDR。

Important

虽然大多数预配置将在两小时内完成，但对于公开发布的范围，完成预配置过程可能需要长达一周的时间。

运行以下命令，直到您在输出中看到 `provisioned` 的状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-  
pool-0a03d430ca3f5c035 --profile ipam-account
```

下面的示例输出显示状态。

```
{  
    "IpamPoolCidrs": [  
        {  
            "Cidr": "130.137.245.0/24",  
            "State": "provisioned"  
        }  
    ]  
}
```

步骤 5：在顶级池中创建区域池

在顶级池中创建区域池。

池的区域设置应为以下选项之一：

- 您希望此 IPAM 池可用于分配的 AWS 区域。

- 您希望此 IPAM 池可用于分配的 AWS 本地区域的网络边界组 ([支持的本地区域](#))。此选项仅适用于公共范围内的 IPAM IPv4 池。
- [AWS 专用本地区域](#)。要在 AWS 专用本地区域内创建池，请在选择器输入中输入 AWS 专用本地区域。
- 当您要在全球范围内跨所有 AWS 区域 (例如 CloudFront 地点) 使用 IP 地址时，为 Global。Global 区域设置仅适用于公有 IPv4 池。

例如，您只能从与 VPC 的区域共享区域设置的 IPAM 池中为 VPC 分配 CIDR。请注意，当您为池选择了区域设置后，无法对其进行修改。如果 IPAM 的主区域由于中断而不可用，并且池的区域设置与 IPAM 的主区域不同，则该池仍可用于分配 IP 地址。

运行本部分中的命令时，`--region` 的值必须包括您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项。例如，如果您使用区域设置 `us-east-1` 创建 BYOIP 池，则 `--region` 应为 `us-east-1`。如果您使用区域设置 `us-east-1-scl-1` (用于本地区域的网络边界组) 创建 BYOIP 池，则 `--region` 应为 `us-east-1`，因为该区域管理区域设置 `us-east-1-scl-1`。

此步骤必须由 IPAM 账户完成。

选择区域设置可确保池与从中分配的资源之间没有跨区域依赖关系。可用的选项来自您在创建 IPAM 时选择的运营区域。在本教程中，我们将使用 `us-west-2` 作为区域池的区域设置。

Important

创建池时，您必须包括 `--aws-service ec2`。您选择的服务将决定可传播 CIDR 的 AWS 服务。目前，唯一的选择是 `ec2`，这意味着从此池中分配的 CIDR 在 Amazon EC2 服务 (适用于弹性 IP 地址) 和 Amazon VPC 服务 (适用于与 VPC 关联的 CIDR) 中是可传播的。

要使用 AWS CLI 创建区域池

1. 运行以下命令以创建池。

```
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
```

在输出中，您将看到创建池的 IPAM。

```
{
  "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. 运行以下命令，直到您在输出中看到 `create-complete` 的状态。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

在输出中，您可以看到您在 IPAM 中拥有的池。在本教程中，我们创建了一个顶级池和一个区域池，所以您会看到这两个池。

步骤 6：向区域池预置 CIDR

向区域池预置 CIDR 块。

Note

将 CIDR 预置到顶级池中的区域池时，您可以预置的最具体的 IPv4 CIDR 为 /24；不允许使用更具体的 CIDR（例如 /25）。创建区域池后，您可以在该区域池内创建较小的池（例如 /25）。请注意，如果您共享该区域池内的一个或多个区域池，则这些池只能在该区域池上设置的区域中使用。

此步骤必须由 IPAM 账户完成。

要使用 AWS CLI 将 CIDR 块分配到区域池

1. 请运行以下命令以预置 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
```

在输出中，您将看到 CIDR 待定预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "pending-provision"
  }
}
```

2. 运行以下命令，直到您在输出中看到 provisioned 的状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

下面的示例输出显示正确的状态。

```
{
  "IpamPoolCidrs": [
    {
      "Cidr": "130.137.245.0/24",
      "State": "provisioned"
    }
  ]
}
```

步骤 7：传播 CIDR

本部分中的步骤必须由 IPAM 账户完成。将弹性 IP 地址 (EIP) 与实例或 Elastic Load Balancer 关联后，您就可以开始传播您带到处于已定义了 `--aws-service ec2` 的池中的 AWS 的 CIDR。在本教程中，这就是您的区域池。默认情况下，CIDR 不会被传播，这意味着它不能通过互联网公开访问。运行本部分中的命令时，`--region` 的值必须与您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项匹配。

此步骤必须由 IPAM 账户完成。

Note

传播状态不会限制您分配弹性 IP 地址的能力。即使您的 BYOIPv4 CIDR 未传播，您仍然可以从 IPAM 池中创建 EIP。

开始使用 AWS CLI 传播 CIDR

- 请运行以下命令以传播 CIDR。

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --  
profile ipam-account
```

在输出中，您将看到 CIDR 被传播。

```
{  
  "ByoipCidr": {  
    "Cidr": "130.137.245.0/24",  
    "State": "advertised"  
  }  
}
```

步骤 8：共享区域池

按照本部分中的步骤使用 AWS Resource Access Manager (RAM) 共享 IPAM 池。

在 AWS RAM 中启用资源共享

创建 IPAM 后，您需要与组织中的其他账户共享区域池。在共享 IPAM 池之前，请先完成本部分中的步骤，启用与 AWS RAM 的资源共享。如果要使用 AWS CLI 启用资源共享，请使用 `--profile management-account` 选项。

启用资源共享

1. 使用 AWS Organizations 管理账户打开 AWS RAM 控制台，地址：<https://console.aws.amazon.com/ram/>。
2. 在左侧导航窗格中，依次选择设置、启用与 AWS Organizations 共享、保存设置。

您现在可以与组织的其他成员共享 IPAM 池。

使用 AWS RAM 共享 IPAM 池

在这一部分，您将与其他 AWS Organizations 成员账户共享区域池。有关共享 IPAM 池的完整说明，例如所需 IAM 权限的相关信息，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。如果要使用 AWS CLI 启用资源共享，请使用 `--profile ipam-account` 选项。

使用 AWS RAM 共享 IPAM 池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 依次选择私有范围、IPAM 池以及操作 > 查看详细信息。
4. 在资源共享下，选择创建资源共享。AWS RAM 控制台将打开。您将使用 AWS RAM 来共享该池。
5. 选择创建资源共享。
6. 在 AWS RAM 控制台中，再次选择创建资源共享。
7. 为共享资源添加名称。
8. 在选择资源类型下，选择 IPAM 池，然后选择要共享的池的 ARN。
9. 选择下一步。
10. 选择 `AWSRAMPermissionIpamPoolByoipCidrImport` 权限。本教程不提供权限选项的详细信息，但您可以在 [使用 AWS RAM 共享 IPAM 池](#) 中查看有关这些选项的更多信息。
11. 选择下一步。

12. 在委托人 > 选择主体类型下，选择 AWS 账户，输入要为 IPAM 提供 IP 地址范围的账户的账户 ID，然后选择添加。
13. 选择下一步。
14. 查看资源共享选项和要共享的主体，然后选择创建。
15. 要允许 **member-account** 账户从 IPAM 池中分配 IP 地址 CIDRS，请使用 `AWSRAMDefaultPermissionsIpamPool` 创建第二个资源共享。 `--resource-arns` 的值是您在上一步中创建的 IPAM 池的 ARN。 `--principals` 的值是 **member-account** 的账户 ID。 `--permission-arns` 的值是 `AWSRAMDefaultPermissionsIpamPool` 权限的 ARN。

步骤 9：从池中分配弹性 IP 地址

完成本部分中的步骤，以从池中分配弹性 IP 地址。请注意，如果您使用公有 IPv4 池来分配弹性 IP 地址，则可以使用 [步骤 9 的替代方案](#) 中的替代步骤而不是本部分中的步骤。

Important

如果您看到与无权调用 `ec2:AllocateAddress` 相关的错误，则需要更新当前分配给与您共享的 IPAM 池的托管权限。联系创建资源共享的人员，要求他们将托管权限 `AWSRAMPermissionIpamResourceDiscovery` 更新为默认版本。有关更多信息，请参阅《AWS RAM 用户指南》中的 [更新资源共享](#)。

AWS Management Console

按照《Amazon EC2 用户指南》中的 [分配弹性 IP 地址](#) 中的步骤分配地址，但请注意以下几点：

- 此步骤必须由成员账户完成。
- 确保您的 EC2 控制台所在的 AWS 区域与您在创建区域池时选择的区域设置选项相匹配。
- 选择地址池时，选择使用 IPv4 IPAM 池分配选项，然后选择您创建的区域池。

Command line

使用 `allocate-address` 命令从池中分配一个地址。您使用的 `--region` 必须与您在步骤 2 中创建池时选择的 `-locale` 选项相匹配。包括您在 `--ipam-pool-id` 中在步骤 2 中创建的 IPAM 池的 ID。或者，您也可以使用 `--address` 选项在 IPAM 池中选择特定的 `/32`。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce
```

示例响应：

```
{
  "PublicIp": "18.97.0.41",
  "AllocationId": "eipalloc-056cdd6019c0f4b46",
  "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
  "NetworkBorderGroup": "us-east-1",
  "Domain": "vpc"
}
```

有关更多信息，请参阅《Amazon EC2 用户指南》中的[分配弹性 IP 地址](#)。

步骤 10：将弹性 IP 地址与 EC2 实例相关联

完成本部分中的步骤将弹性 IP 地址与 EC2 实例相关联。

AWS Management Console

按照《Amazon EC2 用户指南》中的[关联弹性 IP 地址](#)中的步骤从 IPAM 池中分配弹性 IP 地址，但请注意以下几点：使用 AWS 管理控制台选项时，您关联弹性 IP 地址所在的 AWS 区域必须与您在创建区域池时选择的区域设置选项相匹配。

此步骤必须由成员账户完成。

Command line

此步骤必须由成员账户完成。使用 `--profile member-account` 选项。

使用 `associate-address` 命令将弹性 IP 地址与实例相关联。您关联弹性 IP 地址所在的 `--region` 区域必须与您创建区域池时选择的 `--locale` 选项匹配。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --public-ip 18.97.0.41
```

示例响应：

```
{
```

```
"AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

有关更多信息，请参阅《Amazon EC2 用户指南》中的[将弹性 IP 地址与实例或网络接口相关联](#)。

步骤 11：清除

按照本部分中的步骤清除您在本教程中预置和创建的资源。运行本部分中的命令时，`--region` 的值必须包括您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项。

使用 AWS CLI 清除

1. 查看 IPAM 中管理的 EIP 分配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

输出将显示 IPAM 中的分配。

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "130.137.245.0/24",
      "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
      "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
      "ResourceType": "ec2-public-ipv4-pool",
      "ResourceOwner": "123456789012"
    }
  ]
}
```

2. 停止传播 IPv4 CIDR。

此步骤必须由 IPAM 账户完成。

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
profile ipam-account
```

在输出中，您将看到 CIDR 状态从 advertised (已传播) 更改为 provisioned (已预置)。

```
{
  "ByoipCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "provisioned"
  }
}
```

3. 释放弹性 IP 地址。

此步骤必须由成员账户完成。

```
aws ec2 release-address --region us-west-2 --allocation-id eipalloc-0db3405026756dbf6 --profile member-account
```

运行此命令时，您不会看到任何输出。

4. 查看 IPAM 中不再管理的 EIP 分配。IPAM 可能需要一些时间才能发现弹性 IP 地址已被删除。在看到已从 IPAM 中删除分配之前，您无法继续清理和取消预置 IPAM 池 CIDR。运行本部分中的命令时，`--region` 的值必须包括您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项。

此步骤必须由 IPAM 账户完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

输出将显示 IPAM 中的分配。

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

5. 取消预置区域池 CIDR。运行本步骤中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由 IPAM 账户完成。

```
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
```

在输出中，您将看到 CIDR 待定取消预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "pending-deprovision"
  }
}
```

取消预置需要一些时间才能完成。检查取消预置的状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

等到您看到 deprovisioned (取消预置) 后再继续下一步。

```
{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "deprovisioned"
  }
}
```

6. 删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成。完成《AWS RAM 用户指南》中 [删除 AWS RAM 中的资源共享](#) 和 [禁用与 AWS Organizations 的资源共享](#) 所述的步骤，删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成。

此步骤必须分别由 IPAM 账户和管理账户完成。要使用 AWS CLI 删除 RAM 共享并禁用 RAM 集成，请使用 `--profile ipam-account` 和 `--profile management-account` 选项。

7. 删除区域池。运行本步骤中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

在输出中，您可以看到删除状态。

```
{
  "IpamPool": {
    "OwnerId": "123456789012",
    "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
    "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
    "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-pool-0d8f3646b61ca5987",
    "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-scope-0087d83896280b594",
    "IpamScopeType": "public",
    "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
    "Locale": "us-east-1",
    "PoolDepth": 2,
    "State": "delete-in-progress",
    "Description": "reg-ipv4-pool",
    "AutoImport": false,
    "Advertisable": true,
    "AddressFamily": "ipv4"
  }
}
```

8. 取消预置顶级池 CIDR。运行本步骤中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由 IPAM 账户完成。

```
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
```

在输出中，您将看到 CIDR 待定取消预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
  }
}
```

```
    "State": "pending-deprovision"
  }
}
```

取消预置需要一些时间才能完成。运行以下命令检查取消预置的状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-  
pool-0a03d430ca3f5c035 --profile ipam-account
```

等到您看到 deprovisioned (取消预置) 后再继续下一步。

```
{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "deprovisioned"
  }
}
```

9. 删除顶级池。运行本步骤中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-  
pool-0a03d430ca3f5c035 --profile ipam-account
```

在输出中，您可以看到删除状态。

```
{
  "IpamPool": {
    "OwnerId": "123456789012",
    "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
    "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-  
pool-0a03d430ca3f5c035",
```

```
    "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-  
scope-0087d83896280b594",  
    "IpamScopeType": "public",  
    "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",  
    "Locale": "us-east-1",  
    "PoolDepth": 2,  
    "State": "delete-in-progress",  
    "Description": "top-level-pool",  
    "AutoImport": false,  
    "Advertisable": true,  
    "AddressFamily": "ipv4"  
  }  
}
```

10. 删除 IPAM。运行本步骤中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --  
profile ipam-account
```

在输出中，您将看到 IPAM 响应。这意味着 IPAM 已删除。

```
{  
  "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"
      }
    ],
  }
}
```

步骤 9 的替代方案

如果您使用公有 IPv4 池来分配弹性 IP 地址，则可以本部分中的步骤，而不是 [步骤 9：从池中分配弹性 IP 地址](#) 中的步骤。

内容

- [步骤 1：创建公有 IPv4 池](#)
- [步骤 2：将公有 IPv4 CIDR 预调配到您的公有 IPv4 池](#)
- [步骤 3：从公有 IPv4 池创建弹性 IP 地址](#)
- [步骤 9 清理的替代方案](#)

步骤 1：创建公有 IPv4 池

此步骤通常由不同的想要预调配弹性 IP 地址的 AWS 账户完成，如成员账户。

Important

公有 IPv4 池和 IPAM 池由 AWS 中的不同资源管理。公共 IPv4 池是单一账户资源，使您能够将公有 CIDR 转换为弹性 IP 地址。IPAM 池可用于将公有空间分配给公有 IPv4 池。

要使用 AWS CLI 创建公有 IPv4 池

- 请运行以下命令以预置 CIDR。运行本部分中的命令时，`--region` 的值必须与您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项匹配。

```
aws ec2 create-public-ipv4-pool --region us-west-2 --profile member-account
```

在输出中，您将看到公有 IPv4 池 ID。在下一步骤中，您需要用到此 ID。

```
{
  "PoolId": "ipv4pool-ec2-0019eed22a684e0b2"
```

```
}
```

步骤 2：将公有 IPv4 CIDR 预调配到您的公有 IPv4 池

将公有 IPv4 CIDR 预置到您的公有 IPv4 池。--region 的值为必须与您在创建将用于 BYOIP CIDR 的池时输入的 --locale 值匹配。您可以定义的最不具体的 --netmask-length 是 24。

此步骤必须由成员账户完成。

要使用 AWS CLI 创建公有 IPv4 池

1. 请运行以下命令以预置 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
```

在输出中，您将看到预置的 CIDR。

```
{
  "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
  "PoolAddressRange": {
    "FirstAddress": "130.137.245.0",
    "LastAddress": "130.137.245.255",
    "AddressCount": 256,
    "AvailableAddressCount": 256
  }
}
```

2. 运行以下命令，以查看公有 IPv4 池中预置的 CIDR。

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-account
```

在输出中，您将看到预置的 CIDR。默认情况下，CIDR 不会被传播，这意味着它不能通过互联网公开访问。在本教程的最后一步中，您将有机会将此 CIDR 设置为进行传播。

```
{
  "ByoipCidrs": [
    {
```

```

        "Cidr": "130.137.245.0/24",
        "StatusMessage": "Cidr successfully provisioned",
        "State": "provisioned"
    }
]
}

```

步骤 3：从公有 IPv4 池创建弹性 IP 地址

从公有 IPv4 池创建弹性 IP 地址 (EIP)。运行本部分中的命令时，`--region` 的值必须与您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项匹配。

此步骤必须由成员账户完成。

要使用 AWS CLI 从公有 IPv4 池中创建 EIP

1. 运行以下命令以创建 EIP。

```
aws ec2 allocate-address --region us-west-2 --public-ipv4-pool ipv4pool-ec2-0019eed22a684e0b2 --profile member-account
```

在输出中，您将看到分配。

```

{
  "PublicIp": "130.137.245.100",
  "AllocationId": "eipalloc-0db3405026756dbf6",
  "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
  "NetworkBorderGroup": "us-east-1",
  "Domain": "vpc"
}

```

2. 运行以下命令，以查看 IPAM 中管理的 EIP 分配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

输出将显示 IPAM 中的分配。

```
{
```

```
"IpamPoolAllocations": [  
  {  
    "Cidr": "130.137.245.0/24",  
    "IpamPoolAllocationId": "ipam-pool-  
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",  
    "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",  
    "ResourceType": "ec2-public-ipv4-pool",  
    "ResourceOwner": "123456789012"  
  }  
]
```

步骤 9 清理的替代方案

完成以下步骤，以清理使用步骤 9 的替代方法创建的公有 IPv4 池。在 [步骤 10：清除](#) 中的标准清理过程中，您应在释放弹性 IP 地址后完成这些步骤。

1. 查看您的 BYOIP CIDR。

此步骤必须由成员账户完成。

```
aws ec2 describe-public-ipv4-pools --region us-west-2 --profile member-account
```

在输出中，您将看到 BYOIP CIDR 中的 IP 地址。

```
{  
  "PublicIpv4Pools": [  
    {  
      "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",  
      "Description": "",  
      "PoolAddressRanges": [  
        {  
          "FirstAddress": "130.137.245.0",  
          "LastAddress": "130.137.245.255",  
          "AddressCount": 256,  
          "AvailableAddressCount": 256  
        }  
      ],  
      "TotalAddressCount": 256,  
      "TotalAvailableAddressCount": 256,  
      "NetworkBorderGroup": "us-east-1",  
    }  
  ]  
}
```

```

        "Tags": []
    }
]
}

```

2. 从公有 IPv4 池中释放 CIDR。运行本部分中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由成员账户完成。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.0/24 --profile member-account
```

3. 再次查看您的 BYOIP CIDR，并确保没有更多的预置地址。运行本部分中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由成员账户完成。

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
```

在输出中，您将看到公有 IPv4 池中的 IP 地址计数。

```

{
  "PublicIpv4Pools": [
    {
      "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
      "Description": "",
      "PoolAddressRanges": [],
      "TotalAddressCount": 0,
      "TotalAvailableAddressCount": 0,
      "NetworkBorderGroup": "us-east-1",
      "Tags": []
    }
  ]
}

```

仅使用 AWS CLI 自带 IPv6 CIDR 到 IPAM 中

按照以下步骤将 IPv6 CIDR 带入 IPAM 中，然后仅使用 AWS CLI 分配 VPC。

如果不需要通过互联网公开发布 IPv6 地址，则可向 IPAM 预置私有 GUA IPv6 地址。有关更多信息，请参阅 [启用预置私有 IPv6 GUA CIDR](#)。

Important

- 本教程假定您已完成以下部分中的步骤：
 - [将 IPAM 与 AWS Organization 中的账户集成](#)。
 - [创建 IPAM](#)。
- 本教程的每个步骤都必须由以下三个 AWS Organizations 账户之一完成：
 - 管理账户。
 - [将 IPAM 与 AWS Organization 中的账户集成](#) 中配置为 IPAM 管理员的成员账户。在本教程中，此账户将被称为 IPAM 账户。
 - 将从 IPAM 池中分配 CIDR 的企业中的成员账户。在本教程中，此账户将被称为成员账户。

内容

- [第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色](#)
- [步骤 2：创建 IPAM](#)
- [步骤 3：创建 IPAM 池](#)
- [步骤 4：向顶级池预置 CIDR](#)
- [步骤 5：在顶级池中创建区域池](#)
- [步骤 6：向区域池预置 CIDR](#)
- [第 7 步。共享区域池](#)
- [第 8 步：使用 IPv6 CIDR 创建 VPC](#)
- [步骤 9：传播 CIDR](#)
- [步骤 10：清除](#)

第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色

要以单个 AWS 用户的身份完成本教程，您可以使用 AWS CLI 命名配置文件在 IAM 角色之间切换。[命名配置文件](#) 是您在将 `--profile` 选项与 AWS CLI 结合使用时引用的设置和凭证集合。有关如何为 AWS 账户创建 IAM 角色和命名配置文件的更多信息，请参阅[在 AWS CLI 中使用 IAM 角色](#)。

为您将在本教程中使用的三个 AWS 账户分别创建一个角色和一个命名配置文件：

- 为 AWS Organizations 管理账户创建名为 `management-account` 的配置文件。
- 为配置为 IPAM 管理员的 AWS Organizations 成员账户创建名为 `ipam-account` 的配置文件。
- 为将从 IPAM 池中分配 CIDR 的企业中的 AWS Organizations 成员账户创建名为 `member-account` 的配置文件。

创建 IAM 角色和命名配置文件后，请返回本页面并转至下一步。在本教程的其余部分中，您将注意到示例 AWS CLI 命令会将 `--profile` 选项与其中一个命名配置文件一起使用，以指示哪个账户必须运行该命令。

步骤 2：创建 IPAM

此为可选步骤。如果您已在创建了 `us-east-1` 和 `us-west-2` 的运营区域的情况下创建了 IPAM，您可以跳过此步骤。创建 IPAM 并指定 `us-east-1` 和 `us-west-2` 的运营区域。您必须选择一个运营区域，以便在创建 IPAM 池时可以使用区域设置选项。IPAM 与 BYOIP 集成要求在将用于 BYOIP CIDR 的任何一个池上设置区域设置。

此步骤必须由 IPAM 账户完成。

运行如下命令：

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

在输出中，您将看到您创建的 IPAM。记下 `PublicDefaultScopeId` 值。在下一步中，您将需要使用公有范围 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": []
}
}

```

步骤 3：创建 IPAM 池

由于您将创建一个其中包含一个区域池的顶级 IPAM 池，并且我们将为区域池中的资源 (VPC) 分配空间，因此您将在区域池中设置区域设置，而不是在顶级池中。在后面的步骤中创建区域池时，您将区域设置添加到区域池中。IPAM 与 BYOIP 集成要求在将用于 BYOIP CIDR 的任何一个池上设置区域设置。

此步骤必须由 IPAM 账户完成。

选择是否希望此 IPAM 池 CIDR 可以由 AWS 通过公共互联网 (`--publicly-advertisable` 或 `--no-publicly-advertisable`) 传播。

Note

请注意，范围 ID 必须是公有范围的 ID，且地址系列必须是 ipv6。

要使用 AWS CLI 为您的所有 AWS 资源创建 IPv6 地址池

1. 运行以下命令以创建 IPAM 池。请使用您在上一步中创建的 IPAM 的公有范围的 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

```

在输出中，您将会看到 `create-in-progress`，这表明池的创建正在进行中。

```

{
  "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. 运行以下命令，直到您在输出中看到 `create-complete` 的状态。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

下面的示例输出显示池的状态。

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

步骤 4：向顶级池预置 CIDR

向顶级池预置 CIDR 块。请注意，在将 IPv6 CIDR 预置到顶级池中的池时，对于公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /48；对于不公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /60。

Note

- 如果[使用 X.509 证书验证域控制权](#)，则必须包含 CIDR 和 BYOIP 消息以及在该步骤中创建的证书签名，以便我们验证您是否控制了公共空间。
- 如果[使用 DNS TXT 记录验证域控制权](#)，则必须包含 CIDR 和 IPAM 消息以及在该步骤中创建的验证令牌，以便我们验证您是否控制了公共空间。

在向顶级池预置 BYOIP CIDR 时，您只需要验证域控制权。对于顶级池中的区域池，您可以省略域所有权选项。

此步骤必须由 IPAM 账户完成。

使用 AWS CLI 向池预置 CIDR 块

1. 要为 CIDR 预置证书信息，请使用以下示例命令。除了根据需要替换示例中的值外，务必还要将 Message 和 Signature 值替换为在 [使用 X.509 证书验证域](#) 中获得的 text_message 和 signed_message 值。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-CR7HqMwzcgdS9R1pBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxnP7RAJDvF1mBwxmSgH~CvP6LON3y00Xmp4JENB9uM7sM1u6oeoutGyyhXFeYPz1GSRdcdfKNKaimvPCqVsxGN5AwSi1KQ8byNqoa~G3dvs8ueSawispi~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

要为 CIDR 预置验证令牌信息，请使用以下示例命令。除了根据需要替换示例中的值外，务必还要将 ipam-ext-res-ver-token-0309ce7f67a768cf0 替换为在 [使用 DNS TXT 记录验证域](#) 中获得的 IpamExternalResourceVerificationTokenId 令牌 ID。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method dns-token --ipam-external-resource-verification-token-id ipam-ext-res-ver-token-0309ce7f67a768cf0 --profile ipam-account
```

在输出中，您将看到 CIDR 待定预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "pending-provision"
  }
}
```

2. 在继续之前，请确保已预置此 CIDR。

Important

虽然大多数预配置将在两小时内完成，但对于公开发布的范围，完成预配置过程可能需要长达一周的时间。

运行以下命令，直到您在输出中看到 `provisioned` 的状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --profile ipam-account
```

下面的示例输出显示状态。

```
{
  "IpamPoolCidrs": [
    {
      "Cidr": "2605:9cc0:409::/48",
      "State": "provisioned"
    }
  ]
}
```

步骤 5：在顶级池中创建区域池

在顶级池中创建区域池。`--locale` 在池上是必需的，它必须是您在创建 IPAM 时配置的运营区域之一。

此步骤必须由 IPAM 账户完成。

Important

创建池时，您必须包括 `--aws-service ec2`。您选择的服务将决定可传播 CIDR 的 AWS 服务。目前，唯一的选择是 `ec2`，这意味着从此池中分配的 CIDR 在 Amazon EC2 服务和 Amazon VPC 服务（适用于与 VPC 关联的 CIDR）中是可传播的。

要使用 AWS CLI 创建区域池

1. 运行以下命令以创建池。

```
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
```

在输出中，您将看到创建池的 IPAM。

```
{
  "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. 运行以下命令，直到您在输出中看到 create-complete 的状态。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

在输出中，您可以看到您在 IPAM 中拥有的池。在本教程中，我们创建了一个顶级池和一个区域池，所以您会看到这两个池。

步骤 6：向区域池预置 CIDR

向区域池预置 CIDR 块。请注意，在将 CIDR 预置到顶级池中的池时，对于公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /48；对于不公开发布的 CIDR，可以引入的最具体 IPv6 地址范围是 /60。

此步骤必须由 IPAM 账户完成。

要使用 AWS CLI 将 CIDR 块分配到区域池

1. 请运行以下命令以预置 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
```

在输出中，您将看到 CIDR 待定预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "pending-provision"
  }
}
```

2. 运行以下命令，直到您在输出中看到 provisioned 的状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

下面的示例输出显示正确的状态。

```
{
  "IpamPoolCidrs": [
    {
      "Cidr": "2605:9cc0:409::/48",
      "State": "provisioned"
    }
  ]
}
```

第 7 步。共享区域池

按照本部分中的步骤使用 AWS Resource Access Manager (RAM) 共享 IPAM 池。

在 AWS RAM 中启用资源共享

创建 IPAM 后，您需要与组织中的其他账户共享区域池。在共享 IPAM 池之前，请先完成本部分中的步骤，启用与 AWS RAM 的资源共享。如果要使用 AWS CLI 启用资源共享，请使用 `--profile management-account` 选项。

启用资源共享

1. 使用 AWS Organizations 管理账户打开 AWS RAM 控制台，地址：<https://console.aws.amazon.com/ram/>。
2. 在左侧导航窗格中，依次选择设置、启用与 AWS Organizations 共享、保存设置。

您现在可以与组织的其他成员共享 IPAM 池。

使用 AWS RAM 共享 IPAM 池

在这一部分，您将与其他 AWS Organizations 成员账户共享区域池。有关共享 IPAM 池的完整说明，例如所需 IAM 权限的相关信息，请参阅 [使用 AWS RAM 共享 IPAM 池](#)。如果要使用 AWS CLI 启用资源共享，请使用 `--profile ipam-account` 选项。

使用 AWS RAM 共享 IPAM 池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 依次选择私有范围、IPAM 池以及操作 > 查看详细信息。
4. 在资源共享下，选择创建资源共享。AWS RAM 控制台将打开。您将使用 AWS RAM 来共享该池。
5. 选择创建资源共享。
6. 在 AWS RAM 控制台中，再次选择创建资源共享。
7. 为共享资源添加名称。
8. 在选择资源类型下，选择 IPAM 池，然后选择要共享的池的 ARN。
9. 选择下一步。
10. 选择 `AWSRAMPermissionIpamPoolByoipCidrImport` 权限。本教程不提供权限选项的详细信息，但您可以在 [使用 AWS RAM 共享 IPAM 池](#) 中查看有关这些选项的更多信息。

11. 选择下一步。
12. 在委托人 > 选择主体类型下，选择 AWS 账户，输入要为 IPAM 提供 IP 地址范围的账户的账户 ID，然后选择添加。
13. 选择下一步。
14. 查看资源共享选项和要共享的主体，然后选择创建。
15. 要允许 **member-account** 账户从 IPAM 池中分配 IP 地址 CIDRS，请使用 `AWSRAMDefaultPermissionsIpamPool` 创建第二个资源共享。 `--resource-arns` 的值是您在上一部分中创建的 IPAM 池的 ARN。 `--principals` 的值是 **member-account** 的账户 ID。 `--permission-arns` 的值是 `AWSRAMDefaultPermissionsIpamPool` 权限的 ARN。

第 8 步：使用 IPv6 CIDR 创建 VPC

使用 IPAM 池 ID 创建 VPC。您还必须使用 `--cidr-block` 选项将 IPv4 CIDR 块与 VPC 关联，否则请求将失败。运行本部分中的命令时，`--region` 的值必须与您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项匹配。

此步骤必须由成员账户完成。

要使用 AWS CLI 通过 IPv6 CIDR 创建 VPC

1. 请运行以下命令以预置 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
```

在输出中，您将看到正在创建的 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. 在 IPAM 中查看 VPC 分配情况。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

在输出中，您将看到 IPAM 中的分配。

```

{
  "IpamPoolAllocations": [
    {
      "Cidr": "2605:9cc0:409::/56",
      "IpamPoolAllocationId": "ipam-pool-alloc-5f8db726fb9e4ff0a33836e649283a52",
      "ResourceId": "vpc-00b5573ffc3b31a29",
      "ResourceType": "vpc",
      "ResourceOwner": "123456789012"
    }
  ]
}

```

步骤 9：传播 CIDR

一旦您使用 IPAM 中分配的 CIDR 创建了 VPC，就可以开始传播您带入位于定义了 `--aws-service ec2` 的池中的 AWS 的 CIDR。在本教程中，这就是您的区域池。默认情况下，CIDR 不会被传播，这意味着它不能通过互联网公开访问。运行本部分中的命令时，`--region` 的值为必须与您在创建将用于 BYOIP CIDR 的区域池时输入的 `--locale` 选项匹配。

此步骤必须由 IPAM 账户完成。

开始使用 AWS CLI 传播 CIDR

- 请运行以下命令以传播 CIDR。

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --  
profile ipam-account
```

在输出中，您将看到 CIDR 被传播。

```
{  
  "ByoipCidr": {  
    "Cidr": "2605:9cc0:409::/48",  
    "State": "advertised"  
  }  
}
```

步骤 10：清除

按照本部分中的步骤清除您在本教程中预置和创建的资源。运行本部分中的命令时，`--region` 的值为必须与您在创建将用于 BYOIP CIDR 的区域池时输入的 `--locale` 选项匹配。

使用 AWS CLI 清除

- 运行以下命令以查看 IPAM 中管理的 VPC 分配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-  
pool-0053b7d2b4fc3f730 --profile ipam-account
```

输出将显示 IPAM 中的分配。

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "2605:9cc0:409::/56",
      "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
      "ResourceId": "vpc-00b5573ffc3b31a29",
      "ResourceType": "vpc",
      "ResourceOwner": "123456789012"
    }
  ]
}
```

2. 运行以下命令以停止传播 CIDR。运行本步骤中的命令时，`--region` 的值为必须与您在创建将用于 BYOIP CIDR 的区域池时输入的 `--locale` 选项匹配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

在输出中，您将看到 CIDR 状态从 `advertised` (已传播) 更改为 `provisioned` (已预置)。

```
{
  "ByoipCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "provisioned"
  }
}
```

3. 运行以下命令以删除 VPC。运行本部分中的命令时，`--region` 的值为必须与您在创建将用于 BYOIP CIDR 的区域池时输入的 `--locale` 选项匹配。

此步骤必须由成员账户完成。

```
aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
profile member-account
```

运行此命令时，您不会看到任何输出。

4. 运行以下命令以查看 IPAM 中的 VPC 分配情况。IPAM 可能需要一些时间才能发现 VPC 已被删除并删除此分配。运行本部分中的命令时，`--region` 的值为必须与您在创建将用于 BYOIP CIDR 的区域池时输入的 `--locale` 选项匹配。

此步骤必须由 IPAM 账户完成。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

输出将显示 IPAM 中的分配。

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "2605:9cc0:409::/56",
      "IpamPoolAllocationId": "ipam-pool-alloc-5f8db726fb9e4ff0a33836e649283a52",
      "ResourceId": "vpc-00b5573ffc3b31a29",
      "ResourceType": "vpc",
      "ResourceOwner": "123456789012"
    }
  ]
}
```

重新运行命令并查找要删除的分配。在看到已从 IPAM 中删除分配之前，您无法继续清理和取消预置 IPAM 池 CIDR。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

输出将显示从 IPAM 中删除的分配。

```
{
```

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

- 删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成。完成《AWS RAM 用户指南》中 [删除 AWS RAM 中的资源共享](#) 和 [禁用与 AWS Organizations 的资源共享](#) 所述的步骤，删除 RAM 共享并禁用与 AWS Organizations 的 RAM 集成。

此步骤必须分别由 IPAM 账户和管理账户完成。要使用 AWS CLI 删除 RAM 共享并禁用 RAM 集成，请使用 `--profile ipam-account` 和 `--profile management-account` 选项。

- 运行以下命令以取消预置区域池 CIDR。

此步骤必须由 IPAM 账户完成。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

在输出中，您将看到 CIDR 待定取消预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "pending-deprovision"
  }
}
```

取消预置需要一些时间才能完成。继续运行命令，直到看到 CIDR 状态 `deprovisioned` (已取消预置)。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

在输出中，您将看到 CIDR 待定取消预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "deprovisioned"
  }
}
```

7. 运行以下命令，以删除区域池。

此步骤必须由 IPAM 账户完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

在输出中，您可以看到 delete (删除) 状态。

```
{
  "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. 运行以下命令以取消预置顶级池 CIDR。

此步骤必须由 IPAM 账户完成。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

在输出中，您将看到 CIDR 待定取消预置。

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
  }
}
```

```
    "State": "pending-deprovision"
  }
}
```

取消预置需要一些时间才能完成。运行以下命令检查取消预置的状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-  
pool-07f2466c7158b50c4 --profile ipam-account
```

等到您看到 deprovisioned (取消预置) 后再继续下一步。

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "deprovisioned"
  }
}
```

9. 运行以下命令以删除顶级池。

此步骤必须由 IPAM 账户完成。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-  
pool-07f2466c7158b50c4 --profile ipam-account
```

在输出中，您可以看到删除状态。

```
{
  "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. 运行以下命令以删除 IPAM。

此步骤必须由 IPAM 账户完成。

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

在输出中，您将看到 IPAM 响应。这意味着 IPAM 已删除。

```
{
  "Ipam": {
    "OwnerId": "123456789012",
    "IpamId": "ipam-090e48e75758de279",
    "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
    "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",
    "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",
    "ScopeCount": 2,
    "OperatingRegions": [
      {
        "RegionName": "us-east-1"
      },
      {
        "RegionName": "us-west-2"
      }
    ]
  }
}
```

使用 IPAM 自带 IP 到 CloudFront

借助使用全局服务的 IPAM BYOIP，您可以将自己的 IPv4 地址用于 CloudFront 等 AWS 全局服务。与区域 BYOIP 不同，您的 IP 地址将通过任播路由从多个边缘站点同时公布。

为什么要使用此功能？

- 维护 IP 允许列表：使用现有批准的 IP 地址，而无需更新防火墙配置
- 简化迁移：无需更改 IP 基础设施即可从其他 CDN 迁移
- 一致的品牌：在迁移到 AWS 时保留现有的 IP 地址空间

此功能的使用对象

需要使用自己的 IP 地址进行全球内容分发的组织：

- 具有 IP 允许列表要求的大型企业
- 使用现有 IP 地址从其他 CDN 迁移的公司
- 具有严格安全策略且要求特定 IP 范围的组织

此功能的使用场景

适用于全局服务的 BYOIP 适合以下使用场景：

- 维护合作伙伴/客户的现有 IP 允许列表
- 使用您的 IP 地址从其他 CDN 迁移
- 满足特定 IP 范围的合规性要求

Note

需要 /24 IPv4 CIDR 数据块。目前仅适用于 CloudFront。

先决条件

在开始之前，请完成以下步骤：

- IPAM 设置：[将 IPAM 与 AWS Organization 中的账户集成](#)和[创建 IPAM](#)

- 域验证：[验证域控制权](#)
- 创建顶级池：按照[自带 IPv4 CIDR 到 IPAM](#) 中的第 1-2 步进行操作。

全局服务配置步骤

以下步骤不同于标准区域 BYOIP 流程，并且将建立用于全球服务的模式：

第 1 步：为任播服务创建一个全局池

为任播服务创建一个全局池，而不是区域池：

控制台

使用控制台创建全局池：

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择池
3. 选择创建池
4. 源：选择您的顶级 BYOIP 池
5. 区域设置：选择全局
6. 服务：选择全局服务（将在选择“全局”后显示）
7. 公有 IP 源：选择 BYOIP
8. 要预调配的 CIDR：指定您的 /24 CIDR 范围
9. 选择创建池

CLI

使用 `aws ec2 create-ipam-pool` 并将区域设置为“Global”，将地址系列设置为“ipv4”。

然后使用 `aws ec2 provision-ipam-pool-cidr` 预调配该 CIDR。

Important

您必须将完整的 /24 数据块分配给该池。您可以在该数据块中预调配更具体的范围，以满足不同用途的需要。

第 2 步：创建特定于服务的资源

对于 CloudFront，创建一个将使用您的 IPAM 池的任播 IP 列表。有关详细说明，请参阅 CloudFront BYOIP 文档（链接待定）。

IPAM 集成的关键参数：

- IP 地址类型：请选择 BYOIP
- IPAM 池：请选择第 1 步中的全局池
- IP 数量：请输入 3（对于 CloudFront 为必需）

第 3 步：关联到服务资源

将您的任播静态 IP 列表关联到某个 CloudFront 分配。有关详细说明，请参阅 CloudFront BYOIP 文档（链接待定）。

关键配置：

- 在分配设置中，请选择第 2 步中的任播 IP 列表

步骤 4：准备迁移

- DNS TTL 下限：请将记录的 DNS TTL 设置为 60 秒或更短
- 传播等待：新 TTL 在互联网上生效所需的时间

步骤 5：全球公布 CIDR

使用 IPAM 全局公开命令：

控制台

使用控制台公开 CIDR：

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择池
3. 选择您的全局池
4. 选择 CIDR 选项卡。

5. 选择您的 CIDR，然后选择操作 > 公开 CIDR

6. 确认公开

CLI

使用您的 IPAM 池 ID 和 CIDR 执行 `aws ec2 advertise-ipam-byoip-cidr`。

Important

- 在运行此命令之前，请撤回来自之前提供商的公开消息
- 将 DNS 记录更新为指向 CloudFront，以完成迁移

清理

清理在本教程中创建的资源：

- 删除 CloudFront 资源：按照 CloudFront BYOIP 文档中的清理说明进行操作（链接待定）
- 撤回 CIDR 并删除 IPAM 池：按照[步骤 8：清除](#)中的标准清理流程进行操作

Important

请先删除 CloudFront 资源，然后再清理 IPAM，以避免造成服务中断。

教程：将 BYOIP IPv4 CIDR 传输到 IPAM

按照以下步骤将现有的 IPv4 CIDR 传输到 IPAM。如果您已拥有 AWS 的 IPv4 BYOIP CIDR，则可以将 CIDR 从公有 IPv4 池移动到 IPAM。您不能将 IPv6 CIDR 移动到 IPAM。

本教程假定您已使用在[Amazon EC2 中使用您自己的 IP 地址 \(BYOIP\)](#)中所述的过程，成功将 IP 地址范围带到 AWS，并且您现在希望将该 IP 地址范围转移到 IPAM。如果您是第一次将新 IP 地址引入 AWS，请完成[教程：将 IP 地址带入 IPAM](#)中的步骤。

如果您将公有 IPv4 池转移到 IPAM，则不会影响现有分配。将公有 IPv4 池转移到 IPAM 后，根据资源类型，您可能能够监控现有分配。有关更多信息，请参阅[按资源监控 CIDR 使用情况](#)。

Note

- 本教程假设您已完成 [创建 IPAM](#) 中的步骤。
- 本教程的每个步骤都必须由以下两个 AWS 账户之一完成：
 - IPAM 管理员的账户。在本教程中，此账户将被称为 IPAM 账户。
 - 您的组织中拥有 BYOIP CIDR 的账户。在本教程中，此账户将被称为 BYOIP CIDR 拥有者账户。

内容

- [第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色](#)
- [步骤 2：获取 IPAM 的公有范围 ID](#)
- [步骤 3：创建 IPAM 池](#)
- [步骤 4：使用 AWS RAM 共享 IPAM 池](#)
- [步骤 5：将现有的 BYOIP IPV4 CIDR 传输到 IPAM](#)
- [步骤 6：在 IPAM 中查看 CIDR](#)
- [步骤 7：清除](#)

第 1 步：创建 AWS CLI 命名配置文件和 IAM 角色

要以单个 AWS 用户的身份完成本教程，您可以使用 AWS CLI 命名配置文件在 IAM 角色之间切换。[命名配置文件](#) 是您在将 `--profile` 选项与 AWS CLI 结合使用时引用的设置和凭证集合。有关如何为 AWS 账户创建 IAM 角色和命名配置文件的更多信息，请参阅[在 AWS CLI 中使用 IAM 角色](#)。

为您将在本教程中使用的三个 AWS 账户分别创建一个角色和一个命名配置文件：

- 为 IPAM 管理员 AWS 账户创建名为 `ipam-account` 的配置文件。
- 为您所在企业中拥有 BYOIP CIDR 的 AWS 账户创建名为 `byoip-owner-account` 的配置文件。

创建 IAM 角色和命名配置文件后，请返回本页面并转至下一步。在本教程的其余部分中，您将注意到示例 AWS CLI 命令会将 `--profile` 选项与其中一个命名配置文件一起使用，以指示哪个账户必须运行该命令。

步骤 2：获取 IPAM 的公有范围 ID

请按照本部分中的步骤获取 IPAM 的公有范围 ID。此步骤应该由 **ipam-account** 账户执行。

运行以下命令以获取您的公有范围 ID。

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

在输出中，您将看到自己的公有范围 ID。记下 `PublicDefaultScopeId` 的值。您在下一个步骤中需要使用此值。

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

步骤 3：创建 IPAM 池

按照本部分中的步骤创建 IPAM 池。此步骤应该由 **ipam-account** 账户执行。您创建的 IPAM 池必须是 `--locale` 选项与 BYOIP CIDR AWS 区域匹配的顶级池。您只能将 BYOIP 传输到顶级 IPAM 池。

⚠ Important

创建池时，您必须包括 `--aws-service ec2`。您选择的服务将决定可传播 CIDR 的 AWS 服务。目前，唯一的选择是 `ec2`，这意味着从此池中分配的 CIDR 在 Amazon EC2 服务（适用于弹性 IP 地址）和 Amazon VPC 服务（适用于与 VPC 关联的 CIDR）中是可传播的。

要使用 AWS CLI 为传输的 BYOIP CIDR 创建 IPv4 地址池

1. 运行以下命令以创建 IPAM 池。请使用您在上一步中检索的 IPAM 的公有范围的 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
```

在输出中，您将会看到 `create-in-progress`，这表明池的创建正在进行中。

```
{
  "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. 运行以下命令，直到您在输出中看到 `create-complete` 的状态。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

下面的示例输出显示池的状态。在下一步骤中，您需要用到 OwnerId。

```
{
  "IpamPools": [
    {
      "OwnerId": "123456789012",
      "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
      "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
      "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
      "IpamScopeType": "public",
      "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
      "Locale": "us-west-2",
      "PoolDepth": 1,
      "State": "create-complete",
      "Description": "top-level-pool",
      "AutoImport": false,
      "AddressFamily": "ipv4",
      "Tags": [],
      "AwsService": "ec2"
    }
  ]
}
```

步骤 4：使用 AWS RAM 共享 IPAM 池

按照本部分中的步骤使用 AWS RAM 来共享 IPAM 池，以便其他 AWS 账户可以将现有 BYOIP IPv4 CIDR 传输到 IPAM 池并使用 IPAM 池。此步骤应该由 **ipam-account** 账户执行。

使用 AWS CLI 共享 IPv4 地址池

1. 查看 IPAM 池可用的 AWS RAM 权限。您需要两个 ARN 才能完成本部分中的步骤。

```
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. 创建资源共享以使 **byoip-owner-account** 账户能够将 BYOIP CIDR 导入 IPAM。--resource-arns 的值是您在上一部分中创建的 IPAM 池的 ARN。--principals 的值是 BYOIP CIDR 拥有者账户的账户 ID。--permission-arns 的值是 AWSRAMPermissionIpamPoolByoipCidrImport 权限的 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. (可选) 如果要允许 **byoip-owner-account** 账户在传输完成后将 IP 地址 CIDRS 从 IPAM 池分配到公有 IPv4 池，请复制 `AWSRAMDefaultPermissionsIpamPool` 的 ARN 并创建第二个资源共享。--resource-arns 的值是您在上一部分中创建的 IPAM 池的 ARN。--principals 的值是 BYOIP CIDR 所有者账户的账户 ID。--permission-arns 的值是 `AWSRAMDefaultPermissionsIpamPool` 权限的 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"  
  }  
}
```

由于在 RAM 中创建了资源共享，byoip-owner-account 账户现在可以将 CIDR 移至 IPAM。

步骤 5：将现有的 BYOIP IPV4 CIDR 传输到 IPAM

按照本部分中的步骤将现有的 BYOIP IPV4 CIDR 传输到 IPAM。此步骤应该由 **byoip-owner-account** 账户执行。

Important

将 IPv4 地址范围设置为 AWS 后，您可以使用该范围内的所有 IP 地址，包括第一个地址（网络地址）和最后一个地址（广播地址）。

要将 BYOIP CIDR 传输到 IPAM，BYOIP CIDR 所有者必须在其 IAM 策略中拥有以下权限：

- ec2:MoveByoipCidrToIpam
- ec2:ImportByoipCidrToIpam

Note

您可以为此步骤使用 AWS 管理控制台 或 AWS CLI。

AWS Management Console

要将 BYOIP CIDR 传输到 IPAM 池，请执行以下操作：

1. 在 <https://console.aws.amazon.com/ipam/> 以 **byoip-owner-account** 账户身份打开 IPAM 控制台。
2. 在导航窗格中，选择池。

3. 选择在本教程中创建和共享的顶级池。
4. 选择操作 > 传输 BYOIP CIDR。
5. 选择传输 BYOIP CIDR。
6. 选择您的 BYOIP CIDR。
7. 选择预置。

Command line

使用 AWS CLI 通过以下 AWS CLI 命令将 BYIP CIDR 传输到 IPAM 池：

1. 请运行以下命令以传输 CIDR。确保 `--region` 值是 BYOIP CIDR 的 AWS 区域。

```
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
```

在输出中，您将看到 CIDR 待定预置。

```
{
  "ByoipCidr": {
    "Cidr": "130.137.249.0/24",
    "State": "pending-transfer"
  }
}
```

2. 确保 CIDR 已被传输。运行以下命令，直到您在输出中看到 `complete-transfer` 的状态。

```
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
```

下面的示例输出显示状态。

```
{
```

```
"ByoipCidr": {  
  "Cidr": "130.137.249.0/24",  
  "State": "complete-transfer"  
}  
}
```

步骤 6：在 IPAM 中查看 CIDR

请按照本部分中的步骤查看 IPAM 中的 CIDR。此步骤应该由 **ipam-account** 账户执行。

要使用 AWS CLI 在 IPAM 池中查看传输的 BYOIP CIDR

- 运行以下命令以查看 IPAM 中管理的分配。确保 `--region` 值是 BYOIP CIDR 的 AWS 区域。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --profile ipam-account --  
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

输出将显示 IPAM 中的分配。

```
{  
  "IpamPoolAllocations": [  
    {  
      "Cidr": "130.137.249.0/24",  
      "IpamPoolAllocationId": "ipam-pool-  
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",  
      "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",  
      "ResourceType": "ec2-public-ipv4-pool",  
      "ResourceOwner": "111122223333"  
    }  
  ]  
}
```

步骤 7：清除

按照本部分中的步骤删除您在本教程中创建的资源。此步骤应该由 **ipam-account** 账户执行。

要使用 AWS CLI 清除本教程中创建的资源

1. 要删除 IPAM 池共享资源，请运行以下命令以获取第一个资源共享 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. 复制资源共享 ARN 并使用它删除 IPAM 池资源共享。

```
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 [步骤 4：使用 AWS RAM 共享 IPAM 池](#) 中创建了额外的资源共享，请重复前两个步骤以获取 PoolShare2 的第二个资源共享 ARN，然后删除第二个资源共享。
4. 运行以下命令以获取 BYOIP CIDR 的分配 ID。确保 --region 值与 BYOIP CIDR 的 AWS 区域匹配。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --profile ipam-account --  
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

输出将显示 IPAM 中的分配。

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "130.137.249.0/24",
      "IpamPoolAllocationId": "ipam-pool-alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
      "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
      "ResourceType": "ec2-public-ipv4-pool",
      "ResourceOwner": "111122223333"
    }
  ]
}
```

5. 从公有 IPv4 池中释放 CIDR。运行本部分中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由 **byoip-owner-account** 账户完成。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --profile byoip-owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.0/24
```

6. 再次查看您的 BYOIP CIDR，并确保没有更多的预置地址。运行本部分中的命令时，`--region` 的值必须与 IPAM 的区域匹配。

此步骤必须由 **byoip-owner-account** 账户完成。

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
```

在输出中，您将看到公有 IPv4 池中的 IP 地址计数。

```
{
  "PublicIpv4Pools": [
    {
      "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
      "Description": "",
      "PoolAddressRanges": [],
      "TotalAddressCount": 0,
      "TotalAvailableAddressCount": 0,
      "NetworkBorderGroup": "us-east-1",
    }
  ]
}
```

```
        "Tags": []
      }
    ]
  }
}
```

7. 运行以下命令以删除顶级池。

```
aws ec2 delete-ipam-pool --region us-east-1 --profile ipam-account --ipam-pool-id ipam-pool-0a03d430ca3f5c035
```

在输出中，您可以看到删除状态。

```
{
  "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"
  }
}
```

教程：为子网 IP 分配规划 VPC IP 地址空间

完成本教程以规划用于为 VPC 子网分配 IP 地址的 VPC IP 地址空间，并在子网和 VPC 级别监控与 IP 地址相关的指标。

Note

本教程介绍如何在私有 IPAM 范围内向 VPC 和子网分配私有 IPv4 地址空间。您也可以使用 IPv6 CIDR 范围完成本教程，方法是在 VPC 控制台上使用 Amazon 提供的 IPv6 CIDR 块选项创建 VPC。

通过为子网规划 VPC IP 地址空间，您可以执行以下操作：

- 规划和整理 VPC 的 IP 地址以分配给子网：您可以将 VPC IP 地址空间划分为较小的 CIDR 块，并将这些 CIDR 块配置给具有不同业务需求的子网，例如在开发或生产子网中运行工作负载。
- 简化 VPC 子网的 IP 地址分配：规划和整理 VPC 的地址空间后，您可以选择网络掩码长度，而不必手动输入 CIDR。例如，如果开发人员正在创建用于托管开发工作负载的子网，他们需要为子网选择池和网络掩码长度，而 IPAM 会自动将 CIDR 块分配给您的子网。

以下示例显示了池的层次结构，以及您将使用本教程中创建的结构：

- 私有范围
 - 资源规划池 (10.0.0.0/20)
 - 开发子网池 (10.0.0.0/24)
 - 开发子网 (10.0.0.0/28)
 - 生产子网池 (10.0.0.1/24)
 - 生产子网 (10.0.0.16/28)

Important

- 资源规划池可用于将 CIDR 分配给子网，也可以作为源池，您可以在其中创建其他池。在本教程中，我们将资源规划池用作子网池的源池。
- 如果 VPC 预置了多个 CIDR，则可以使用同一 VPC 创建多个资源规划池；例如，如果一个 VPC 分配了两个 CIDR，则可以创建两个资源规划池，每个 CIDR 一个。每个 CIDR 一次可以分配给一个池。

第 1 步：创建 VPC

完成本部分中的步骤以创建用于子网 IP 地址规划的 VPC。有关创建 VPC 所需的 IAM 权限的更多信息，请参阅《Amazon VPC 用户指南》中的 [Amazon VPC 策略示例](#)。

Note

您可以使用现有 VPC 而不是创建新的 VPC，但本教程重点介绍使用手动分配的 CIDR 块配置 VPC，而不是 IPAM 自动分配的 CIDR 块的场景。

创建 VPC

1. 使用 IPAM 管理员账户打开 VPC 控制台，地址：<https://console.aws.amazon.com/vpc/>。
2. 选择创建 VPC。
3. 输入 VPC 的名称，如“tool-vpc”。
4. 选择 IPv4 CIDR 手动输入，然后输入 IPv4 CIDR 块。在本教程中，使用 10.0.0.0/20。
5. 跳过添加 IPv6 CIDR 块的选项。
6. 选择创建 VPC。
7. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
8. 在左侧导航窗格中，选择资源。
9. 等待您创建的 VPC 出现。这需要一定的时间，您可能需要刷新窗口才能看到它出现。VPC 必须先由 IPAM 发现，然后才能继续执行下一步。

步骤 2：创建资源规划池

完成本部分中的步骤以创建资源规划池。

要创建资源规划池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 选择私有作用域。
4. 选择创建池。

5. 在 IPAM 范围下，确保选中私有范围。
6. （可选）添加池的名称标签，如“资源规划池”。
7. 在源下，选择 IPAM 范围。
8. 在资源规划下，选择规划 VPC 内的 IP 空间，然后选择您在上一步中创建的 VPC。VPC 是用于向资源规划池配置 CIDR 的资源。
9. 在要预置的 CIDR 下，选择要为资源池预置的 VPC CIDR。您为资源规划池配置的 CIDR 必须与预置到 VPC 的 CIDR 相匹配。在本教程中，使用 10.0.0.0/20。
10. 选择创建池。
11. 创建池后，选择 CIDR 选项卡以查看已预置的 CIDR 的状态。刷新页面，等待 CIDR 状态从“待预置”变为“已预置”，然后再进入下一步。

步骤 3：创建子网池

完成本部分中的步骤以创建两个子网池，它们将用于向子网分配 IP 空间。

要创建子网池

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 选择私有作用域。
4. 选择创建池。
5. 在 IPAM 范围下，确保选中私有范围。
6. （可选）添加池的名称标签，如“开发子网池”。
7. 在源下，选择 IPAM 池，然后选择您在步骤 3 中创建的资源计划池。地址系列、资源规划配置和区域设置是自动从源池继承的。
8. 在要预置的 CIDR 下，选择要为子网池预置的 CIDR。在本教程中，使用 10.0.0.0/24。
9. 选择创建池。
10. 创建池后，选择 CIDR 选项卡以查看已预置的 CIDR 的状态。刷新页面，等待 CIDR 状态从“待预置”变为“已预置”，然后再进入下一步。
11. 重复此过程以创建另一个名为“生产子网池”的子网。

此时，如果您想让其他 AWS 账户可以使用该子网池，则可以共享该子网池。有关如何执行此操作的说明，请参阅[使用 AWS RAM 共享 IPAM 池](#)。然后返回此处完成教程。

步骤 4：创建子网

完成这些步骤以创建两个子网。

要创建子网

1. 使用适当的账户打开 VPC 控制台，地址：<https://console.aws.amazon.com/vpc/>。
2. 选择子网 > 创建子网。
3. 选择您在本教程开始时创建的 VPC。
4. 输入子网的名称，如“tutorial-subnet”。
5. （可选）选择一个可用区。
6. 在 IPv4 CIDR 块下，选择 IPAM 分配的 IPV4 CIDR 块，然后选择开发子网池和 /28 网络掩码。
7. 选择创建子网。
8. 重复此过程以创建另一个子网。这次选择生产子网池和 /28 网络掩码。
9. 返回 IPAM 控制台并在左侧导航窗格中选择资源。
10. 查找您创建的子网池，然后等待您创建的子网出现在其下面。这需要一定的时间，您可能需要刷新窗口才能看到它出现。

本教程已完成。您可以根据需要创建其他子网池，也可以在 EC2 实例中启动到其中一个子网。

IPAM 会发布与子网中 IP 地址使用情况相关的指标。您可以根据 SubnetipUsage 指标设置 CloudWatch 警报，以便在 IP 利用率阈值被突破时采取行动。例如，如果您为子网分配了 /24 CIDR（256 个 IP 地址），并且您希望在 80% 的 IP 已被利用时收到通知，则可以设置 CloudWatch 警报，以便在达到该阈值时收到提醒。有关为子网 IP 使用情况创建警报的更多信息，请参阅 [创建警报的快速提示](#)。

步骤 5：清除

完成以下步骤以删除您在本教程中创建的资源。

清除资源

1. 使用 IPAM 管理员账户打开 IPAM 控制台，地址：<https://console.aws.amazon.com/ipam/>。
2. 在导航窗格中，选择池。
3. 选择私有作用域。
4. 选择资源规划库，然后选择操作 > 删除。

5. 选择级联删除。资源规划池和子网池将被删除。这样做不会删除子网本身。子网将保留分配给自己的 CIDR，尽管这些 CIDR 将不再来自 IPAM 池。
6. 选择删除。
7. [删除子网](#)。
8. [删除 VPC](#)。

清理已完成。

从 IPAM 池中分配连续弹性 IP 地址

IPAM 允许您向 IPAM 池预调配 Amazon 拥有的公有 IPv4 块，并将这些池中的[连续弹性 IP 地址](#)分配给 AWS 资源。

连续分配的弹性 IP 地址是按顺序分配的公有 IPv4 地址。例如，如果 Amazon 为您提供了一个公有 IPv4 CIDR 块 192.0.2.0/30，而您从该 CIDR 块中分配了四个可用的公有 IPv4 地址，则四个连续弹性 IP 地址的示例是 192.0.2.0、192.0.2.1、192.0.2.2 和 192.0.2.3。

连续分配的弹性 IP 地址使您能够通过以下方式简化安全和联网规则：

- **安全管理：**使用连续的 IPv4 地址可以降低防火墙管理开销。您可以使用单个规则添加整个前缀，并在扩展时关联来自同一前缀的 IP，从而节省时间和精力。
- **企业访问：**您可以使用整个 CIDR 块而不是一长串单独的公有 IPv4 地址，以简化与客户端共享的地址空间。这样就无需在应用程序在 AWS 上扩展时不断沟通 IP 变更。
- **简化的 IP 管理：**使用连续的 IPv4 地址可以简化中央网络团队的公有 IP 管理，因为它减少了跟踪单个公有 IP 的需求，而是使他们能够专注于有限数量的 IP 前缀。

在本教程中，您将完成从 IPAM 池中分配连续弹性 IP 地址所需的步骤。您将使用 Amazon 提供的连续公有 IPv4 CIDR 块创建 IPAM 池，从池中分配弹性 IP 地址，并了解如何监控 IPAM 池的分配。

Note

- 预调配 Amazon 拥有的公有 IPv4 CIDR 块会产生相关费用。有关更多信息，请参阅 [Amazon VPC 定价页面](#)上的 Amazon 提供的连续 IPv4 块选项卡。
- 本教程假设您想要将 [IPAM 用于单个账户](#)以创建 IPAM。如果您想跨账户共享 Amazon 拥有的连续公有 IPv4 区，请先 [将 IPAM 与 AWS Organization 中的账户集成](#)，然后 [使用 AWS](#)

[RAM 共享 IPAM 池](#)。如果您与 AWS Organizations 集成，则可以选择创建[服务控制策略](#)，以防止取消预调配分配给池的连续 IPv4 块。

- 您无法将从 IPAM 池中分配的连续弹性 IP 地址[转移](#)到其他 AWS 账户。相反，通过将 IPAM 与 AWS Organizations 集成，IPAM 允许跨 AWS 账户共享 IPAM 池（如上所述）。
- 您可以预调配的 Amazon 拥有的公有 IPv4 CIDR 块的数量及其大小有限制。有关更多信息，请参阅 [IPAM 的配额](#)。

内容

- [步骤 1：创建 IPAM](#)
- [步骤 2：创建 IPAM 池并预置 CIDR](#)
- [步骤 3：从池中分配弹性 IP 地址](#)
- [步骤 4：将弹性 IP 地址与 EC2 实例相关联](#)
- [步骤 5：跟踪和监控池使用情况](#)
- [清理](#)

步骤 1：创建 IPAM

完成本部分中的步骤创建 IPAM。

AWS Management Console

创建 IPAM

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在 AWS 管理控制台中，选择您要在其中创建 IPAM 的 AWS 区域。在主操作区域创建 IPAM。
3. 在服务主页上，选择创建 IPAM。
4. 选择 Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account（允许 Amazon VPC IP 地址管理器将数据从源账户复制到 IPAM 委托账户中）。如果未选中此选项，则无法创建 IPAM。
5. 选择 IPAM 等级。有关每种套餐中提供的功能以及与套餐相关的费用的更多信息，请参阅 [Amazon VPC 定价页面](#) 中的 IPAM 选项卡。
6. 在运营区域下，选择此 IPAM 可以在其中管理和发现资源的 AWS 区域。默认情况下，您要在其中创建 IPAM 的 AWS 区域被选为运营区域之一。例如，如果您在 AWS 区域 us-east-1

中创建此 IPAM，但是您希望稍后创建区域 IPAM 池，以便在 us-west-2 中向 VPC 提供 CIDR，请在此选择 us-west-2。如果忘记了运营区域，可以稍后返回并编辑 IPAM 设置。

Note

如果您在免费等级中创建 IPAM，则可以为 IPAM 选择多个运营区域，但唯一可在运营区域中使用的 IPAM 功能是[公共 IP 洞察功能](#)。您无法跨 IPAM 运营区域中使用免费等级中的其他功能，例如 BYOIP。你只能在 IPAM 的主区域中只能使用这些功能。要跨运营区域使用所有 IPAM 功能，[请在高级等级中创建 IPAM](#)。

7. 选择创建 IPAM。

Command line

本部分的命令链接到 AWS CLI 参考文档。本文档提供了运行命令时可以使用的选项的详细说明。

使用 `create-ipam` 命令创建 IPAM：

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

示例响应：

```
{
  "Ipam": {
    "OwnerId": "320805250157",
    "IpamId": "ipam-0755477df834ea06b",
    "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
    "IpamRegion": "us-east-1",
    "PublicDefaultScopeId": "ipam-scope-01bc7290e4a9202f9",
    "PrivateDefaultScopeId": "ipam-scope-0a50983b97a7a583a",
    "ScopeCount": 2,
    "OperatingRegions": [
      {
        "RegionName": "us-east-1"
      }
    ],
    "State": "create-in-progress",
    "Tags": [],
    "DefaultResourceDiscoveryId": "ipam-res-disco-02cc5b34cc3f04f09",
    "DefaultResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-06b3a4dccfc81f7c1",
  }
}
```

```
    "ResourceDiscoveryAssociationCount": 1,  
    "Tier": "advanced"  
  }  
}
```

在下一步中，您将需要 `PublicDefaultScopeId`。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。

步骤 2：创建 IPAM 池并预置 CIDR

完成本部分中的步骤创建 IPAM 池，您将从中分配弹性 IP 地址。

AWS Management Console

如需创建池

1. 在 <https://console.aws.amazon.com/ipam/> 中打开 IPAM 控制台。
2. 在导航窗格中，选择池。
3. 选择公有范围。有关范围的更多信息，请参阅 [IPAM 的工作原理](#)。
4. 选择创建池。
5. （可选）添加池的名称标签和池的描述。
6. 在源下，选择 IPAM 范围。
7. 在地址系列下，选择 IPv4。
8. 在资源规划下，保持选中在范围内规划 IP 空间。
9. 在 Locale（区域设置）下，选择池的区域设置。区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。可用的选项来自您在创建 IPAM 时选择的运营区域。
10. 在服务下，选择 EC2 (EIP/VPC)。您选择的服务将决定传播 CIDR 的 AWS 服务。目前，唯一的选择是 EC2 (EIP/VPC)，这意味着从此池中分配的 CIDR 将在 Amazon EC2 服务（适用于弹性 IP 地址）中传播。
11. 在公有 IP 来源下，选择 Amazon 拥有。
12. 在要预调配的 CIDR 下，选择添加 Amazon 拥有的公有 CIDR。选择介于 /29（8 个 IP 地址）和 /30（4 个 IP 地址）之间的网络掩码长度。默认情况下，您最多可以添加 2 个 CIDR。有关提高 Amazon 提供的连续公有 IPv4 CIDR 限制的信息，请参阅 [IPAM 的配额](#)。
13. 将配置此池的分配规则设置保持未选中状态。
14. （可选）为池选择 Tags（标签）。

15. 选择创建池。

在继续之前，请确保已预置此 CIDR。您可以在池详细信息页面的 CIDR 选项卡中查看资源调配状态。

Command line

如需创建池

1. 使用 [create-ipam-pool](#) 命令创建 IPAM 池。区域设置是您希望此 IPAM 池可用于分配的 AWS 区域。可用的选项来自您在创建 IPAM 时选择的运营区域。

```
aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-  
scope-01bc7290e4a9202f9 --address-family ipv4 --locale us-east-1 --aws-service  
ec2 --public-ip-source amazon
```

带有 create-in-progress 状态的示例响应：

```
{  
  
  "IpamPool": {  
  
    "OwnerId": "320805250157",  
  
    "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",  
  
    "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-  
pool-07ccc86aa41bef7ce",  
    "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-  
scope-01bc7290e4a9202f9",  
    "IpamScopeType": "public",  
  
    "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",  
  
    "IpamRegion": "us-east-1",  
  
    "Locale": "us-east-1",  
  
    "PoolDepth": 1,  
  
    "State": "create-in-progress",  
  
  }  
}
```

```
"AutoImport": false,  
  
"AddressFamily": "ipv4",  
  
"Tags": [],  
  
"AwsService": "ec2",  
  
"PublicIpSource": "amazon"  
  
}  
  
}
```

2. 使用 [describe-ipam-pools](#) 命令检查池是否已成功创建。

```
aws ec2 describe-ipam-pools --region us-east-1 --ipam-pool-ids ipam-  
pool-07ccc86aa41bef7ce
```

带有 create-complete 状态的示例响应：

```
{  
  
  "IpamPools": [  
    {  
      "OwnerId": "320805250157",  
      "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",  
      "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-  
pool-07ccc86aa41bef7ce",  
      "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-  
scope-01bc7290e4a9202f9",  
      "IpamScopeType": "public",  
      "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",  
      "IpamRegion": "us-east-1",  
      "Locale": "us-east-1",  
      "PoolDepth": 1,  
      "State": "create-complete",  
      "AutoImport": false,  
      "AddressFamily": "ipv4",  
      "Tags": [],  
      "AwsService": "ec2",  
      "PublicIpSource": "amazon"  
    }  
  ]  
}
```

```
]
}
```

3. 使用 [provision-ipam-pool-cidr](#) 命令向池预置 CIDR。选择介于 /29 (8 个 IP 地址) 和 /30 (4 个 IP 地址) 之间的 `--netmask-length`。默认情况下，您最多可以添加 2 个 CIDR。有关提高 Amazon 提供的连续公有 IPv4 CIDR 限制的信息，请参阅 [IPAM 的配额](#)。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce --netmask-length 29
```

带有 `pending-provision` 状态的示例响应：

```
{
  "IpamPoolCidr": {
    "State": "pending-provision",
    "IpamPoolCidrId": "ipam-pool-cidr-01856e43994df4913b7bc6aac47adf983",
    "NetmaskLength": 29
  }
}
```

4. 在继续之前，请确保已预置此 CIDR。您可以使用 [get-ipam-pool-cidrs](#) 命令查看预置状态。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce
```

带有 `provisioned` 状态的示例响应：

```
{
  "IpamPoolCidrs": [
    {
      "Cidr": "18.97.0.40/29",
      "State": "provisioned",
      "IpamPoolCidrId": "ipam-pool-cidr-01856e43994df4913b7bc6aac47adf983",
      "NetmaskLength": 29
    }
  ]
}
```

步骤 3：从池中分配弹性 IP 地址

完成本部分中的步骤，以从池中分配弹性 IP 地址。

AWS Management Console

按照《Amazon EC2 用户指南》中的[分配弹性 IP 地址](#)中的步骤分配地址，但请注意以下几点：

- 确保您的 EC2 控制台所在的 AWS 区域与您在步骤 2 中创建池时选择的区域设置选项相匹配。
- 选择地址池时，选择使用 IPv4 IPAM 池分配选项，然后选择您在步骤 1 中创建的池。

Command line

使用 [allocate-address](#) 命令从池中分配一个地址。您使用的 `--region` 必须与您在步骤 2 中创建池时选择的 `-locale` 选项相匹配。包括您在 `--ipam-pool-id` 中在步骤 2 中创建的 IPAM 池的 ID。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce
```

示例响应：

```
{
  "PublicIp": "18.97.0.41",
  "AllocationId": "eipalloc-056cdd6019c0f4b46",
  "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
  "NetworkBorderGroup": "us-east-1",
  "Domain": "vpc"
}
```

或者，您也可以使用 `--address` 选项在 IPAM 池中选择特定的 /32。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce --address 18.97.0.41
```

示例响应：

```
{
```

```
"PublicIp": "18.97.0.41",  
"AllocationId": "eipalloc-056cdd6019c0f4b46",  
"PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",  
"NetworkBorderGroup": "us-east-1",  
"Domain": "vpc"  
}
```

有关更多信息，请参阅《Amazon EC2 用户指南》中的[分配弹性 IP 地址](#)。

步骤 4：将弹性 IP 地址与 EC2 实例相关联

完成本部分中的步骤将弹性 IP 地址与 EC2 实例相关联。

AWS Management Console

按照《Amazon EC2 用户指南》中的[关联弹性 IP 地址](#)中的步骤从 IPAM 池中分配弹性 IP 地址，但请注意以下几点：使用 AWS 管理控制台选项时，您关联弹性 IP 地址所在的 AWS 区域必须与您在步骤 2 中创建池时选择的区域设置选项相匹配。

Command line

使用 [associate-address](#) 命令将弹性 IP 地址与实例相关联。您关联弹性 IP 地址所在的 `--region` 区域必须与您在步骤 2 中创建池时选择的 `--locale` 选项匹配。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --  
public-ip 18.97.0.41
```

示例响应：

```
{  
  "AssociationId": "eipassoc-06aa85073d3936e0e"  
}
```

有关更多信息，请参阅《Amazon EC2 用户指南》中的[将弹性 IP 地址与实例或网络接口相关联](#)。

步骤 5：跟踪和监控池使用情况

从 IPAM 池中分配弹性 IP 地址之后，您可以跟踪和监控 IPAM 池的分配：

AWS Management Console

- 在 IPAM 控制台的分配选项卡中查看 IPAM 池详细信息。从 IPAM 池分配的任何弹性 IP 地址的资源类型均为 EIP。
- 使用 [公共 IP 洞察功能](#)：
 - 在公有 IP 类型下，按 Amazon 拥有的 EIP 进行筛选。这显示了分配给 Amazon 拥有的弹性 IP 地址的公有 IPv4 地址的总数。如果您按此衡量标准进行筛选并滚动到页面底部的公有 IP 地址，则将看到您分配的弹性 IP 地址。
 - 在 EIP 使用情况下，按 Amazon 拥有的关联的 EIP 或 Amazon 拥有的未关联的 EIP 进行筛选。这将显示您在 AWS 账户中分配且将其与 EC2 实例、网络接口或 AWS 资源关联或未关联的弹性 IP 地址总数。如果您按此衡量标准进行筛选并滚动到页面底部的公有 IP 地址，您将会看到有关已筛选资源的详细信息。
 - 在 Amazon 拥有的 IPv4 连续 IP 使用情况下，监控一段时间内连续的公有 IPv4 地址使用情况以及 Amazon 拥有的相关的 IPv4 IPAM 池。
- 使用 Amazon CloudWatch 跟踪和监控与 Amazon 提供的已预调配到 IPAM 池的连续公有 IPv4 区块相关的指标。有关特定于连续 IPv4 区块的可用指标，请参阅 [IPAM 指标](#) 下方的公有 IP 指标。除查看指标外，您还可以在 Amazon CloudWatch 中创建警报，以便在达到阈值时通知您。使用 Amazon CloudWatch 创建告警和设置通知不在本教程的范围内。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的 [使用 Amazon CloudWatch 警报](#)。

Command line

- 使用 [get-ipam-pool-allocations](#) 命令查看 IPAM 池分配。从 IPAM 池分配的任何弹性 IP 地址的资源类型均为 eip。

```
aws ec2 get-ipam-pool-allocations --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce
```

示例响应：

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "18.97.0.40/32",
      "IpamPoolAllocationId": "ipam-pool-alloc-0bd07df786e8148aba2763e2b6c1c44bd",
      "ResourceId": "eipalloc-0c9decaa541d89aa9",
```

```
        "ResourceType": "eip",
        "ResourceRegion": "us-east-1",
        "ResourceOwner": "320805250157"
    }
]
}
```

- 使用 Amazon CloudWatch 跟踪和监控与 Amazon 提供的已预调配到 IPAM 池的连续公有 IPv4 区块相关的指标。有关特定于连续 IPv4 区块的可用指标，请参阅 [IPAM 指标](#) 下方的公有 IP 指标。除查看指标外，您还可以在 Amazon CloudWatch 中创建警报，以便在达到阈值时通知您。使用 Amazon CloudWatch 创建告警和设置通知不在本教程的范围内。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的 [使用 Amazon CloudWatch 警报](#)。

本教程现已完成。您已经使用 Amazon 提供的连续公有 IPv4 CIDR 块创建 IPAM 池，从池中分配弹性 IP 地址，并了解了如何监控 IPAM 池的分配。继续下一部分以删除您在本教程中创建的资源。

清理

按照本部分中的步骤清除您在本教程中创建的资源。

步骤 1：解除弹性 IP 地址的关联

完成《Amazon EC2 用户指南》中的 [解除弹性 IP 地址的关联](#) 的步骤，以解除弹性 IP 地址的关联。

步骤 2：释放弹性 IP 地址

完成《Amazon EC2 用户指南》中的 [释放弹性 IP 地址](#) 的步骤，从公有 IPv4 池释放弹性 IP 地址。

步骤 3：从 IPAM 池中取消预调配 CIDR

完成 [从池中取消预置 CIDR](#) 中的步骤，从 IPAM 池中取消预调配 Amazon 拥有的公有 CIDR。此步骤是删除池所必需的。在此步骤完成之前，您需要为 Amazon 提供的连续 IPv4 块付费。

步骤 4：删除 IPAM 池

完成 [删除池](#) 中的步骤以删除 IPAM 池。

步骤 5：删除 IPAM

完成 [删除 IPAM](#) 中的步骤以删除 IPAM。

本教程清理已完成。

IPAM 中的 Identity and Access Management

AWS 使用安全凭证来识别您的身份并向您授予对 AWS 资源的访问权限。利用 AWS Identity and Access Management (IAM) 的功能，可在不共享您的安全凭证的情况下允许其他用户、服务和应用程序完全使用或受限使用您的 AWS 资源。

本部分介绍专门为 IPAM 创建的 AWS 服务相关角色以及附加到 IPAM 服务相关角色的托管策略。有关 AWS IAM 角色和策略的更多信息，请参阅 IAM 用户指南中的[角色术语和概念](#)。

有关 VPC 的 Identity and Access Management 的更多信息，请参阅《Amazon VPC 用户指南》中的[适用于 Amazon VPC 的 Identity and Access Management](#)。

内容

- [IPAM 的服务相关角色](#)
- [IPAM 的 AWS 托管策略](#)
- [策略示例](#)

IPAM 的服务相关角色

IPAM 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色。服务相关角色由 IPAM 预定义，并包含该服务代表您调用其他 AWS 服务所需的一切权限。

服务相关角色可让您更轻松地设置 IPAM，因为您不必手动添加必要的权限。IPAM 定义其服务相关角色的权限，除非另外定义，否则只有 IPAM 可以代入该角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其他 IAM 实体。

服务相关角色权限

IPAM 使用 `AWSServiceRoleForIPAM` 服务相关角色调用附加的 `AWSIPAMServiceRolePolicy` 托管策略中的操作。有关该策略中允许执行的操作的详细信息，请参阅[IPAM 的 AWS 托管策略](#)。

服务相关角色还附加一个允许 `ipam.amazonaws.com` 服务代入服务相关角色的[IAM 信任策略](#)。

创建服务相关角色

IPAM 通过在账户中担任服务相关角色、发现资源及其 CIDR 并将资源与 IPAM 集成来监控一个或多个账户中的 IP 地址使用情况。

可通过以下两种方式之一创建服务相关角色：

- 当与 AWS Organizations 集成时

如果 [将 IPAM 与 AWS Organization 中的账户集成](#) 使用 IPAM 控制台或使用 `enable-ipam-organization-admin-account` AWS CLI CLI 命令，则 `AWSServiceRoleForIPAM` 服务相关角色将在您的每个 AWS Organizations 成员账户中自动创建。因此，IPAM 可以发现所有成员账户中的资源。

Important

要让 IPAM 代表您创建服务相关角色，请执行以下操作：

- 启用 IPAM 与 AWS Organizations 集成的 AWS Organizations 管理账户必须附加允许以下操作的 IAM 策略：
 - `ec2:EnableIpamOrganizationAdminAccount`
 - `organizations:EnableAwsServiceAccess`
 - `organizations:RegisterDelegatedAdministrator`
 - `iam:CreateServiceLinkedRole`
- IPAM 账户必须附加允许 `iam:CreateServiceLinkedRole` 操作的 IAM 策略。

- 当您使用单个 AWS 账户创建 IPAM 时

如果 [将 IPAM 用于单个账户](#)，则当您为 IPAM 创建账户时，将自动创建 `AWSServiceRoleForIPAM` 服务相关角色。

Important

如果您将 IPAM 与单个 AWS 账户一起使用，则在创建 IPAM 之前，必须确保您使用的 AWS 账户附加了允许 `iam:CreateServiceLinkedRole` 操作的 IAM 策略。创建 IPAM 时，将自动创建 `AWSServiceRoleForIPAM` 服务相关角色。有关管理 IAM 策略的更多信息，请参阅《IAM 用户指南》中的 [编辑服务相关角色描述](#)。

编辑服务相关角色

您无法编辑 `AWSServiceRoleForIPAM` 服务相关角色。

删除服务相关角色

如果您不再需要使用 IPAM，我们建议您删除 AWSServiceRoleForIPAM 服务相关角色。

Note

只有删除您的AWS账户中的所有 IPAM 资源之后，您才可以删除服务相关角色。这可确保您不会无意中删除 IPAM 的监控功能。

请按照以下步骤使用 AWS CLI 删除服务相关角色：

1. 使用 [deprovision-ipam-pool-cidr](#) 和 [delete-ipam](#) 删除 IPAM 资源。有关更多信息，请参阅 [从池中取消预置 CIDR](#) 和 [删除 IPAM](#)。
2. 使用 [disable-ipam-organization-admin-account](#) 禁用 IPAM 账户。
3. 使用 `--service-principal ipam.amazonaws.com` 选项通过 [disable-aws-service-access](#) 禁用 IPAM 服务。
4. 删除服务相关角色：[delete-service-linked-role](#)。删除服务相关角色时，IPAM 托管策略也将删除。有关更多信息，请参阅《IAM 用户指南》中的[删除服务相关角色](#)。

IPAM 的 AWS 托管策略

如果将 IPAM 与单个 AWS 账户一起使用，并且创建了 IPAM，则会在 IAM 账户中自动创建 AWSIPAMServiceRolePolicy 托管策略，并将其附加到 AWSServiceRoleForIPAM [服务相关角色](#)。

如果您启用 IPAM 与 AWS Organizations 的集成，将自动在您的 IAM 账户和每个 AWS Organizations 成员账户中创建 AWSIPAMServiceRolePolicy 托管策略，并且该托管策略将附加到 AWSServiceRoleForIPAM 服务相关角色。

此托管策略允许 IPAM 执行以下操作：

- 在您的 AWS 企业的所有成员中监控与联网资源关联的 CIDR。
- 在 Amazon CloudWatch 中存储与 IPAM 相关的指标，例如 IPAM 池中可用的 IP 地址空间以及符合分配规则的资源 CIDR 数量。
- 修改和读取托管前缀列表。

以下示例显示所创建托管策略的详细信息。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAMDiscoveryDescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:ModifyManagedPrefixList",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchMetricsPublishActions",
      "Effect": "Allow",
      "Action": "cloudwatch:PutMetricData",
      "Resource": "*"
    }
  ]
}
```

```

        "Condition": {
            "StringEquals": {
                "cloudwatch:namespace": "AWS/IPAM"
            }
        }
    ]
}

```

前面示例中的第一条语句使 IPAM 能够监控单个 AWS 账户或 AWS Organization 成员使用的 CIDR。

上述示例中的第二条语句使用 `cloudwatch:PutMetricData` 条件键允许 IPAM 将 IPAM 指标存储在您的 AWS/IPAM [Amazon CloudWatch 命名空间中](#)。这些指标被 AWS 管理控制台用于显示有关 IPAM 池和范围中的分配的数据。有关更多信息，请参阅 [使用 IPAM 控制面板监控 CIDR 使用情况](#)。

对 AWS 托管策略的更新

查看有关 IPAM 的 AWS 托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。

更改	描述	日期
AWSIPAMServiceRolePolicy	在 AWSIPAMServiceRolePolicy 托管策略 (<code>ec2:ModifyManagedPrefixList</code> 、 <code>ec2:DescribeManagedPrefixLists</code> 和 <code>ec2:GetManagedPrefixListEntries</code>) 中添加了操作，以使 IPAM 能够修改和读取托管前缀列表。	2025 年 10 月 31 日
AWSIPAMServiceRolePolicy	向 AWSIPAMServiceRolePolicy 托管策略 (<code>organizations:ListChildren</code> 、 <code>organizations:ListParents</code> 和 <code>organizations:DescribeOrganizationalUnit</code>) 添加了操作，	2024 年 11 月 21 日

更改	描述	日期
	使 IPAM 能够获取 AWS Organizations 中组织单元 (OU) 的详细信息，以便客户可以在 OU 级别使用 IPAM。	
AWSIPAMServiceRolePolicy	在 AWSIPAMServiceRole Policy 托管策略 (ec2:GetIpamDiscoveredPublicAddresses) 中添加了操作，以使 IPAM 能够在资源发现期间获取公有 IP 地址。	2023 年 11 月 13 日
AWSIPAMServiceRolePolicy	在 AWSIPAMServiceRole Policy 托管策略 (ec2:DescribeAccountAttributes 、 ec2:DescribeNetworkInterfaces 、 ec2:DescribeSecurityGroups 、 ec2:DescribeSecurityGroupRules 、 ec2:DescribeVpnConnections 、 globalaccelerator:ListAccelerators 和 globalaccelerator:ListByoipCidrs) 中添加了操作，使 IPAM 能够在资源发现期间获取公有 IP 地址。	2023 年 11 月 1 日

更改	描述	日期
AWSIPAMServiceRolePolicy	向 AWSIPAMServiceRole Policy 托管式策略添加了两个操作 (ec2:GetIpamDiscoveredAccounts 和 ec2:GetIpamDiscoveredResourceCidrs) , 以便 IPAM 在资源发现期间获取 AWS 账户和监控资源 CIDR。	2023 年 1 月 25 日
IPAM 已开启跟踪更改	IPAM 为其 AWS 托管策略开启了跟踪更改。	2021 年 12 月 2 日

策略示例

这一部分中的示例策略包含完全使用 IPAM 时的所有相关 AWS Identity and Access Management (IAM) 操作。根据您使用 IPAM 的方式，您可能不需要包含所有 IAM 操作。要获得使用 IPAM 控制台的完整体验，您可能需要包含 AWS Organizations、AWS Resource Access Manager (AWS RAM) 和 Amazon CloudWatch 等服务的额外 IAM 操作。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIpamByoasn",
        "ec2:DeprovisionIpamByoasn",
        "ec2:DescribeIpamByoasn",
        "ec2:DisassociateIpamByoasn",
        "ec2:ProvisionIpamByoasn",
        "ec2:CreateIpam",
        "ec2:DescribeIpams",
        "ec2:ModifyIpam",

```

```

        "ec2:DeleteIpam",
        "ec2:CreateIpamScope",
        "ec2:DescribeIpamScopes",
        "ec2:ModifyIpamScope",
        "ec2:DeleteIpamScope",
        "ec2:CreateIpamPool",
        "ec2:DescribeIpamPools",
        "ec2:ModifyIpamPool",
        "ec2:DeleteIpamPool",
        "ec2:ProvisionIpamPoolCidr",
        "ec2:GetIpamPoolCidrs",
        "ec2:DeprovisionIpamPoolCidr",
        "ec2:AllocateIpamPoolCidr",
        "ec2:GetIpamPoolAllocations",
        "ec2:ReleaseIpamPoolAllocation",
        "ec2:CreateIpamResourceDiscovery",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:ModifyIpamResourceDiscovery",
        "ec2:DeleteIpamResourceDiscovery",
        "ec2:AssociateIpamResourceDiscovery",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DisassociateIpamResourceDiscovery",
        "ec2:GetIpamResourceCidrs",
        "ec2:ModifyIpamResourceCidr",
        "ec2:GetIpamAddressHistory",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "ipam.amazonaws.com"
        }
    }
}
]

```

```
}
```

IPAM 的配额

本部分列出了与 IPAM 相关的配额。“Service Quotas”控制台还提供有关 IPAM 配额的信息。您可以使用“Service Quotas”控制台查看默认配额，并对可调整的配额[请求增加配额](#)。有关更多信息，请参阅《服务配额用户指南》中的[Requesting a quota increase](#)。

名称	默认值	可调整
Amazon 提供的连续公有 IPv4 CIDR 块	2	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
Amazon 提供的连续公有 IPv4 CIDR 块网络掩码长度	/29	可接受的大小介于 /29 和 /30 之间。要请求提高，请按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
Amazon 提供的 IPv6 CIDR 块网络掩码长度	/52	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每个区域池的 Amazon 提供的 IPv6 CIDR 块	1	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
您可以自带到 IPAM 的自治系统号 (ASN)	5	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每个池的 CIDR	50	是

名称	默认值	可调整
每个 IPAM 策略启用的目标数	100	可以。要申请调整配额，请按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每个企业的 IPAM 管理员数	1	否
每个区域的 IPAM	1	否
每个 IPAM 的 IPAM 策略数	10	可以。要申请调整配额，请按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每个资源区域对的 IPAM 策略分配规则数*	10	可以。要申请调整配额，请按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每次资源发现的组织单元排除项数	10	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
池深度 (池内的池数量)	10	是
每个范围的池	50	是
每个 IPAM 的前缀列表解析器数	10	是
每个前缀列表解析器的前缀列表解析器目标数	50	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。

名称	默认值	可调整
每个前缀列表解析器的规则数	100	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每个前缀列表解析器版本的 CIDR 条目数	1000	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每个 IPAM 的资源发现关联	5	是
每个区域的资源发现	1	否
资源利用率指标	50	可以。按照《AWS 一般参考》中 AWS service quotas 所述联系 AWS 支持中心。
每个 IPAM 的范围	5	可以 。创建 IPAM 时，系统将为您创建私有和公有默认范围。如果要创建额外的范围，这些范围将属于私有范围。您不能创建额外的公有范围。

* 资源区域设置对：设置分配规则时，必须同时指定资源类型（EIP、ALB 或 RDS 集群等 AWS 资源）和区域设置（规则适用的 AWS 区域或本地区域）。分配规则的作用域仅限于该资源类型和区域设置组合。例如，假设您为 us-east-1 中的 EIP 设置了一个策略，则最多可以为该特定的资源区域设置对指定 10 条规则*。

IPAM 定价

Amazon VPC IP 地址管理器 (IPAM) 是一项服务，可帮助您跨 AWS 资源和本地网络管理您的 IP 地址空间。IPAM 提供了一种集中方式来规划、监控和控制您的 AWS 和本地资源使用的 IP 地址。

本部分介绍如何查看与定价相关的信息以及您当前的 IPAM 成本。

内容

- [查看定价信息](#)
- [使用 AWS Cost Explorer 查看您当前的费用和使用情况](#)

查看定价信息

IPAM 提供两种套餐：免费套餐和高级套餐。有关每种套餐中提供的功能以及与套餐相关的费用的更多信息，请参阅 [Amazon VPC 定价页面](#) 中的 IPAM 选项卡。

使用 AWS Cost Explorer 查看您当前的费用和使用情况

使用 IPAM 高级套餐时，您需要为 IPAM 管理的每个活动 IP 地址按小时计费。如果您想查看和分析 IPAM 成本和使用情况，可以使用 AWS Cost Explorer。

1. 打开 AWS Cost Management 控制台，网址为 <https://console.aws.amazon.com/cost-management/home>。
2. 选择 Cost Explorer。
3. 选择使用类型并输入 **IPAddressManager**，筛选 IPAM 使用情况。
4. 选中一个或多个复选框。它们各自代表一个不同的 AWS 区域。
5. 单击应用。

例如，如果选择 USE1-IPAddressManager-IP-Hours(Hrs)，而 us-east-1 是您的 IPAM 主区域，则将看到 IPAM 在所有区域中计费的活动 IP 小时数和成本。例如，如果使用时间为 18 小时，这意味着您可以有一个活跃 IP 地址 18 小时，3 个不同区域 3 个 IP 地址，每个活跃 IP 地址 6 小时，或者这些地址加起来长达 18 小时的任意组合。

有关 AWS Cost Explorer 的更多信息，请参阅《AWS Cost Management 用户指南》中的 [使用 AWS Cost Explorer 分析费用](#)。

相关信息

虽然 AWS 技术文档网站是一个综合资源，但还有许多其他地方可以找到有关 AWS 服务的信息。AWS 博客、白皮书、案例研究和社群论坛可以提供宝贵的见解、真实示例以及官方技术细节之外的替代视角。探索这些不同的来源可以让您对 AWS 产品有更全面的了解。

下列相关资源在您使用 Amazon VPC IP 地址管理器的过程中会有所帮助：

- [Amazon VPC IP Address Manager Best Practices](#) (Amazon VPC IP 地址管理器最佳实践) ：一篇关于如何使用 Amazon VPC IP 地址管理器规划和创建可扩展地址方案的最佳实践的 AWS 博客文章。
- [Network Address Management and Auditing at Scale with Amazon VPC IP Address Manager](#) (使用 Amazon VPC IP 地址管理器大规模进行网络地址管理和审计) ：一篇介绍 Amazon VPC IP 地址管理器并向演示如何在 AWS 控制台使用该服务的 AWS 博客文章。
- [Configure fine-grained access to your resources shared using AWS Resource Access Manager](#) ：这篇 AWS 博客介绍了如何与 AWS Organizations 组织单位中的账户共享 IPAM 池。
- [使用 CIDR 映射可视化企业 IP 地址管理和规划](#) ：AWS 博客介绍了如何使用 IPAM 控制台中的 IPAM CIDR 映射可视化整个 IPv4 和 IPv6 场景。

IPAM 的文档历史记录

下表介绍了 IPAM 的版本。

功能	描述	发行日期
使用 IPAM 将您自己的 IP 引入 CloudFront	使用 IPAM 管理 AWS 全局服务的 BYOIP CIDR，首先是 CloudFront 任播服务。	2025 年 11 月 21 日
使用 IPAM 策略定义公有 IPv4 分配策略	您现在可以使用 IPAM 策略来定义将 AWS 服务映射到特定 IPAM 池的规则，从而帮助定义公有 IPv4 分配策略。	2025 年 11 月 19 日
将 IPAM 与 Infoblox 基础设施集成	您现在可以将 IPAM 与 Infoblox 基础设施集成，从而通过现有的 Infoblox 工作流管理 AWS IP 地址，同时获得云原生 AWS 功能。此集成适用于私有作用域，并且需要具有 IPAM 高级套餐。	2025 年 11 月 7 日
自动更新前缀列表	您现在可以使用 IPAM 前缀列表解析器根据 IPAM 池 CIDR 自动更新前缀列表。	2025 年 10 月 31 日
通过 IPAM 控制台管理警报	您现在可以直接从 IPAM 控制台中创建和管理 Amazon CloudWatch 警报。当处于 INSUFFICIENT_DATA 或 ALARM 状态时，与 IPAM 相关的警报将作为警告栏和视觉指示器出现。	2025 年 8 月 21 日
启用成本分配	启用成本分配后，可以将 活动 IP 地址的费用 分配给使用 IP 地址的账户，而不是分配给 IPAM 所有者。这对于大型组织非常有用，在这些组织中，委派的 IPAM 管理员使用 IPAM 集中管理 IP 地址，并且每个账户负责自己的使用，从而无需手动计算账单。	2025 年 5 月 1 日
从 IPAM 中排除组织单元	如果您的 IPAM 已与 AWS Organizations 集成，则现在可以从 IPAM 中排除组织单元。IPAM 不会管理组织单元排除项中账户的 IP 地址。	2024 年 11 月 21 日

功能	描述	发行日期
AWS 托管式策略更新 – 对现有策略的更新	现有 AWSIPAMServiceRolePolicy 已更新。	2024 年 11 月 21 日
从 IPAM 池中分配连续弹性 IP 地址	IPAM 现在允许您向 IPAM 池预调配 Amazon 拥有的公有 IPv4 块，并将这些池中的连续弹性 IP 地址分配给 AWS 资源。连续弹性 IP 地址使您能够简化您的联网和安全许可列表需求。	2024 年 8 月 28 日
私有 IPv6 GUA 及 ULA	现在可向私有范围内的 IPAM 池预置私有 IPv6 GUA 及 ULA 范围。私有 IPv6 地址仅在 IPAM 中可用。有关私有 IPv6 寻址的更多信息，请参阅《Amazon VPC 用户指南》中的 私有 IPv6 地址 。	2024 年 8 月 8 日
IPAM 免费等级和高级等级	现在，您可以在 IPAM 的免费等级和高级等级之间进行选择。	2023 年 11 月 17 日
公共 IP 洞察功能	以前，您只能查看单个区域的公共 IP 洞察功能。现在，您可以跨区域查看公共 IP 洞察功能。此外，您现在可以在 Amazon CloudWatch 中查看公有 IP 地址洞察 。	2023 年 11 月 17 日
为子网 IP 分配规划 VPC IP 地址空间	现在，您可以使用 IPAM 规划 VPC 内的子网 IP 空间，并在子网和 VPC 级别监控与 IP 地址相关的指标。	2023 年 11 月 17 日
自带 ASN (BYOASN)	现在，您可以自带自治系统编号 (ASN) 至 AWS。	2023 年 11 月 17 日
AWS 托管式策略更新 – 对现有策略的更新	现有 AWSIPAMServiceRolePolicy 已更新。	2023 年 11 月 17 日
AWS 托管式策略更新 – 对现有策略的更新	现有 AWSIPAMServiceRolePolicy 已更新。	2023 年 11 月 1 日

功能	描述	发行日期
资源利用率指标	现在，IPAM 会将 IPAM 监控的资源的 IP 利用率指标发布到 Amazon CloudWatch。	2023 年 8 月 2 日
公共 IP 洞察功能	公共 IP 洞察功能会向您显示您的账户中此区域的服务使用的所有公有 IPv4 地址。您可以使用这些洞察来确定公有 IPv4 地址的使用情况，并查看释放未使用的弹性 IP 地址的建议。	2023 年 7 月 28 日
AWS 托管式策略更新 – 对现有策略的更新	现有 AWSIPAMServiceRolePolicy 已更新。	2023 年 1 月 25 日
将 IPAM 与组织外部的账户集成	现在，您不仅可以通过单个 IPAM 账户管理组织外部的 IP 地址，还可以与其他 AWS Organizations 账户共享 IPAM 池。	2023 年 1 月 25 日
Amazon 为 IPAM 池提供的 IPv6 连续 CIDR 块	现在，在公有作用域中创建 IPAM 池时，您可以向该池预置 Amazon 提供的 IPv6 连续 CIDR 块。有关更多信息，请参阅 在 IPAM 中创建 IPv6 地址池 。	2023 年 1 月 25 日
初始版本	此版本介绍了 Amazon VPC IP 地址管理器。	2021 年 12 月 2 日