Amazon Virtual Private Cloud

IP 地址管理器

亚马逊云科技

Amazon Virtual Private Cloud: IP 地址管理器

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 Amazon Web Services 服务入门。

Table of Contents

什么是 IPAM？

Amazon VPC IP 地址管理器 (IPAM) 是一项 VPC 功能，可让您更轻松地计划、跟踪和监控 Amazon 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

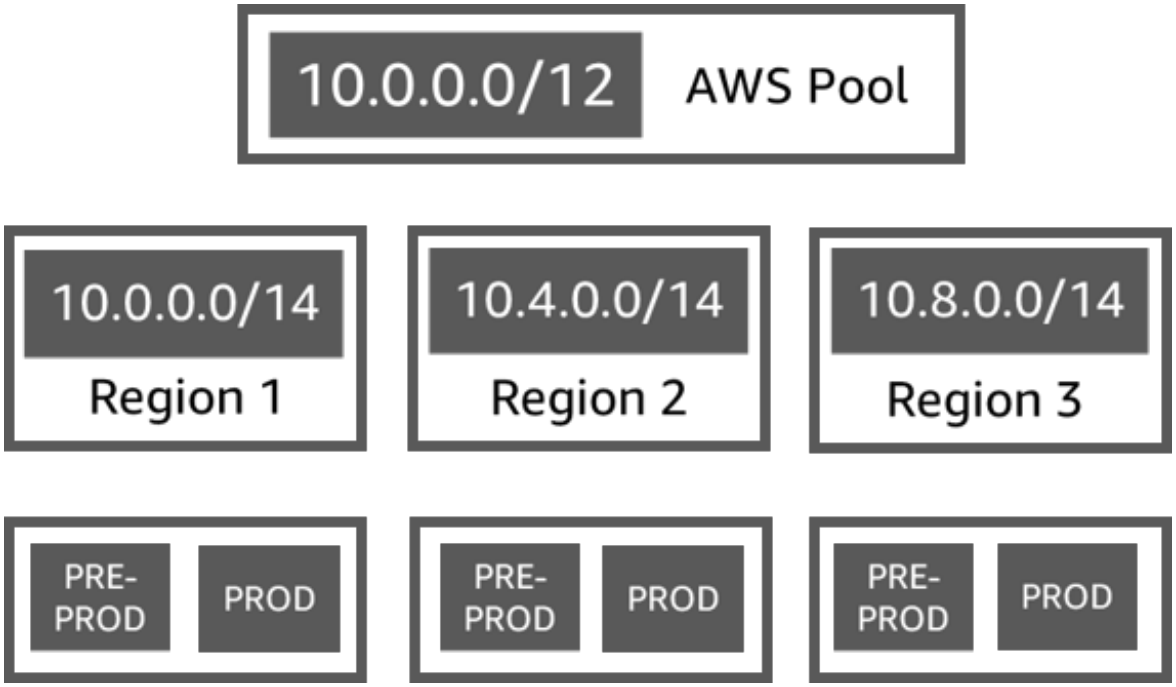
本指南由以下部分组成：

- IPAM 的工作原理 (p. 2)：IPAM 概念和术语。
- IPAM 入门 (p. 3)：通过 Amazon 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 (p. 15)：管理 IPAM、范围、池和分配的步骤。
- 跟踪 IPAM 中的 IP 地址使用情况 (p. 26)：使用 IPAM 监控和跟踪 IP 地址使用情况的步骤。
- 教程 (p. 32)：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 Amazon 区域的 IPAM 池层次结构。每个 Amazon 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 Amazon 区域。创建 IPAM 时，Amazon 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。IPAM 包含两个默认范围。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。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 Amazon 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 可以管理和监控您拥有的私有 IPv4 CIDR 和公有 IPv4/IPv6 CIDR。IPAM 只能监控（不能管理）Amazon 拥有的公有 IP 空间。

要开始使用并创建 IPAM，请参阅 IPAM 入门 (p. 3)。

IPAM 入门

按照本部分中的步骤来开始使用 IPAM。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。

目录

访问 IPAM

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

- Amazon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/。
- Amazon 命令行界面 (Amazon CLI)：为众多 Amazon 服务（包括 Amazon VPC）提供命令。Amazon CLI 在 Windows、macOS 和 Linux 上受支持。要获取 Amazon CLI，请参阅 Amazon Command Line Interface。
- Amazon 开发工具包：提供特定于语言的 API。Amazon 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 Amazon 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 Amazon 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 Amazon CLI 文档的链接，其中显示了如何使用 Amazon CLI 执行同样的操作。

如果您是第一次使用 IPAM 的用户，请查看 IPAM 的工作原理 (p. 2) 了解 IPAM 在 Amazon VPC 中的角色，然后继续执行 为 IPAM 配置权限 (p. 3) 中的说明。

为 IPAM 配置权限

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 能够与 Amazon Organizations 集成，从而使 Amazon VPC IPAM 服务能够管理和监控所有 Amazon Organizations 成员账户创建的联网资源，请参阅 将 IPAM 与 Amazon Organizations 集成 (p. 4)。
- 要将单个 Amazon 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 (p. 5)。

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。

目录

将 IPAM 与 Amazon Organizations 集成

或者，您可以按照本部分中的步骤将 IPAM 与 Amazon 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 Amazon 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 Amazon Organizations 成员账户，用于从使用 Amazon 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 Amazon Organizations 用户指南中的什么是 Amazon 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 Amazon Organizations 成员账户之间使用的 CIDR 自动导入 IPAM 中。

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

Important

- 必须通过在 Amazon 管理控制台中使用 IPAM 或 enable-ipam-organization-admin-account Amazon CLI 命令来启用与 Amazon Organizations 的集成。这将确保创建与 `AWSServiceRoleForIPAM` 服务相关角色。如果通过使用 Amazon Organizations 控制台或 register-delegated-administrator Amazon CLI 命令启用对 Amazon 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。

Note

将与 Amazon Organizations 集成时：

- 您不能使用 IPAM 跨多个 Amazon Organizations 管理 IP 地址。
- 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 Amazon 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 Amazon 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 Amazon Organizations。
- IPAM 账户必须是 Amazon Organizations 成员账户。您不能将 Amazon Organizations 管理账户作为 IPAM 账户。
- IPAM 账户必须附加允许 `iam:CreateServiceLinkedRole` 操作的 IAM 策略。创建 IPAM 时，将自动创建 AWSServiceRoleForIPAM 服务相关角色。
- 与 Amazon Organizations 管理账户关联的 IAM 用户账户必须附加以下 IAM 策略操作：
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`

- `organizations:RegisterDelegatedAdministrator`
- `iam:CreateServiceLinkedRole`

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。

Amazon Management Console

要选择 IPAM 账户

1. 在 https://console.aws.amazon.com/ipam/ 中打开 IPAM 控制台。
2. 在 Amazon 管理控制台中，选择您要在其中与 IPAM 合作的 Amazon 区域。
3. 在导航窗格中，选择 Settings (设置)。
4. 对于 IPAM 账户，输入 Amazon 账户 ID。IPAM 管理员必须是 Amazon Organizations 成员账户。
5. 选择 Delegate (委派)。

Command line

本部分的命令链接到 Amazon 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。

- 要使用 Amazon 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 Amazon 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 用于单个账户

如果选择不将 IPAM 与 Amazon Organizations 集成 (p. 4)，则可以将 IPAM 与单个 Amazon 账户一起使用。

当您在下一部分创建 IPAM 时，将自动在 Amazon Identity and Access Management 中为 Amazon VPC IPAM 服务创建服务相关角色。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 (p. 92)。

Important

如果您将 IPAM 与单个 Amazon 账户一起使用，则必须确保用于创建 IPAM 的 Amazon 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 IAM 策略。

一旦单个 Amazon 账户有权创建 IPAM 服务相关角色，请转到 创建 IPAM (p. 5)。

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 Amazon 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 Amazon 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 Amazon 区域。这些 Amazon 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 Amazon 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 Amazon 区域将如何影响将可用于以后创建的池的区域。

- 在 Amazon 区域 1 和 Amazon 区域 2 中运营的 IPAM
  - 私有范围
    - 顶级 IPAM 池
      - Amazon 区域 2 中的区域 IPAM 池
        - 开发池
          - Amazon 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 (p. 95)。

Amazon Management Console

创建 IPAM

1. 在 https://console.aws.amazon.com/ipam/ 中打开 IPAM 控制台。
2. 在 Amazon 管理控制台中，选择您要在其中创建 IPAM 的 Amazon 区域。
3. 在服务主页上，选择 Create IPAM（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 Operating regions（运营区域）下，选择此 IPAM 可以在其中管理和发现资源的 Amazon 区域。默认情况下，您要在其中创建 IPAM 的Amazon区域被选为运营区域之一。例如，如果您在 Amazon 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。
6. 选择创建。

Command line

本部分的命令链接到 Amazon 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。

请使用以下 Amazon 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 Scopes（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 (p. 2)。

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。

> Important
>
> 要跨 Amazon 账户使用 IPAM 池，您必须将 IPAM 与 Amazon 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 Amazon Organizations 集成 (p. 4)。

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 Amazon 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 (p. 95)。

> 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 Amazon 区域 1 和 Amazon 区域 2 中运营
  - 私有范围
    - 顶级池
      - Amazon 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。如果您正在创建单个 IPAM 池，请完成 创建顶级池 (p. 8) 中的步骤，然后跳至 分配 CIDR (p. 13)。

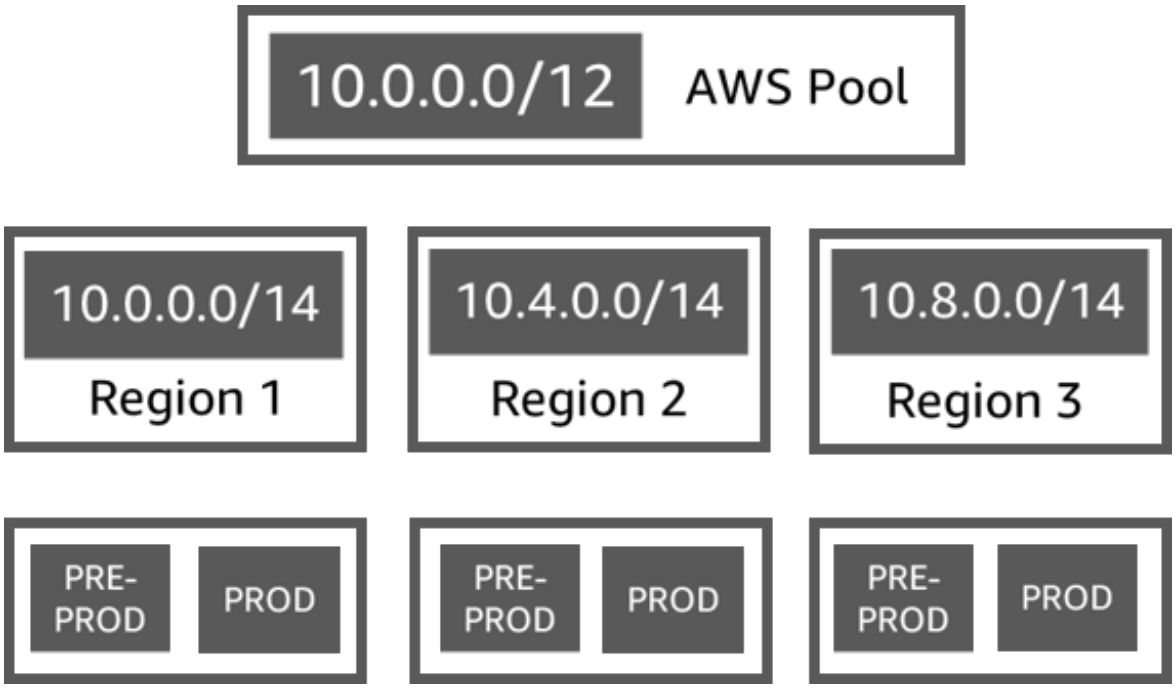
目录

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。

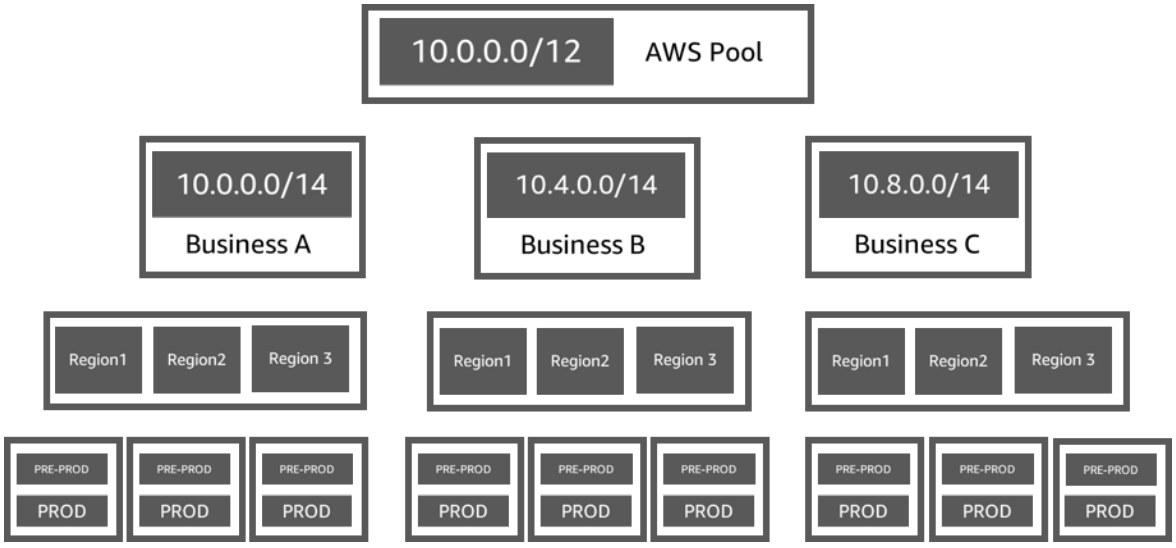
多个 Amazon 区域中的池

以下示例显示了顶级池内多个Amazon区域的 IPAM 池层次结构。每个 Amazon 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。



适用于多个业务线的池

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 Amazon 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。



创建顶级池

按照本部分中的步骤创建顶级 IPAM 池。创建池时，您需要为池预置 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。

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 Amazon 区域 1 和 Amazon 区域 2 中运营
  - 私有范围
    - 顶级池 (10.0.0.0/8)
      - Amazon 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。

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 Amazon 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 (p. 27)。

> **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 Amazon Resource Access Manager (RAM) 中的共享资源），必须将资源所有者配置为 Amazon RAM 中的主体。有关使用 RAM 共享池的更多信息，请参阅 使用 Amazon RAM 共享 IPAM 池 (p. 16)。

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，如果空间可用，仍然可以使用该池中大于 /24 的 CIDR 创建资源，但是由于这样做违反了池中的分配规则，IPAM 会将此资源标记为不合规。

Amazon Management Console

要创建池

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。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 (p. 2)。
4. 选择 Create pool。
5. （可选）添加池的 Name tag（名称标签）和池的描述。
6. 选择 No source pool（没有源池）。
7. 对于 Locale（区域设置），选择 None（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 Amazon 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。

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。

8. 为此池选择 Address family（地址系列）。如果此池中的 IP 地址将是 IPv4 地址，请选择 IPv4。如果它们将是 IPv6 地址，请选择 IPv6。如果您为此池选择的范围是公有范围，则可以选择使用 IPv4 或 IPv6。如果您为此池选择的范围是私有的，则 IPv4 是唯一的选择。
9. （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。
10. 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。
    - 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**，则此池中的任何新分配都将默认为网络掩码长度 **/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。
11. （可选）为池选择 Tags（标签）。
12. 选择 Create pool。

Command line

本部分的命令链接到 Amazon 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。

请使用以下 Amazon 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 分配 CIDR (p. 13)。

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 Amazon 区域 1 和 Amazon 区域 2 中运营
  - 私有范围
    - 顶级池 (10.0.0.0/8)
      - Amazon 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。

Amazon 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 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 (p. 2)。
4. 选择 Create pool。
5. （可选）添加池的 Name tag（名称标签）和池的描述。
6. 在 Source pool（源池）下，选择您在上一部分中创建的顶级池。
7. 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 Amazon 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。
8. （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。
9. 这里的分配规则选项与创建顶级池时的选项相同。请参阅 创建顶级池 (p. 8) 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。
10. （可选）为池选择 Tags（标签）。
11. 配置完池后，选择 Create pool（创建池）。

Command line

本部分的命令链接到 Amazon 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。

请使用以下 Amazon 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 分配 CIDR (p. 13)。

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 Amazon 区域 1 和 Amazon 区域 2 中运营
  - 私有范围
    - 顶级池 (10.0.0.0/8)
      - Amazon 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)
        - 生产 VPC 的开发池 (10.0.1.0/24)
      - Amazon 区域 2 中的区域池 (10.1.0.0/16)

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。

Amazon 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 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 (p. 2)。
4. 选择 Create pool。
5. （可选）添加池的 Name tag（名称标签）和池的描述。
6. 在 Source pool（源池）下，选择区域池。
7. 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。此处的可用选项来自您在创建 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 Amazon 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。
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级和区域池时的选项相同。请参阅 创建顶级池 (p. 8) 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 Tags（标签）。
11. 配置完池后，选择 Create pool（创建池）。

Command line

本部分的命令链接到 Amazon 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。

请使用以下 Amazon 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。

分配 CIDR

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。

以下示例显示了池结构的层次结构，您可以使用本部分中的说明创建这些结构：

- IPAM 在 Amazon 区域 1 和 Amazon 区域 2 中运营
  - 私有范围
    - 顶级 IPAM 池 (10.0.0.0/8)
      - Amazon 区域 2 中的区域 IPAM 池 (10.0.0.0/16)
        - 开发池 (10.0.0.0/24)
          - 分配 - VPC (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。

您可以通过以下方式从 IPAM 池分配 CIDR：

- 使用与 IPAM 集成的 Amazon 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 Amazon 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 Amazon 服务以预置 IPAM 池 CIDR，以及如何手动预留 IP 地址空间。

目录

创建使用 IPAM 池 CIDR 的 VPC

按 Amazon VPC 用户指南的创建 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，Amazon 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 Amazon CLI 的完整说明（包括创建 VPC），请参阅 教程 (p. 32) 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。

Important

不能从公有范围内的池中手动分配 CIDR。

Amazon 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 (p. 2)。
4. 在内容窗格中，选择池。
5. 选择 Actions（操作）> Allocate CIDR（分配 CIDR）。
6. 选择是否定义要分配的确切 CIDR（例如 **`10.0.0.0/24`**），或者只选择网络掩码长度（或者，例如 **`/24`**）。
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

本部分的命令链接到 Amazon 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。

使用以下 Amazon 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 (p. 23)。

管理 IPAM 中的 IP 地址空间

此部分中的任务是可选的。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 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。

目录

强制使用 IPAM 进行 VPC 创建

Note

此部分仅在您启用了 IPAM 与 Amazon Organizations 集成时适用您。有关更多信息，请参阅 将 IPAM 与 Amazon Organizations 集成 (p. 4)。

此部分描述如何在 Amazon 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 Amazon 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. 按照创建《Amazon Organizations 用户指南》中的创建 SCP 中的步骤操作，并在 JSON 编辑器中输入以下文本：

```
{
 "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 Amazon Organizations 用户指南中的附加和分离服务控制策略。

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. 按照创建《Amazon Organizations 用户指南》中的创建 SCP 中的步骤操作，并在 JSON 编辑器中输入以下文本：

```
{
 "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 Amazon Organizations 用户指南中的附加和分离服务控制策略。

使用 Amazon RAM 共享 IPAM 池

按照此部分中的步骤适用 Amazon 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 Amazon 资源，例如 VPC。主体是 RAM 中的一个概念，表示 Amazon Organizations 中的任何Amazon账户、IAM 角色、IAM 用户或企业单位。有关更多信息，请参阅 Amazon RAM 用户指南中的使用共享的共享您的 Amazon 资源。

Note

- 如果您已将 IPAM 与 Amazon Organizations 集成，您只能与 Amazon RAM 共享 IPAM 池。有关更多信息，请参阅 将 IPAM 与 Amazon Organizations 集成 (p. 4)。如果您是单个账户 IPAM 用户，则无法与 Amazon RAM 共享 IPAM 池。
- 您必须启用在 Amazon RAM 中与 Amazon Organizations 共享资源。有关更多信息，请参阅 Amazon RAM 用户指南中的在 Amazon Organizations 内启用资源共享。
- RAM 共享仅在您 IPAM 所在的主 Amazon 区域中可用。您必须在 IPAM 所在的 Amazon 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其 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。

Amazon 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 (p. 2)。
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，Amazon RAM 控制台将打开。您将在 Amazon 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：将现有的 BYOIP IPv4 CIDR 传输到 IPAM (p. 86)。
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

本部分的命令链接到 Amazon CLI 参考文档。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 Amazon 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 (p. 27)。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。

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 (p. 26)。

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。

Amazon 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 (p. 2)
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. 输入要添加的 CIDR，然后选择 Add new CIDR（添加新 CIDR）获取额外的 CIDR。

   Note

   当您将 CIDR 预置到池时：

   - 您要预置的 CIDR 必须在范围内可用。
   - 如果要将 CIDR 预置到池中的池，则您要预置的 CIDR 空间必须在池中可用。
7. 选择 Request provisioning（请求预置）。
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

本部分的命令链接到 Amazon 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。

使用以下 Amazon 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

从池中取消预置 CIDR

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。

Important

如果池中有分配，则无法取消预置 CIDR。要删除分配，请参阅 释放分配 (p. 23)。

Amazon 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 (p. 2)。
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

本部分的命令链接到 Amazon 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。

使用以下 Amazon 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 (p. 18)。如果要删除池，请参阅 删除池 (p. 19)。

编辑池

按照本部分中的步骤编辑 IPAM 池。您可能需要编辑池以更改池中的分配规则。有关分配规则的更多信息，请参阅 创建顶级池 (p. 8)。

Amazon 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 (p. 2)
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 创建顶级池 (p. 8)。
7. 选择 Update (更新)。

Command line

使用以下 Amazon CLI 命令编辑池：

1. 获取 IPAM 池 ID：describe-ipam-pools
2. 修改池：modify-ipam-pool

删除池

按照本部分中的步骤删除 IPAM 池。

Important

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 (p. 18)，然后才能删除池。

Amazon 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 (p. 2)。
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

本部分的命令链接到 Amazon 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。

使用以下 Amazon 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 创建顶级池 (p. 8)。

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 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 在范围之间移动资源 CIDR (p. 21)。

Amazon 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

本部分的命令链接到 Amazon 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。

请使用以下 Amazon 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

在范围之间移动资源 CIDR

按照本部分中的步骤将一个范围中的 CIDR 分配给另一个范围。

Important

- 您只能将资源 CIDR 从一个私有范围移动到另一个私有范围。您不能将资源 CIDR 从公有范围移动到私有范围或从私有范围移动到公有范围。
- 您只能为 IPAM 可以管理的资源移动 CIDR。
- 相同的 Amazon 账户必须同时拥有这两个范围。
- 如果资源 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资源 CIDR 分配之后，系统才会移动资源 CIDR。有关释放分配的信息，请参阅释放分配。

Amazon Management Console

要移动分配给资源的单个 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。
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，选择资源并查看资源的详细信息。
5. 在 Associated CIDRs（关联的 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 移动到不同的范围）。
6. 选择要将资源 CIDR 移动到的范围。
7. 选择 Change scope（更改范围）。

要移动分配给资源的所有 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。
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，选择要移动其 CIDR 的资源。
5. 选择 Actions（操作）> Move all associated CIDRs to different scope（将所有关联的 CIDR 移动到不同范围）。
6. 选择要将资源 CIDR 移动到的范围。
7. 选择 Move scope（移动范围）。

Command line

使用以下 Amazon CLI 命令修改池：

1. 获取 IPAM 池 ID：describe-ipam-pools
2. 获取当前范围内的资源 CIDR：get-ipam-pool-cidrs
3. 移动资源 CIDR：modify-ipam-resource-cidr
4. 获取其他范围内的资源 CIDR：get-ipam-pool-cidrs

更改资源 CIDR 的监控状态

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

Note

不能忽略公有范围内的资源。

您可以将资源 CIDR 的监控状态更改为已监控或已忽略：

- 已监控：IPAM 已检测到资源 CIDR，目前正在监控该资源是否与其他 CIDR 和分配规则合规性重叠。
- 已忽略：已选择该资源免于监控。不会评估忽略的资源是否与其他 CIDR 或分配规则合规性重叠。选择忽略资源后，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资源（如果在池中设置了自动导入分配规则）。

Amazon Management Console

要更改分配给资源的单个 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。
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，选择资源并查看资源的详细信息。
5. 在 Associated CIDRs（关联的 CIDR）下，选择分配给资源的 CIDR 之一，然后选择 Actions（操作）> Mark as ignored（标记为已忽略）或 Unmark as ignored（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）。

要更改分配给资源的所有 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。
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，选择要更改其监控状态的资源。
5. 选择 Actions（操作）> Mark all associated CIDRs as ignored（将所有关联的 CIDR 标记为已忽略）或 Unmark all associated CIDRs as ignored（将所有关联的 CIDR 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 Amazon CLI 命令更改资源 CIDR 监控状态的：

1. 获取范围 ID：describe-ipam-scopes
2. 查看资源的当前监控状态：get-ipam-resource-cidrs
3. 更改资源 CIDR 的状态：modify-ipam-resource-cidr
4. 查看资源的新监控状态：get-ipam-resource-cidrs

删除范围

按照本部分中的步骤删除 IPAM 范围。

Important

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 (p. 19)，然后才能删除范围。

Amazon 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

本部分的命令链接到 Amazon 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。

使用以下 Amazon 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 (p. 20)。要删除 IPAM，请参阅 删除 IPAM (p. 24)。

释放分配

按照本部分中的步骤从 IPAM 池中释放 CIDR 分配。分配是从一个 IPAM 池到另一个资源或 IPAM 池的 CIDR 分配。

如果您计划删除池，则可能需要释放池分配。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 更改资源 CIDR 的监控状态 (p. 22)。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 Amazon CLI 自带公有 IPv4 CIDR 到 IPAM 中 (p. 61) 中的清理或 仅使用 Amazon CLI 自带 IPv6 CIDR 到 IPAM 中 (p. 74) 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 (p. 5)或多账户使用 (p. 4)。

当您释放由 IPAM 管理的 CIDR 时，Amazon VPC IPAM 会将 CIDR 回收回 IPAM 池中。CIDR 需要几分钟时间才能用于将来的分配。有关池和分配的更多信息，请参阅 IPAM 的工作原理 (p. 2)。

Amazon 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 (p. 2)。
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并选择 Deallocate CIDRs（取消分配 CIDR）。
7. 选择 Deallocate CIDR（取消分配 CIDR）。

Command line

本部分的命令链接到 Amazon 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。

使用以下 Amazon 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 分配 CIDR (p. 13)。要在释放分配后删除池，首先必须 从池中取消预置 CIDR (p. 18)。

删除 IPAM

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 (p. 95)。

Important

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。

Amazon 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. 请执行下列操作之一：
   - 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 (p. 23)。
     - 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 (p. 18)。
     - 删除任何其他非默认范围。有关更多信息，请参阅删除范围 (p. 23)。
     - 删除 IPAM 池。有关更多信息，请参阅删除池 (p. 19)。
6. 输入 **`delete`**，然后选择 Delete（删除）。

Command line

本部分的命令链接到 Amazon 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。

使用以下 Amazon 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 (p. 5)。

跟踪 IPAM 中的 IP 地址使用情况

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。

可以按照本部分中的步骤跟踪 IPAM 的 IP 地址使用情况。

目录

使用 IPAM 控制面板监控 CIDR 使用情况

按照本部分中的步骤访问 IPAM 控制面板并查看特定 IPAM 范围内所有 CIDR 的状态。

Amazon 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 Dashboard (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 (p. 2)。
4. 在以下部分中查看监控数据：

   - Scope（范围）：此范围的详细信息。
     - Scope ID（范围 ID）：此范围的 ID。
     - Description（说明）：范围的可选说明。
     - IPAM ID：范围所在的 IPAM 的 ID。
     - Scope type（范围类型）：范围的类型。
   - Summary（摘要）：每个类别的 CIDR 数量。
     - 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。
     - 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）。
     - Pools（池）：范围内的池数量。
     - Compliant CIDRs（合规的 CIDR）：符合范围内 IPAM 池分配规则的资源 CIDR 数量。
     - Overlapping CIDRs（重叠 CIDR）：在范围中的池内重叠的资源 CIDR 的数量。
     - 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。
   - Compliant vs. noncompliant CIDRs（合规与不合规 CIDR）：范围内合规与不合规 CIDR 的数量
   - 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。

- Pool assignment（池分配）：已分配给资源和范围内的人工分配的 IP 空间百分比。
- Pool allocation（池分配）：已分配给范围内其他池的池 IP 空间的百分比。

Command line

控制面板中显示的信息来自 Amazon CloudWatch 中存储的指标。使用 Amazon 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 (p. 17)。

按资源监控 CIDR 使用情况

在 IPAM 中，资源是分配 IP 地址或 CIDR 块的 Amazon 服务实体。IPAM 管理一些资源，但只监控其他资源。

- 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：
  - VPC
  - 公有 IPv4 池

    Important

    公有 IPv4 池和 IPAM 池由 Amazon 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。
- 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 Amazon 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：
  - VPC
  - 公有 IPv4 池
  - VPC 子网
  - 弹性 IP 地址
  - 子网预留

以下步骤演示如何按资源监控 CIDR 使用情况和分配规则合规性。

Amazon 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 (p. 2)。
4. 在以下部分中查看监控数据：
   - Resource ID（资源 ID）：范围的 ID。
   - 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。
- 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。

- 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 Amazon 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。
  - 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。
- Resource name（资源名称）：资源的名称。
- IP 使用情况：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。
- CIDR：与资源关联的 CIDR。
- Region（区域）：资源的 Amazon 区域。
- Owner ID（拥有者 ID）：创建此资源的人员的 Amazon 账户 ID。
- Pool ID（池 ID）：资源所在的 IPAM 池的 ID。

Command line

本部分的命令链接到 Amazon 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。

请使用以下 Amazon 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 IPAM IP 地址使用情况相关的指标（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）。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。创建告警和设置通知不在本用户指南的范围内。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的使用 Amazon CloudWatch 告警。

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

IPAM 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 创建顶级池 (p. 8)。
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 创建顶级池 (p. 8)。
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

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	在范围中的池内重叠的资源 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。

下面列出了可用于筛选 IPAM 指标的维度。

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

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 不监控 Amazon EC2 实例或连接到实例的 EC2 网络接口，但您可以使用 IP 历史洞察功能搜索 EC2 实例和网络接口 CIDR 上的历史数据。

Amazon 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 IP historical insights（IP 历史洞察）。
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。

   #### 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。
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

本部分的命令链接到 Amazon 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。

- 查看 CIDR 的历史记录：get-ipam-address-history

要查看如何使用 Amazon CLI 分析和审计 IP 地址使用情况的示例，请参阅教程：使用 Amazon 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 IP 历史洞察功能搜索此 VPC 的 ID 时，您的 VPC 的开始时间采样为下午 3:05，即 IPAM 发现它的时间，而不是创建 VPC 的时间下午 2:00。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 IP 历史洞察中搜索此 VPC 的 ID 时，下午 5:05 是 VPC CIDR 的结束时间采样，而不是删除 VPC 的时间下午 5:00。

- 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Amazon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。
  - 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）。
- CIDR：与此资源关联的 CIDR。
- Region（区域）：此资源的 Amazon 区域。
- Owner ID（拥有者 ID）：创建此资源的用户的 Amazon 账户 ID（如果适用）。

教程

以下教程为您演示如何使用 Amazon CLI 执行常见 IPAM 任务。要获取 Amazon CLI，请参阅 访问 IPAM (p. 3)。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 (p. 2)。

目录

教程：使用 Amazon CLI 创建 IPAM、创建池并分配 VPC

按照本教程中的步骤使用 Amazon CLI 创建 IPAM、创建池并分配 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 Amazon 区域 1、Amazon 区域 2 中运营
  - 私有范围
    - 顶级池
      - Amazon 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 (p. 95)。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。

目录

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 Amazon 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 Amazon Organizations 集成 (p. 4)。

此请求必须来自 Amazon 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 策略：

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

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

您应看到以下输出，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 Amazon 区域。有关这些运营区域的更多信息，请参阅创建 IPAM (p. 5)。

要使用 Amazon 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，Amazon 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。公有范围适用于将要通过公共互联网访问的 IP 地址。私有范围适用于不会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 Amazon 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 Amazon CLI 为您的所有 Amazon 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 (p. 17)。

使用 Amazon 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"
        }
    ]
}
```

第 5 步 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 Amazon 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 Amazon 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 Amazon 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 Amazon Organizations 集成 (p. 4) 后，您才能完成此步骤。

当您创建 IPAM 池 Amazon RAM 共享时，它将支持跨账户分配 IP。RAM 共享仅在主 Amazon 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 Amazon RAM 共享 IPAM 池 (p. 16)。

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
    }
}
```

第 8 步 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 清除

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 Amazon 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 Amazon CLI 分析和审计 IP 地址使用情况。有关使用 Amazon CLI 的一般信息，请参阅 Amazon 命令行界面用户指南中的使用 Amazon CLI。

目录

概览

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 不监控 Amazon EC2 实例或连接到实例的 EC2 网络接口，但您可以使用 IP 历史洞察功能搜索 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 Amazon 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。

方案

本部分中的场景将向您展示如何使用 Amazon 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 (p. 29)。

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. 运行以下命令：

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

2. 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 (p. 29)。

```
{
    "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 Amazon 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. 运行以下命令：

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

2. 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 (p. 29)。

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

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 (p. 29)。

```
{
    "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. 运行以下命令：

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

2. 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 (p. 29)。

```
{
    "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. 运行以下命令：

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

2. 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 (p. 29)。


```
{
    "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. 运行以下命令：

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

2. 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 (p. 29)。

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

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 Amazon 企业的弹性 IP 地址。

1. 运行以下命令：

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

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

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

教程：BYOIP 地址 CIDR 到 IPAM

本部分中的教程将引导您完成将公有 IP 地址空间带到 Amazon，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 Amazon 账户共享 IP 地址空间。如果不使用 IPAM，您将无法跨 Amazon Organizations 账户共享您的公有 IP 空间。
- 简化将公有 IP 空间带到 Amazon 的过程：您可以使用 IPAM 引导一次公有 IP 地址空间，然后使用 IPAM 在不同区域之间分发公有 IP。如果没有 IPAM，您必须为每个 Amazon 区域登记您的公有 IP。

Important

要完成本教程中的步骤，首先需要使用适用于 Linux 实例的 Amazon EC2 用户指南为您想要带入 Amazon 和 IPAM 的 CIDR 范围完成以下步骤。完成这些步骤后，继续本教程。

按照以下步骤授权 Amazon 发布您的 IP 地址范围。

1. 在 RIR 中创建 ROA 对象。这可能需要您创建密钥对，如创建密钥对和证书中所述。

   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 Amazon 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 Amazon 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`。另外，请注意，`/24` 是最小的 IPv4 块，`/48` 是您可以从区域向互联网传播的最小 IPv6 块。
2. 在 RIR 中更新 RDAP 记录。

按照以下步骤创建证书，使 Amazon 能够验证您是否拥有您想要带入 Amazon 的 IP 地址范围。

1. 创建密钥对和证书。这与创建 ROA 对象时使用的密钥对不同，而是仅用于 Amazon 验证目的的新密钥对。
2. 在 RIR 中创建 ROA 对象。

   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 Amazon 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 Amazon 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`。另外，请注意，`/24` 是最小的 IPv4 块，`/48` 是您可以从区域向互联网传播的最小 IPv6 块。

目录

使用 Amazon 管理控制台和 Amazon CLI 自带公有 IPv4 CIDR 到 IPAM 中

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

Important

要完成本教程中的步骤，首先需要使用适用于 Linux 实例的 Amazon EC2 用户指南为您想要带入 Amazon 和 IPAM 的 CIDR 范围完成以下步骤。完成这些步骤后，继续本教程。

按照以下步骤授权 Amazon 发布您的 IP 地址范围。

1. 在 RIR 中创建 ROA 对象。这可能需要您创建密钥对，如创建密钥对和证书中所述。

   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 Amazon 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 Amazon 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。另外，请注意，/24 是最小的 IPv4 块，/48 是您可以从区域向互联网传播的最小 IPv6 块。
2. 在 RIR 中更新 RDAP 记录。

按照以下步骤创建证书，使 Amazon 能够验证您是否拥有您想要带入 Amazon 的 IP 地址范围。

1. 创建密钥对和证书。这与创建 ROA 对象时使用的密钥对不同，而是仅用于 Amazon 验证目的的新密钥对。
2. 在 RIR 中创建 ROA 对象。

   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 Amazon 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 Amazon 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。另外，请注意，/24 是最小的 IPv4 块，/48 是您可以从区域向互联网传播的最小 IPv6 块。

目录

使用 Amazon 管理控制台和 Amazon 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 Amazon 管理控制台和 Amazon 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 Amazon Organizations 集成 (p. 4).
- 创建 IPAM (p. 5).

- 本教程的每个步骤都必须由以下三个 Amazon Organizations 账户之一完成：
  - 管理账户。
  - 将 IPAM 与 Amazon Organizations 集成 (p. 4) 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。

目录

步骤 1：创建 Amazon CLI 命名配置文件

要以单个 Amazon 用户的身份完成本教程，可以使用 Amazon CLI 命名配置文件从一个 Amazon 账户切换到另一个。命名配置文件是 IAM 访问密钥 ID 和秘密访问密钥的集合，存储在本地，然后在使用 Amazon CLI 时使用 `--profile` 选项。有关如何为 Amazon 账户创建或检索 IAM 访问密钥的更多信息，请参阅 Amazon Identity and Access Management 用户指南中的管理 IAM 用户的访问密钥。

完成 Amazon 命令行界面用户指南中创建命名配置文件的步骤，为本教程中使用的三个 Amazon 账户分别创建命名配置文件：

- 为 Amazon 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 Amazon 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 Amazon Organizations 成员账户创建名为 `member-account` 的配置文件。

创建命名配置文件后，请返回本页面并转至下一步骤。在本教程的其余部分中，您将注意到示例 Amazon 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。

要创建池

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 (p. 2)。
4. 选择 Create pool。
5. （可选）添加池的 Name tag（名称标签）和池的 Description（描述）。
6. 在 Source pool（源池）下，选择 No source pool（无源池）。
7. 在 Address family（地址族）下，选择 IPv4。
8. 在 Locale（区域设置）下，选择 None（无）。

   区域设置是您希望此 IPAM 池可用于分配的 Amazon 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。

   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。
9. 在 CIDRs to provision（要预置的 CIDR）下，选择要为池预置的 CIDR。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`）。您必须在请求中包含 CIDR、BYOIP 消息和证书签名，以便我们验证您是否拥有公有空间。有关 BYOIP 先决条件的列表，包括如何获取此 BYOIP 消息和证书签名，请参阅 使用 Amazon 管理控制台和 Amazon CLI 自带公有 IPv4 CIDR 到 IPAM 中 (p. 47)。
10. 不选中 Use this pool to allocate CIDRs to resources such as VPCs（使用此池将 CIDR 分配给 VPC 等资源）。
11. （可选）为池选择 Tags（标签）。
12. 选择 Create pool。

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 CIDRs 选项卡中查看资源调配状态。请注意，预置 BYOIP CIDR 最多可能需要一周。

第 3 步 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 时配置的操作区域之一。

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 (p. 2)。
4. 选择 Create pool。
5. （可选）添加池的 Name tag（名称标签）和池的 Description（描述）。
6. 在 Source pool（源池）下，选择您在上一部分中创建的顶级池。
7. 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。

区域设置是您希望此 IPAM 池可用于分配的 Amazon 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。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。

8. 在 Service（服务）下，选择 EC2 (EIP/VPC)。您选择的服务将决定可传播 CIDR 的 Amazon 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。
9. 在 CIDRs to provision（要预置的 CIDR）下，选择要为池预置的 CIDR。请注意，将 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`）。
10. 选择 Use this pool to allocate CIDRs to resources such as VPCs（使用此池将 CIDR 分配给 VPC 等资源）。这里的分配规则选项与创建顶级池时的选项相同。请参阅 创建顶级池 (p. 8) 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。
11. 选择 Use this pool to allocate CIDRs to resources such as VPCs（使用此池将 CIDR 分配给 VPC 等资源），并为此池选择可选分配规则：

    - 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。
    - 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`**，则此池中的任何新分配都将默认为网络掩码长度 `/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。
12. （可选）为池选择 Tags（标签）。
13. 配置完池后，选择 Create pool（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 CIDRs 选项卡中查看资源调配状态。

步骤 4：启用使用 Amazon RAM 与 Amazon Organizations 共享资源

您将使用 Amazon RAM 与希望从区域池中为弹性 IP 地址 (EIP) 分配 CIDR 的 Amazon Organizations 成员账户共享您的区域池。在此之前，您必须启用与 Amazon Organizations 的 RAM 集成。

使用管理账户完成 Amazon RAM 用户指南中启用在 Amazon Organizations 内部资源共享中的步骤。如果要使用 Amazon CLI 启用资源共享，请使用 `--profile` **`management-account`** 选项。在 RAM 中启用资源共享后，转到本教程的下一步骤。

步骤 5：使用 Amazon RAM 与 Amazon Organizations 成员账户共享您的区域池

完成 使用 Amazon RAM 共享 IPAM 池 (p. 16) 中的流程，并与 Amazon Organizations 成员账户共享区域池。

此步骤必须由 IPAM 账户完成。如果要使用 Amazon CLI 共享池，请使用 `--profile` **`ipam-account`** 选项。

Important

创建资源共享时，请确保：

- 主体是将从池中为弹性 IP 地址分配 CIDR 的成员账户的账户 ID。
- 将 AWSRAMPermissionIpamPoolByoipCidrImport 权限分配给池。

步骤 6：创建公有 IPv4 池

创建公有 IPv4 池是将公有 IPv4 地址带入将通过 IPAM 管理的 Amazon 中的必要步骤。此步骤应该由预置弹性 IP 地址的成员账户完成。

此步骤必须由成员账户使用 Amazon CLI 完成。

Important

公有 IPv4 池和 IPAM 池由 Amazon 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 Amazon 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 7：将公有 IPv4 CIDR 预置到您的公有 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。

此步骤必须由成员账户使用 Amazon CLI 完成。

要使用 Amazon 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-byoip-cidrs --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。

```
{
    "ByoipCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "StatusMessage": "Cidr successfully provisioned",
            "State": "provisioned"
        }
    ]
}
```

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 Allocations（分配）或 Resources（资源）下查看区域池中的分配。

步骤 8：从公有 IPv4 池创建弹性 IP 地址

完成适用于 Linux 实例的 Amazon EC2 用户指南中分配弹性 IP 地址的步骤，从公有 IPv4 池创建弹性 IP 地址 (EIP)。在 Amazon 管理控制台中打开 EC2 时，分配 EIP 的 Amazon 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 Amazon CLI，请使用 `--profile` **`member-account`** 选项。

步骤 9：将弹性 IP 地址与 EC2 实例相关联

完成适用于 Linux 实例的 Amazon EC2 用户指南中将弹性 IP 地址与实例或网络接口相关联的步骤，以将 EIP 与 EC2 实例相关联。在 Amazon 管理控制台中打开 EC2 时，与 EIP 相关联的 Amazon 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。

此步骤必须由成员账户完成。如果要使用 Amazon CLI，请使用 `--profile` **`member-account`** 选项。

步骤 10：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 Amazon 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 (p. 2)。

4. 选择您在本教程中创建的区域池。
5. 选择 CIDRs 选项卡。
6. 选择 BYOIP CIDR，然后选择 Actions（操作）> Advertise（传播）。
7. 选择 Advertise CIDR（传播 CIDR）。

此时将传播 BYOIP CIDR，而且 Advertising（传播）栏中的值将从 Withdrawn（已撤回）变为 Advertised（已传播）。

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。

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 CIDRs 选项卡。
6. 选择 BYOIP CIDR，然后选择 Actions（操作）> Withdraw from advertising（撤回传播）。
7. 选择 Withdraw CIDR（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：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 Amazon CLI，请使用 `--profile` **`member-account`** 选项。

- 完成适用于 Linux 实例的 Amazon EC2 用户指南中解除弹性 IP 地址的关联的步骤，以解除 EIP 的关联。在 Amazon 管理控制台中打开 EC2 时，解除 EIP 关联的 Amazon 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 Amazon CLI，请使用 `--profile` **`member-account`** 选项。

- 完成适用于 Linux 实例的 Amazon EC2 用户指南中释放弹性 IP 地址的步骤，从公有 IPv4 池释放弹性 IP 地址 (EIP)。在 Amazon 管理控制台中打开 EC2 时，分配 EIP 的 Amazon 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：从您的公有 IPv4 池中取消预置公有 IPv4 CIDR

此步骤必须由成员账户使用 Amazon 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. 运行以下命令以从公有 IPv4 池中释放 CIDR 中的最后一个 IP 地址。输入网络掩码为 `/32` 的 IP 地址。

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

在输出中，您将看到取消预置的 CIDR。

```
{
    "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

> **Important**
>
> 您必须为 CIDR 范围内的每个 IP 地址重新运行此命令。如果您的 CIDR 是 `/24`，则必须运行此命令才能取消预置 `/24` CIDR 中 256 个 IP 地址中的每个地址。

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 5：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 Amazon 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 true（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 Allocations（分配）下查看区域池的详细信息。

步骤 6：删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成

此步骤必须分别由 IPAM 账户和管理账户完成。如果要使用 Amazon CLI 删除 RAM 共享并禁用 RAM 集成，请使用 `--profile ipam-account` 和 `--profile management-account` 选项。

- 按照 Amazon RAM 用户指南中删除 Amazon RAM 中的资源共享和禁用与 Amazon Organizations 的资源共享的顺序，完成删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成的步骤。

步骤 7：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。如果要使用 Amazon 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 (p. 18) 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 8：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 Amazon CLI 共享该池，请使用 `--profile ipam-account` 选项。

- 按顺序完成 删除池 (p. 19) 中的步骤，删除区域池，然后删除顶级池。

使用 Amazon 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 Amazon 管理控制台和 Amazon CLI 分配带有 CIDR 的 VPC。

Important

- 本教程假定您已完成以下部分中的步骤：
  - 将 IPAM 与 Amazon Organizations 集成 (p. 4).
  - 创建 IPAM (p. 5).
- 本教程的每个步骤都必须由以下三个 Amazon Organizations 账户之一完成：
  - 管理账户。
  - 将 IPAM 与 Amazon Organizations 集成 (p. 4) 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。

目录

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（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。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。

要创建池

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 (p. 2)。
4. 选择 Create pool。
5. （可选）添加池的 Name tag（名称标签）和池的 Description（描述）。
6. 在 Source pool（源池）下，选择 No source pool（无源池）。
7. 在 Address family（地址族）下，选择 IPv6。
8. 确保选择了 Allow CIDRs in this pool to be publicly advertisable（允许此池中的 CIDR 可公开传播）。
9. 在 Locale（区域设置）下，选择 None（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 Amazon 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。

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 CIDRs to provision（要预置的 CIDR）下，选择要为池预置的 CIDR。请注意，将 IPv6 CIDR 预置到顶级池中的资源池时，您可以为可传播 IPAM 池预置的最低 IPv6 CIDR 为 `/48`；不允许使用更具体的 CIDR（例如 `/49`）。您可以为不可传播的 IPAM 池带来的最低 CIDR 为 `/56;`；不允许使用更具体的 CIDR（例如 `/57`）。您必须在请求中包含 CIDR、BYOIP 消息和证书签名，以便我们验证您是否拥有公有空间。有关 BYOIP 先决条件的列表，包括如何获取此 BYOIP 消息和证书签名，请参阅 使用 Amazon 管理控制台和 Amazon CLI 自带公有 IPv4 CIDR 到 IPAM 中 (p. 47)。
11. 不选中 Use this pool to allocate CIDRs to resources such as VPCs（使用此池将 CIDR 分配给 VPC 等资源）。
12. （可选）为池选择 Tags（标签）。
13. 选择 Create pool。

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 CIDRs 选项卡中查看资源调配状态。请注意，预置 BYOIP CIDR 最多可能需要一周。

第 2 步 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 (p. 2)。
4. 选择 Create pool。
5. （可选）添加池的 Name tag（名称标签）和池的描述。
6. 在 Source pool（源池）下，选择您在上一部分中创建的顶级池。
7. 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 Amazon 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。
8. 在 Service（服务）下，选择 EC2 (EIP/VPC)。您选择的服务将决定可传播 CIDR 的 Amazon 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。
9. 在 CIDRs to provision（要预置的 CIDR）下，选择要为池预置的 CIDR。请注意，将 IPv6 CIDR 预置到顶级池中的资源池时，您可以为可传播 IPAM 池预置的最低 IPv6 CIDR 为 `/48`；不允许使用更具体的 CIDR（例如 `/49`）。您可以为不可传播的 IPAM 池带来的最低 CIDR 为 `/56`；不允许使用更具体的 CIDR（例如 `/57`）。
10. 选择 Use this pool to allocate CIDRs to resources such as VPCs（使用此池将 CIDR 分配给 VPC 等资源），并为此池选择可选分配规则：

    - 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。
- 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。

11. （可选）为池选择 Tags（标签）。
12. 配置完池后，选择 Create pool（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 CIDRs 选项卡中查看资源调配状态。

步骤 3：启用使用 Amazon RAM 与 Amazon Organizations 共享资源

您将使用 Amazon RAM 与希望从区域池中为 VPC 分配 CIDR 的 Amazon Organizations 成员账户共享您的区域池。在此之前，您必须启用与 Amazon Organizations 的 RAM 集成。

在继续本教程之前，管理账户必须完成 Amazon RAM 用户指南中启用在 Amazon Organizations 内部资源共享中的步骤。在 RAM 中启用资源共享后，转到本教程的下一步骤。

步骤 4：使用 Amazon RAM 与 Amazon Organizations 成员账户共享您的区域池

完成 使用 Amazon RAM 共享 IPAM 池 (p. 16) 中的流程，并与 Amazon Organizations 成员账户共享区域池。

此步骤必须由 IPAM 账户完成。

Important

创建资源共享时，请确保：

- 主体是将从池中分配 CIDR 的成员账户的账户 ID。
- 将 AWSRAMPermissionIpamPoolByoipCidrImport 权限分配给池。

步骤 5：创建 VPC

完成 Amazon VPC 用户指南的创建 VPC 中的步骤。

此步骤必须由成员账户完成。

Note

- 在 Amazon 管理控制台中打开 VPC 时，创建 VPC 的 Amazon 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。
- 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，Amazon 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 Allocations（分配）选项卡来查看 IPAM 中的分配。

步骤 6：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 Amazon 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 (p. 2)。
4. 选择您在本教程中创建的区域池。
5. 选择 CIDRs 选项卡。
6. 选择 BYOIP CIDR，然后选择 Actions（操作）> Advertise（传播）。
7. 选择 Advertise CIDR（传播 CIDR）。

此时将传播 BYOIP CIDR，Advertising（传播）栏中的值将从 Withdrawn（已撤回）变为 Advertised（已传播）。

步骤 7：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 CIDRs 选项卡。
6. 选择 BYOIP CIDR，然后选择 Actions（操作）> Withdraw from advertising（撤回传播）。
7. 选择 Withdraw CIDR（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 用户指南中删除 VPC 的步骤，删除 VPC。在 Amazon 管理控制台中打开 VPC 时，从中删除 VPC 的 Amazon 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 Allocations（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。

步骤 3：删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成

此步骤必须分别由 IPAM 账户和管理账户完成。

- 按照 Amazon RAM 用户指南中删除 Amazon RAM 中的资源共享和禁用与 Amazon Organizations 的资源共享的顺序，完成删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成的步骤。

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 (p. 18) 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 (p. 19) 中的步骤，删除区域池，然后删除顶级池。

仅使用 Amazon CLI 自带公有 IPv4 CIDR 到 IPAM 中

按照以下步骤，仅使用 Amazon CLI 将 IPv4 或 IPv6 CIDR 带入 IPAM 中。

Important

要完成本教程中的步骤，首先需要使用适用于 Linux 实例的 Amazon EC2 用户指南为您想要带入 Amazon 和 IPAM 的 CIDR 范围完成以下步骤。完成这些步骤后，继续本教程。

按照以下步骤授权 Amazon 发布您的 IP 地址范围。

1. 在 RIR 中创建 ROA 对象。这可能需要您创建密钥对，如创建密钥对和证书中所述。

   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 Amazon 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 Amazon 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。另外，请注意，/24 是最小的 IPv4 块，/48 是您可以从区域向互联网传播的最小 IPv6 块。
2. 在 RIR 中更新 RDAP 记录。

按照以下步骤创建证书，使 Amazon 能够验证您是否拥有您想要带入 Amazon 的 IP 地址范围。

1. 创建密钥对和证书。这与创建 ROA 对象时使用的密钥对不同，而是仅用于 Amazon 验证目的的新密钥对。
2. 在 RIR 中创建 ROA 对象。

   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 Amazon 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 Amazon 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。另外，请注意，/24 是最小的 IPv4 块，/48 是您可以从区域向互联网传播的最小 IPv6 块。

目录

仅使用 Amazon 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 Amazon 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 Amazon Organizations 集成 (p. 4).
  - 创建 IPAM (p. 5).
- 本教程的每个步骤都必须由以下三个 Amazon Organizations 账户之一完成：
  - 管理账户。
  - 将 IPAM 与 Amazon Organizations 集成 (p. 4) 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。

目录

步骤 1：创建 Amazon CLI 命名配置文件

要以单个 Amazon 用户的身份完成本教程，可以使用 Amazon CLI 命名配置文件从一个 Amazon 账户切换到另一个。命名配置文件是 IAM 访问密钥 ID 和秘密访问密钥的集合，存储在本地，然后在使用 Amazon CLI 时使用 `--profile` 选项。有关如何为 Amazon 账户创建或检索 IAM 访问密钥的更多信息，请参阅 Amazon Identity and Access Management 用户指南中的管理 IAM 用户的访问密钥。

完成 Amazon 命令行界面用户指南中创建命名配置文件的步骤，为本教程中使用的三个 Amazon 账户分别创建命名配置文件：

- 为 Amazon 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 Amazon 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 Amazon Organizations 成员账户创建名为 `member-account` 的配置文件。

创建命名配置文件后，请返回本页面并转至下一步骤。在本教程的其余部分中，您将注意到示例 Amazon 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。

运行以下 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 Amazon CLI 为您的所有 Amazon 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`）。您必须在请求中包含 CIDR、BYOIP 消息和证书签名，以便我们验证您是否拥有公有空间。有关 BYOIP 先决条件的列表，包括如何获取此 BYOIP 消息和证书签名，请参阅 仅使用 Amazon CLI 自带公有 IPv4 CIDR 到 IPAM 中 (p. 60)。

此步骤必须由 IPAM 账户完成。

> **Important**
>
> 当您将 BYOIP CIDR 预置到顶级池时，您只需要添加 `--cidr-authorization-context`。对于顶级池中的区域池，您可以省略 `--cidr-authorization-context` 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 Amazon 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-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --cidr-authorization-
context Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsMaUOP7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d65uyZZiD
hApR89Kt6GxRYOdRaNx8yt~uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUcO2o8oJZQyYXRpgqcWGVJdQ__" --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。请注意，预置 BYOIP CIDR 最多可能需要一周。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。`--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。区域设置是您希望此 IPAM 池可用于分配的 Amazon 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。

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 Amazon 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 Amazon 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。请注意，将 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`）。

此步骤必须由 IPAM 账户完成。

要使用 Amazon 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：启用使用 Amazon RAM 与 Amazon Organizations 共享资源

您将使用 Amazon RAM 与希望从区域池中为 VPC 分配 CIDR 的 Amazon Organizations 成员账户共享您的区域池。在此之前，您必须启用与 Amazon Organizations 的 RAM 集成。

使用管理账户完成 Amazon RAM 用户指南中启用在 Amazon Organizations 内部资源共享中的步骤。如果要使用 Amazon CLI 启用资源共享，请使用 `--profile` **`management-account`** 选项。在 RAM 中启用资源共享后，转到本教程的下一步骤。

步骤 8：使用 Amazon RAM 与 Amazon Organizations 成员账户共享您的区域池

完成 使用 Amazon RAM 共享 IPAM 池 (p. 16) 中的流程，并与 Amazon Organizations 成员账户共享区域池。

此步骤必须由 IPAM 账户完成。如果要使用 Amazon CLI 共享池，请使用 `--profile` **`ipam-account`** 选项。

> **Important**
>
> 创建资源共享时，请确保：
>
> - 主体是将从池中为弹性 IP 地址分配 CIDR 的成员账户的账户 ID。
> - 将 AWSRAMPermissionIpamPoolByoipCidrImport 权限分配给池。

步骤 9：创建公有 IPv4 池

创建公有 IPv4 池是将公有 IPv4 地址带入将通过 IPAM 管理的 Amazon 中的必要步骤。此步骤通常由不同的想要预置弹性 IP 地址的 Amazon 账户完成。

此步骤必须由成员账户完成。

> **Important**
>
> 公有 IPv4 池和 IPAM 池由 Amazon 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 Amazon 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 10：将公有 IPv4 CIDR 预置到您的公有 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。

此步骤必须由成员账户完成。

要使用 Amazon 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 11：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 Amazon 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 12：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 Amazon 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。

开始使用 Amazon 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 13：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` 的值必须与您在创建将用于 BYOIP CIDR 的池时输入的 `--locale` 选项匹配。

使用 Amazon 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": []
        }
    ]
}
```

5. 从公有 IPv4 池中释放 CIDR 中的最后一个 IP 地址。输入网络掩码为 /32 的 IP 地址。您必须为 CIDR 范围内的每个 IP 地址重新运行此命令。如果您的 CIDR 是 `/24`，则必须运行此命令才能取消预置 `/24` CIDR 中 256 个 IP 地址中的每个地址。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 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-
ec2-0019eed22a684e0b2 --cidr 130.137.245.255/32 --profile member-account
```

   在输出中，您将看到取消预置的 CIDR。

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",

    "DeprovisionedAddresses": [

        "130.137.245.255"
```

```
    ]

}
```

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": []
        }
    ]
}
```

7. 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。

```
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": []
}
```

8. 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"

    }

}
```

9. 删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成。按照 Amazon RAM 用户指南中删除 Amazon RAM 中的资源共享和禁用与 Amazon Organizations 的资源共享的顺序，完成删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成的步骤。

   此步骤必须分别由 IPAM 账户和管理账户完成。如果要使用 Amazon CLI 删除 RAM 共享并禁用 RAM 集成，请使用 `--profile ipam-account` 和 `--profile management-account` 选项。

10. 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 delete（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"
    }
}
```

11. 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"

    }

}
```

12. 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 delete（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"
    }
}
```

13. 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"
            }
        ],
    }
}
```

仅使用 Amazon 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 Amazon CLI 分配 VPC。

Important

- 本教程假定您已完成以下部分中的步骤：
  - 将 IPAM 与 Amazon Organizations 集成 (p. 4).
  - 创建 IPAM (p. 5).
- 本教程的每个步骤都必须由以下三个 Amazon Organizations 账户之一完成：
  - 管理账户。
  - 将 IPAM 与 Amazon Organizations 集成 (p. 4) 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。

目录

步骤 1：创建 Amazon CLI 命名配置文件

要以单个 Amazon 用户的身份完成本教程，可以使用 Amazon CLI 命名配置文件从一个 Amazon 账户切换到另一个。命名配置文件是 IAM 访问密钥 ID 和秘密访问密钥的集合，存储在本地，然后在使用 Amazon CLI 时使用 `--profile` 选项。有关如何为 Amazon 账户创建或检索 IAM 访问密钥的更多信息，请参阅 Amazon Identity and Access Management 用户指南中的管理 IAM 用户的访问密钥。

完成 Amazon 命令行界面用户指南中创建命名配置文件的步骤，为本教程中使用的三个 Amazon 账户分别创建命名配置文件：

- 为 Amazon 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 Amazon 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 Amazon Organizations 成员账户创建名为 `member-account` 的配置文件。

创建命名配置文件后，请返回本页面并转至下一步骤。在本教程的其余部分中，您将注意到示例 Amazon 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。

运行以下 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 Amazon 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 Amazon CLI 为您的所有 Amazon 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，将 IPv6 CIDR 预置到顶级池中的资源池时，您可以为可传播 IPAM 池预置的最低 IPv6 CIDR 为 `/48`；不允许使用更具体的 CIDR（例如 `/49`）。您可以为不可传播的 IPAM 池带来的最低 CIDR 为 `/56`；不允许使用更具体的 CIDR（例如 `/57`）。您必须在请求中包含 CIDR、BYOIP 消息和证书签名，以便我们验证您是否拥有公有空间。有关 BYOIP 先决条件的列表，包括如何获取此 BYOIP 消息和证书签名，请参阅 仅使用 Amazon CLI 自带公有 IPv4 CIDR 到 IPAM 中 (p. 60)。

当您将 BYOIP CIDR 预置到顶级池时，您只需要添加 `--cidr-authorization-context`。对于顶级池中的区域池，您可以省略 `--cidr-authorization-context` 选项。

此步骤必须由 IPAM 账户完成。

使用 Amazon 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-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --cidr-authorization-
context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|
SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~Crt-
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSaDcT~tW4C
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --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。请注意，预置 BYOIP CIDR 最多可能需要一周。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 Amazon 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 Amazon 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，将 CIDR 预置到顶级池中的资源池时，您可以为可传播 IPAM 池预置的最低 IPv6 CIDR 为 `/48`；不允许使用更具体的 CIDR（例如 `/49`）。您可以为不可传播的 IPAM 池带来的最低 CIDR 为 `/56`；不允许使用更具体的 CIDR（例如 `/57`）。

此步骤必须由 IPAM 账户完成。

要使用 Amazon 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"
        }
    ]
}
```

步骤 7：启用使用 Amazon RAM 与 Amazon Organizations 共享资源

您将使用 Amazon RAM 与希望从区域池中为 VPC 分配 CIDR 的 Amazon Organizations 成员账户共享您的区域池。在此之前，您必须启用与 Amazon Organizations 的 RAM 集成。

使用管理账户完成 Amazon RAM 用户指南中启用在 Amazon Organizations 内部资源共享中的步骤。如果要使用 Amazon CLI 启用资源共享，请使用 `--profile` **`management-account`** 选项。在 RAM 中启用资源共享后，转到本教程的下一步骤。

步骤 8：使用 Amazon RAM 与 Amazon Organizations 成员账户共享您的区域池

完成 使用 Amazon RAM 共享 IPAM 池 (p. 16) 中的流程，并与 Amazon Organizations 成员账户共享区域池。

此步骤必须由 IPAM 账户完成。如果要使用 Amazon CLI 共享池，请使用 `--profile` **`ipam-account`** 选项。

Important

创建资源共享时，请确保：

- 主体是将从池中为弹性 IP 地址分配 CIDR 的成员账户的账户 ID。
- 将 AWSRAMPermissionIpamPoolByoipCidrImport 权限分配给池。

步骤 9：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 Amazon 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 10：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 Amazon 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 Amazon 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 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 Amazon CLI 清除

1. 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": []
}
```

5. 删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成。按照 Amazon RAM 用户指南中删除 Amazon RAM 中的资源共享和禁用与 Amazon Organizations 的资源共享的顺序，完成删除 RAM 共享并禁用与 Amazon Organizations 的 RAM 集成的步骤。

   此步骤必须分别由 IPAM 账户和管理账户完成。如果要使用 Amazon CLI 删除 RAM 共享并禁用 RAM 集成，请使用 `--profile ipam-account` 和 `--profile management-account` 选项。

6. 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 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"
    }
}
```

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"
            }
        ]
    }
}
```

教程：将现有的 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 Amazon 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。如果您是第一次将新 IP 地址引入 Amazon，请完成 教程：BYOIP 地址 CIDR 到 IPAM (p. 46) 中的步骤。

Important

- 本教程假设您已完成 创建 IPAM (p. 5) 中的步骤。
- 本教程的每个步骤都必须由以下两个 Amazon 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。

Note

IPAM 账户必须通过 Amazon RAM 与 BYOIP CIDR 所有者共享池，并包括关于共享资源的 `AWSRAMPermissionIpamPoolByoipCidrImport` 策略。有关更多信息，请参阅 使用 Amazon RAM 共享 IPAM 池 (p. 16)。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`

目录

步骤 1：创建 Amazon CLI 命名配置文件

要以单个 Amazon 用户的身份完成本教程，可以使用 Amazon CLI 命名配置文件从一个 Amazon 账户切换到另一个。命名配置文件是 IAM 访问密钥 ID 和秘密访问密钥的集合，存储在本地，然后在使用 Amazon CLI 时使用 `--profile` 选项。有关如何为 Amazon 账户创建或检索 IAM 访问密钥的更多信息，请参阅 Amazon Identity and Access Management 用户指南中的管理 IAM 用户的访问密钥。

完成 Amazon 命令行界面用户指南中创建命名配置文件的步骤，为本教程中使用的各个 Amazon 账户分别创建命名配置文件：

- 为 IPAM 管理员 Amazon 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 Amazon 账户创建名为 `byoip-owner-account` 的配置文件。

创建命名配置文件后，请返回本页面并转至下一步骤。在本教程的其余部分中，您将注意到示例 Amazon 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 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 账户执行。您创建的 IPAM 池必须是 `--locale` 选项与 BYOIP CIDR Amazon 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 Amazon 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 Amazon 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 --ipam-scope-id ipam-
scope-0087d83896280b594 --description "top-level-pool" --locale us-west-2 --aws-service
 ec2 --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": "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：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 CIDR 所有者账户执行。

要使用 Amazon CLI 将 BYOIP 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 Amazon 区域。

```
aws ec2 move-byoip-cidr-to-ipam --region us-west-2 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --ipam-pool-owner 123456789012 --cidr 130.137.249.0/24 --
profile byoip-owner-account
```

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 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --ipam-pool-owner 123456789012 --cidr 130.137.249.0/24 --
profile byoip-owner-account
```

下面的示例输出显示状态。

```
{
```

```
    "ByoipCidr": {
        "Cidr": "130.137.249.0/24",
        "State": "complete-transfer"

    }
}
```

步骤 5：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 账户执行。

要使用 Amazon 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 Amazon 区域。

```
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": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "470889052924"
        }
    ]
}
```

步骤 6：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 账户执行。

要使用 Amazon CLI 清除本教程中创建的资源

1. 运行以下命令以获取 BYOIP CIDR 的分配 ID。确保 `--region` 值与 BYOIP CIDR 的 Amazon 区域匹配。

```
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": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "470889052924"
        }
    ]
```

```
}
```

2. 运行以下命令以取消分配 BYOIP CIDR。IPAM 可能需要一些时间才能发现 VPC 已被删除并删除此分配。确保 `--region` 值是 BYOIP CIDR 的 Amazon 区域。

```
aws ec2 release-ipam-pool-allocation --region us-west-2 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --cidr 130.137.249.0/24 --ipam-pool-allocation-id ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46 --profile ipam-account
```

输出将显示从 IPAM 中删除的分配。

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

3. 运行以下命令以删除顶级池。

```
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",
        "AwsService": "ec2"
    }
}
```

IPAM 中的 Identity and Access Management

Amazon 使用安全凭证来识别您的身份并向您授予对 Amazon 资源的访问权限。利用 Amazon 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 Amazon 资源。

本部分介绍专门为 IPAM 创建的 Amazon 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 Amazon 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。

目录

IPAM 的服务相关角色

Amazon Identity and Access Management (IAM) 中的服务相关角色使 Amazon 服务能够代表您调用 Amazon 服务。有关服务相关角色的更多信息，请参见 IAM 用户指南中的使用服务相关角色。

目前 IPAM 只有一个服务相关角色：AWSServiceRoleForIPAM。

授予给服务相关角色的权限

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 Amazon 托管策略 (p. 93)。

附加到此服务相关角色的还包括允许 `ipam.amazonaws.com` 服务代入所需服务相关角色的 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 Amazon Organizations 集成时

  如果 将 IPAM 与 Amazon Organizations 集成 (p. 4) 使用 IPAM 控制台或使用 `enable-ipam-organization-admin-account` Amazon CLI CLI 命令，则 AWSServiceRoleForIPAM 服务相关角色将在您的每个 Amazon 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 Amazon Organizations 集成的 Amazon 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 Amazon 账户创建 IPAM 时

  如果将 IPAM 用于单个账户 (p. 5)，则当您将 IPAM 创建为账户时，将自动创建 AWSServiceRoleForIPAM 服务相关角色。

  Important

  如果您将 IPAM 与单个 Amazon 账户一起使用，则在创建 IPAM 之前，必须确保您使用的 Amazon 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 IAM 策略。

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Amazon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。

请按照以下步骤通过 Amazon 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 (p. 18) 和 删除 IPAM (p. 24)。
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 Amazon 托管策略

如果将 IPAM 与单个 Amazon 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 Amazon Organizations 的集成，将自动在您的 IAM 账户和每个 Amazon 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 Amazon 企业的所有成员中监控与 EC2 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。

以下示例显示所创建托管策略的详细信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        },
        {
            "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 Amazon 账户或 Amazon 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 Amazon 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 (p. 26)。

对 Amazon 托管策略的更新

查看有关 IPAM 的 Amazon 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
IPAM 已开启跟踪更改	IPAM 为其 Amazon 托管策略开启了跟踪更改。	2021 年 12 月 2 日

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 Service Quotas 用户指南 中的请求增加配额。

名称	默认值	可调整
每个企业的 IPAM 管理员数	1	否
每个区域的 IPAM	1	否
每个 IPAM 的范围	5	是
每个范围的池	50	是
每个池的 CIDR	50	是
池深度（池内的池数量）	10	是

Note

您不能使用 IPAM 跨多个 Amazon Organizations 管理 IP 地址。

Pricing

对于 IPAM 监控的每个活动 IP 地址，您需要按小时付费。活动 IP 地址定义为分配给 EC2 实例或弹性网络接口 (ENI) 等资源的 IP 地址。有关更多信息，请参阅 IPAM 定价。

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
首次发布	此版本介绍了 Amazon VPC IP 地址管理器。	2021 年 12 月 2 日