IP Address Manager

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: IP Address Manager

Table of Contents

IPAM とは

Amazon VPC IP Address Manager (IPAM)は、AWS ワークロードの IP アドレスを計画、追跡、監視しやすくする VPC 機能です。IPAM の自動ワークフローを使用して、IP アドレスをより効率的に管理できます。

IPAM を使用して、以下を行うことができます。

- IP アドレス空間をルーティングドメインとセキュリティードメインに整理する
- 使用中の IP アドレス空間を監視し、空間を使用しているリソースをビジネスルールに照らし合わせて監視する
- 組織内の IP アドレス割り当ての履歴を表示する
- 特定のビジネスルールを使用して CIDR を VPC に自動的に割り当てる
- ネットワーク接続に関する問題のトラブルシューティングを行う
- 独自の IP (BYOIP) アドレスのクロスリージョンおよびクロスアカウント共有を有効にする
- VPC の作成のために Amazon 提供の連続した IPv6 CIDR ブロックをプールにプロビジョニングする

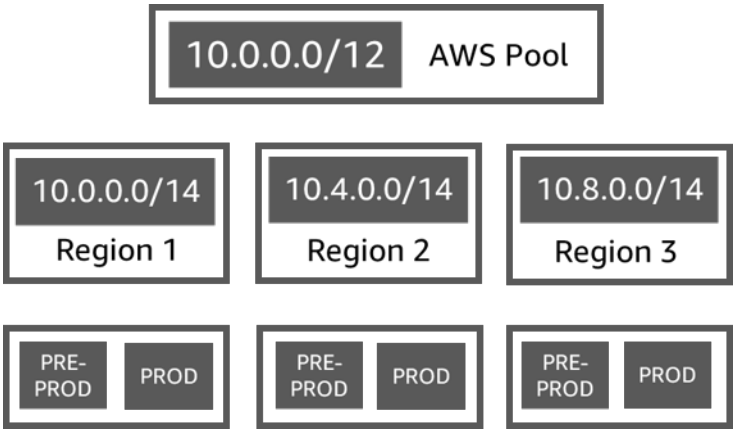
このガイドには以下のセクションがあります。

- IPAM の仕組み: IPAM の概念と用語
- IPAM の開始方法: AWS Organizations による全社的な IP アドレス管理を可能にし、IPAM を作成し、IP アドレス使用を計画するステップ。
- IPAM で IP アドレス空間を管理する: IPAM、スコープ、プール、および割り当てを管理するステップ。
- IPAM での IP アドレス使用状況の追跡: IPAM を使用して IP アドレスの使用状況を監視および追跡するステップ。
- Amazon VPC IP Address Manager のチュートリアル: IPAM とプールを作成し、VPC CIDR を割り当て、独自のパブリック IP アドレス CIDR を IPAM に取り込むための詳細な説明。

IPAM の仕組み

このトピックでは、IPAM の使用開始に役立ついくつかの重要な概念について説明します。

次の図に示しているのは、トップレベル IPAM プール内の複数の AWS リージョンの IPAM プール階層です。各 AWS リージョンプールには、2 つの IPAM 開発プールがあります。1 つは本番稼働前用のプールでもう 1 つは本番稼働リソース用のプールです。IPAM の概念に関する詳細については、この図の下の説明を参照してください。



Amazon VPC IP Address Manager を使用するには、まず IPAM を作成します。

IPAM の作成時に、作成先の AWS リージョンを選択します。IPAM を作成すると、AWS VPC IPAM では、IPAM 用の 2 つのスコープが自動的に作成されます。スコープは、プールおよび割り当てとともに、IPAM の主要なコンポーネントです。

- スコープは IPAM 内の最上位のコンテナです。IPAM を作成すると、デフォルトのパブリックスコープとデフォルトのプライベートスコープが自動的に作成されます。各スコープは、単一のネットワークの IP 空間を表します。[プライベートスコープ] は、インターネットにアドバタイズできないすべての IP アドレスを対象としています。[パブリックスコープ] は通常、 AWS からインターネットにアドバタイズできるすべての IP アドレスを対象としています。BYOIPv6 アドレスを IPAM プールにプロビジョニングする際には、パブリックスコープ内のアドレスがパブリックにアドバタイズされないように設定できます。スコープを使用すると、IP アドレスの重複や競合を引き起こすことなく、接続されていない複数のネットワーク間で IP アドレスを再利用できます。スコープ内で、IPAM プールを作成します。
- プールは、連続した IP アドレス範囲 (CIDR) の集合です。IPAM プールを使用すると、ルーティングとセキュリティのニーズに応じて IP アドレスを整理できます。トップレベルプール内に複数のプールを含めることができます。例えば、開発アプリケーションと本番アプリケーションで別々

のルーティングとセキュリティのニーズがある場合は、それぞれにプールを作成できます。IPAM プール内では、CIDR を AWS リソースに割り当てることができます。

- 割り当てとは、IPAM プールから別のリソースまたは IPAM プールへの CIDR 割り当てです。VPC を作成し、VPC の CIDR の IPAM プールを選択すると、IPAM プールにプロビジョニングされた CIDR から CIDR が割り当てられます。IPAM を使用して、割り振りを監視および管理できます。

IPAM は、パブリック IPv6 スペースとプライベート IPv6 スペースを管理およびモニタリングできます。パブリックおよびプライベート IPv6 アドレスの詳細については、「Amazon VPC ユーザーガイド」の「IPv6 アドレス」を参照してください。

開始して IPAM を作成するには、IPAM の開始方法を参照してください。

IPAM の開始方法

このセクションのステップに従って IPAM の使用を開始します。このセクションは IPAM の使用を迅速に開始することを目的としていますが、このセクションのステップで達成できることはニーズに合わない場合があります。IPAM を使用するさまざまな方法については、「IP アドレスのプロビジョニング計画」および「Amazon VPC IP Address Manager のチュートリアル」を参照してください。

このセクションでは、まず、IPAM にアクセスし、IPAM アカウントを委任するかどうかを決定します。このセクションを完了すると、IPAM を作成し、複数の IP アドレスプールを作成し、プール内の CIDR を VPC に割り当てることができます。

タスク

- IPAM へのアクセス
- IPAM の統合オプションを設定する
- IPAM を作成する
- IP アドレスのプロビジョニング計画
- IPAM プールから CIDR を割り当てる

IPAM へのアクセス

他の AWS サービスと同様に、次の方法を使用して IPAM の作成、アクセス、管理を行うことができます。

- AWSマネジメントコンソール: IPAM の作成と管理に使用するウェブインターフェイスを提供します。https://console.aws.amazon.com/ipam/ を開きます。
- AWS Command Line Interface (AWS CLI): Amazon VPC を含む一連のさまざまな AWS のサービス用のコマンドを提供します。AWS CLI は、Windows、macOS、Linux でサポートされています。を取得する方法については、「AWS CLI」を参照してください。。AWS Command Line Interface
- AWS SDK: 言語固有の API を提供します。AWS SDK は、署名の計算、リクエストの再試行処理、エラー処理など、接続のさまざまな詳細を処理します。詳細については、AWS SDK をご参照ください。
- クエリ API: HTTPS リクエストを使用して呼び出す低レベル API アクションを提供します。クエリ API の使用は、IPAM にアクセスする最も直接的な方法です。ただし、この方法では、リクエストに署名するハッシュの生成やエラー処理など、低レベルの詳細な作業をアプリケーションで処理

する必要があります。詳細については、Amazon EC2 API リファレンスの Amazon IPAM アクションを参照してください。

このガイドでは、主に AWS マネージメントコンソールを使用して、IPAM の作成、アクセス、管理を行います。コンソールでプロセスを完了する方法の各説明には、AWS CLI を使用して同じタスクを実行できるように、AWS CLI コマンドリファレンスへのリンクを含めています。

IPAM を初めて使用する場合は、IPAM の仕組み を参照して Amazon VPC での IPAM のロールについて学習し、IPAM の統合オプションを設定する の手順に進みます。

IPAM の統合オプションを設定する

このセクションでは、IPAM を AWS Organizations や他の AWS アカウントと統合する方法、または単一の AWS アカウントで使用する方法のオプションについて説明します。

IPAM の使用を開始する前に、このセクションのオプションのいずれかを選択して、IPAM が EC2 ネットワークリソースに関連付けられた CIDR をモニタリングし、メトリクスを保存できるようにする必要があります。

- IPAM を AWS Organizations と統合して、Amazon VPC IPAM サービスがすべての AWS Organizations メンバーアカウントによって作成されたネットワークリソースを管理および監視できるようにするには、「IPAM を AWS Organizations 内のアカウントと統合する」を参照してください。
- AWS Organizations との統合後に IPAM を組織外のアカウントと統合する場合は、「IPAM を組織外のアカウントに統合する」を参照してください。
- IPAM で単一の AWS アカウントを使用し、単一のアカウントで作成したネットワークリソースを Amazon VPC IPAM サービスが管理および監視できるようにするには、IPAM を 1 つのアカウントで使用する を参照してください。

これらのオプションのいずれかを選択しない場合でも、プールなどの IPAM リソースを作成できますが、ダッシュボードにメトリクスが表示されず、リソースのステータスを監視できません。

内容

IPAM を AWS Organizations 内のアカウントと統合する

必要に応じて、このセクションの手順に従って、IPAM をAWS Organizations と統合し、メンバーアカウントを IPAM アカウントとして委任します。

IPAM アカウントは、IPAM を作成し、それを使用して IP アドレスの使用状況を管理および監視します。

IPAM を AWS Organizations と統合し、IPAM 管理者を委任すると、次の利点があります。

- IPAM プールを組織と共有する: IPAM アカウントを委任すると、IPAM によって、組織内の他の AWS Organizations メンバーアカウントで、AWS Resource Access Manager (RAM) を使用して共有される IPAM プールから CIDR を割り当てることができるようになります。組織のセットアップの詳細については、AWS Organizations ユーザーガイドの AWS Organizations とは を参照してください。
- 組織内の IP アドレスの使用状況をモニタリングする: IPAM アカウントを委任する場合、すべてのアカウントに IP 使用状況を監視する IPAM アクセス許可を付与します。その結果、IPAM では、他の AWS Organizations メンバーアカウント間で既存の VPC によって使用されている CIDR が自動的にインポートされます。

AWS Organizations メンバーアカウントを IPAM アカウントとして委任しない場合は、IPAM を作成するために使用した AWS アカウント内のみで、リソースが IPAM によってモニタリングされます。

> **Note**
>
> AWS Organizations と統合する場合:
>
> - AWS マネジメントコンソールで IPAM を使用するか enable-ipam-organization-admin-account AWS CLI コマンドを使用して、AWS Organizations との統合を有効にする必要があります これにより、`AWSServiceRoleForIPAM` サービスにリンクされたロールが確実に作成されます。AWS Organizations コンソールまたは register-delegated-administrator AWS CLI コマンドを使用して、AWS Organizations への信頼されたアクセスを有効にする場合、`AWSServiceRoleForIPAM` サービスにリンクされたロールは作成されず、組織内のリソースを管理または監視することはできません。
> - IPAM アカウントは AWS Organizations のメンバーアカウントである必要があります。AWS Organizations 管理アカウントを IPAM アカウントとして使用することはできません。IPAM が AWS Organizations と既に統合されているかどうかを確認するには、以下のステップを使用して、[Organization の設定] で統合の詳細を表示します。

- IPAM では、組織のメンバーアカウントで監視するアクティブな IP アドレスごとに課金されます。料金に関する詳細については、IPAM の料金を参照してください。
- AWS Organizations アカウントおよび 1 つ以上のメンバーアカウントで設定された管理アカウントが必要です。アカウントタイプの詳細については、AWS ユーザーガイドの用語とコンセプトを参照してください。詳細については、Organizations ユーザーガイドの AWS Organizations の開始方法を参照してください。
- IPAM アカウントには、`iam:CreateServiceLinkedRole` アクションを許可する IAM ポリシーがアタッチされている IAM ロールを使用する必要があります。IPAM を作成した場合、AWSServiceRoleForIPAM サービスにリンクされたロールが自動的に作成されます。
- AWS Organizations 管理アカウントに関連付けられているユーザーは、次の IAM ポリシーアクションがアタッチされている IAM ロールを使用する必要があります。
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`
  - `iam:CreateServiceLinkedRole`

  IAM ロールの作成について詳しくは、「IAM ユーザーガイド」の「IAM ユーザーにアクセス許可を委任するロールの作成」を参照してください。
- AWS Organizations 管理アカウントに関連付けられているユーザーは、次の IAM ポリシーアクションがアタッチされた IAM ロールを使用して、現在の AWS Orgs の委任された管理者を一覧表示することができます: `organizations:ListDelegatedAdministrators`

AWS Management Console

IPAM アカウントを選択するには

1. AWS Organizations 管理アカウントを使用して、IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. AWS マネジメントコンソールで、IPAM を使用する AWS リージョンを選択します。
3. ナビゲーションペインで [組織の設定] を選択します。
4. [委任] オプションは、AWS Organizations 管理アカウントでコンソールにログインしている場合にのみ使用できます。[委任] を選択します。

5. [IPAM account] (IPAM アカウント) に、AWS アカウント ID を入力します。IPAM 管理者は AWS Organizations のメンバーアカウントである必要があります。
6. [Save changes] (変更の保存) をクリックします。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

- AWS CLI を使用して IPAM 管理者アカウントを委任するには、コマンド enable-ipam-organization-admin-account を使用します。

Organizations メンバーアカウントを IPAM アカウントとして委任すると、組織内のすべてのメンバーアカウントに、サービスにリンクされた IAM ロールが IPAM によって自動的に作成されます。IPAM は、各メンバーアカウント内のサービスにリンクされた IAM ロールを継承して、リソースとその CIDR を検出し、それらを IPAM に統合することによって、これらのアカウントの IP アドレスの使用状況を監視します。組織単位に関係なく、すべてのメンバーアカウント内のリソースは、IPAM によって検出可能になります。例えば、VPC を作成したメンバーアカウントがある場合、IPAM コンソールの [Resources] (リソース) セクションに VPC とその CIDR が表示されます。

> **Important**
>
> IPAM 管理者を委任した AWS Organizations 管理アカウントの役割はこれで完了です。IPAM を引き続き使用するには、IPAM 管理者アカウントで Amazon VPC IPAM にログインし、IPAM を作成する必要があります。

IPAM を組織外のアカウントに統合する

このセクションでは、IPAM を AWS 組織外のアカウントに統合する方法を説明します。このセクションの手順を完了するには、「IPAM を AWS Organizations 内のアカウントと統合する」の手順を既に完了しており、IPAM アカウントが委任済みである必要があります。

IPAM を組織外の AWS アカウントに統合することで、以下を実行することが可能になります。

- 単一の IPAM アカウントから組織外の IP アドレスを管理する。
- 他の AWS Organizations 内にある他の AWS アカウントがホストするサードパーティサービスと IPAM プールを共有する。

IPAM を組織外の AWS アカウントに統合すると、他の組織の目的のアカウントと IPAM プールを直接共有できます。

内容

考慮事項と制限

このセクションには、IPAM を組織外のアカウントに統合する場合の考慮事項と制限事項が記載されています。

- リソース検出を別のアカウントと共有する場合に交換されるデータは、IP アドレスとアカウントステータスのモニタリングデータのみです。このデータは、get-ipam-discovered-resource-cidrs および get-ipam-discovered-accounts CLI コマンド、または GetIpamDiscoveredResourceCidrs および GetIpamDiscoveredAccounts API を使用して、共有する前に表示できます。組織全体のリソースを監視するリソース検出で、組織データ (組織内の組織単位の名前など) が共有されることはありません。
- リソース検出を作成すると、リソース検出が所有者アカウントで表示できるすべてのリソースを監視します。所有者アカウントが、複数の独自の顧客のためにリソースを作成するサードパーティーサービス AWS アカウントである場合、これらのリソースはリソース検出によって検出されます。サードパーティー AWS アカウントがエンドユーザー AWS アカウントとリソース検出を共有する場合、このエンドユーザーは、サードパーティー AWS サービスの他の顧客のリソースに対する可視性を得ます。そのため、サードパーティ AWS サービスは、リソース検出の作成と共有を慎重に行う、または顧客ごとに別個の AWS アカウントを使用する必要があります。

プロセスの概要

このセクションでは、IPAM を組織外の AWS アカウントに統合する方法を説明します。このセクションは、本ガイドの他のセクションに含まれるトピックを参照します。このページを表示した状態のまま、新しいウィンドウで以下のリンク先のトピックを開くことで、このページに戻ってガイダンスを確認できるようにしてください。

IPAM を組織外の AWS アカウントに統合する場合のプロセスには、4 つの AWS アカウントが関与します。

- プライマリ組織の所有者 – 組織 1 の AWS Organizations 管理アカウント。

- プライマリ組織の IPAM アカウント – 組織 1 の IPAM 委任管理者アカウント。
- セカンダリ組織の所有者 – 組織 2 の AWS Organizations 管理アカウント。
- セカンダリ組織の管理者アカウント – 組織 2 の IPAM 委任管理者アカウント。

ステップ

1. プライマリ組織の所有者が、その組織のメンバーをプライマリ組織の IPAM アカウントとして委任します (「IPAM を AWS Organizations 内のアカウントと統合する」を参照)。
2. プライマリ組織の IPAM アカウントが IPAM を作成します (「IPAM を作成する」を参照)。
3. セカンダリ組織の所有者が、その組織のメンバーをセカンダリ組織の管理者アカウントとして委任します (「IPAM を AWS Organizations 内のアカウントと統合する」を参照)。
4. セカンダリ組織の管理者アカウントがリソース検出を作成し、AWS RAM を使用してリソース検出をプライマリ組織の IPAM アカウントと共有します (「別の IPAM と統合するリソース検出を作成する」および「リソース検出を別の AWS アカウントと共有する」を参照)。リソース検出は、プライマリ組織の IPAM と同じホームリージョン内で作成される必要があります。
5. プライマリ組織の IPAM アカウントが、AWS RAM を使用してリソース共有招待を承諾します (「AWS RAM ユーザーガイド」の「リソース共有招待の承諾と拒否」を参照)。
6. プライマリ組織の IPAM アカウントが、リソース検出をその IPAM に関連付けます (「リソース検出を IPAM に関連付ける」を参照)。
7. プライマリ組織の IPAM アカウントが、セカンダリ組織内のアカウントが作成した IPAM リソースを管理および/または監視できるようになります。
8. (オプション) プライマリ組織の IPAM アカウントが、セカンダリ組織内のメンバーアカウントと IPAM プールを共有します (「AWS RAM を使用して IPAM プールを共有する」を参照)。
9. (オプション) プライマリ組織の IPAM アカウントがセカンダリ組織内のリソースの検出を停止したい場合は、リソース検出と IPAM との関連付けを解除できます (「リソース検出の関連付けを解除する」を参照)。
10. (オプション) セカンダリ組織の管理者アカウントがプライマリ組織の IPAM への参加を停止したい場合は、リソース検出の共有を解除 (「AWS RAM ユーザーガイド」の「AWS RAM のリソース共有を更新する」を参照) するか、リソース検出を削除できます (「リソース検出を削除する」を参照)。

IPAM を 1 つのアカウントで使用する

IPAM を AWS Organizations 内のアカウントと統合する を選択しない場合、1 つの AWS アカウントで IPAM を使用できます。

次のセクションで IPAM を作成した場合、AWS Identity and Access Management (IAM) の Amazon VPC IPAM サービスに対して、サービスリンクロールが自動的に作成されます。

サービスにリンクされたロールは、AWS サービスがユーザーに代わって他の AWS サービスにアクセスすることを許可する IAM ロールの一種です。これにより、特定の AWS サービスが必要なアクションを実行するために必要な許可を自動的に作成して管理し、これらのサービスの設定と管理を合理化することで、許可管理プロセスが簡素化されます。

IPAM は、サービスにリンクされたロールを使用して、組織の EC2 ネットワークリソースに関連付けられた CIDR のモニタリングを行い、メトリクスを保存します。サービスリンクロールの詳細と IPAM での使用方法については、IPAM のサービスリンクロールを参照してください。

> **Important**
>
> 1 つの AWS アカウントで IPAM を使用する場合は、IPAM の作成に使用する AWS アカウントに、`iam:CreateServiceLinkedRole` アクションを許可するポリシーがアタッチされている IAM ロールを使用していることを確認する必要があります。IPAM を作成した場合、AWSServiceRoleForIPAM サービスにリンクされたロールが自動的に作成されます。IAM ユーザーポリシーの管理の詳細については、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。

AWS アカウントの 1 つに、IPAM サービスにリンクされたロールを作成できる許可が付与された後、IPAM を作成する に移動します。

IPAM を作成する

このセクションの手順に従って IPAM を作成します。IPAM 管理者を委任した場合は、これらの手順を IPAM アカウントで実行する必要があります。

> **Important**
>
> IPAM を作成すると、IPAM がソースアカウントから IPAM 委任アカウントにデータをレプリケートすることを許可するように求められます。IPAM を AWS Organizations と統合するに

は、IPAM には、アカウント間 (メンバーアカウントから委任された IPAM メンバーアカウントへ) および AWS リージョン間 (運用リージョンから IPAM のホームリージョンへ) で、リソースおよび IP の使用の詳細をレプリケートするためのアクセス許可が必要です。単一アカウントの IPAM ユーザーの場合、IPAM には、運用リージョン全体のリソースおよび IP の使用の詳細を IPAM のホームリージョンにレプリケートするためのアクセス許可が必要です。

IPAM を作成するときは、IPAM が IP アドレス CIDR の管理を許可されている AWS リージョンを選択します。これらの AWS リージョンは運用リージョンと呼ばれます。IPAM は、運用リージョンとして選択された AWS リージョンのリソースのみを検出および監視します。IPAM では、選択した運用リージョン外のデータは保存されません。

以下の階層例は、IPAM の作成時に割り当てる AWS リージョンが、後で作成するプールで使用できるリージョンにどのような影響を与えるかを示しています。

- AWS リージョン 1 と AWS リージョン 2 で運用されている IPAM
  - プライベートスコープ
    - トップレベルの IPAM プール
      - AWS リージョン 2 のリージョン IPAM プール
        - 開発プール
          - AWSリージョン 2 での VPC の割り当て

作成できる IPAM は 1 つだけです。IPAM に関連したクォータの引き上げについて詳しくは、IPAM のクォータ を参照してください。

AWS Management Console

IPAM を作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. AWS マネジメントコンソールで、IPAM を作成する AWS リージョンを選択します。オペレーションの主要リージョンに IPAM を作成します。
3. サービスホームページで [IPAM の作成] を選択します。
4. [Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account] (Amazon VPC IP Address Manager がソースアカウントから IPAM

委任アカウントにデータをレプリケートするのを許可する) を選択します。このオプションを選択しないと、IPAM を作成できません。

5. IPAM 階層を選択します。各利用枠で利用できる機能と利用枠に関連するコストの詳細については、「Amazon VPC の料金」で [IPAM] タブを参照してください。
6. [運用リージョン] で、この IPAM がリソースを管理および検出できる AWS リージョンを選択します。IPAM を作成している AWS リージョンは、デフォルトで運用リージョンの 1 つとして選択されています。たとえば、この IPAM を AWS リージョン `us-east-1` で作成しているが、`us-west-2` の VPC に CIDR を提供するリージョン IPAM プールを後で作成したい場合は、ここで `us-west-2` を選択します。運用リージョンを忘れた場合は、後で戻って IPAM の設定を編集できます。

> **Note**
>
> 無料利用枠で IP アドレス管理を作成する場合、IP アドレス管理用に複数の運用地域を選択できますが、運用リージョン全体で利用できる IP アドレス管理機能はPublic IP Insightsだけです。無料利用枠の他の機能 (BYOIP など) を IP アドレス管理の対象リージョン全体で使用することはできません。IPAM のホームリージョンを通じてのみ使用できます。運用リージョン全体ですべての IP アドレス管理機能を使用するには、アドバンスト枠で [IP アドレス管理] を作成してください。

7. [プライベート IPv6 GUA CIDR] を有効にするか選びます。このオプションの詳細については、「プライベート IPv6 GUA CIDR のプロビジョニングを有効にする」を参照してください。
8. [計測モード] を有効にするか選びます。このオプションの詳細については、「コスト配分を有効にする」を参照してください。
9. [Create IPAM] (IPAM を作成) を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

以下の AWS CLI コマンドを使用して IPAM に関連する詳細を作成、変更、および表示します。

1. IPAM を作成します。create-ipam
2. 作成した IPAM を表示します。describe-ipams
3. 自動的に作成されるスコープを表示します。describe-ipam-scopes

4. 既存の IPAM を変更します。modify-ipam

これらの手順を完了すると、IPAM によって次の処理が行われます。

- IPAM を作成しました。コンソールの左側のナビゲーションペインで [IPAM] を選択すると、IPAM および現在選択されている運用リージョンが表示されます。
- プライベートスコープとパブリックスコープを 1 つ作成しました。スコープを表示するには、ナビゲーションペインで[Scopes] (スコープ) を選択します。スコープの詳細については、IPAM の仕組み を参照してください。

IP アドレスのプロビジョニング計画

IPAM プールを使用して IP アドレスのプロビジョニングを計画するには、このセクションのステップに従います。IPAM アカウントを設定した場合は、そのアカウントでこれらの手順を完了する必要があります。プールの作成プロセスは、パブリックスコープとプライベートスコープで異なります。このセクションでは、プライベートスコープにリージョンプールを作成する手順について説明します。BYOIP および BYOASN のチュートリアルについては、「チュートリアル」を参照してください。

> **Important**
>
> AWS アカウント間で IPAM プールを使用するには、IPAM と AWS Organizations を統合する必要があります。統合しないと一部の機能が正常に動作しない場合があります。(詳しくは、「IPAM を AWS Organizations 内のアカウントと統合する」を参照してください。)

IPAM では、プールは連続した IP アドレス範囲 (CIDR) の集合です。プールを使用すると、ルーティングとセキュリティのニーズに応じて IP アドレスを整理できます。IPAM リージョン外の AWS リージョンにもプールを作成することができます。例えば、開発アプリケーションと本番アプリケーションで別々のルーティングとセキュリティのニーズがある場合は、それぞれにプールを作成できます。

このセクションの最初のステップでは、最上位プールを作成します。次に、最上位プール内にリージョンプールを作成します。リージョンプール内では、本番環境や開発環境プールなど、必要に応じて追加のプールを作成できます。デフォルトでは、深さ 10 までプールを作成できます。IPAM クォータに関する詳細については、IPAM のクォータを参照してください。

> **Note**
>
> プロビジョンおよび割り当てという用語は、このユーザーガイドと IPAM コンソール全体で使用されています。プロビジョンは、CIDR を IPAM プールに追加するときに使用されます。割り当ては、IPAM プールの CIDR をリソースに関連付けるときに使用されます。

次に、このセクションのステップによって作成するプール構造の階層の例を示します。

- AWS リージョン 1 と AWS リージョン 2 で運用されている IPAM
  - プライベートスコープ
    - 最上位プール
      - AWS リージョン 1 のリージョンプール
        - 開発プール
          - VPC の割り当て

この構造は、IPAM の使用方法の例として役立ちますが、組織のニーズに合わせて IPAM を使用できます。ベストプラクティスについては、「Amazon VPC IP Address Manager Best Practices」(Amazon VPC IP Address Manager のベストプラクティス) を参照してください。

1 つの IPAM プールを作成する場合は、トップレベル IPv4 プールを作成する のステップを完了してから IPAM プールから CIDR を割り当てる に進みます。

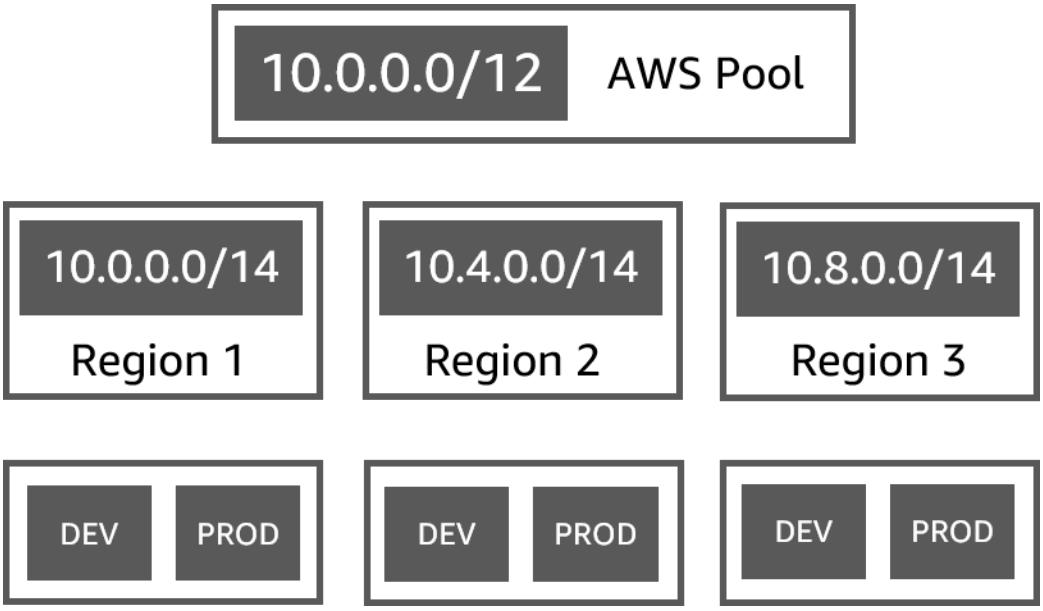
内容

IPAM プール計画の例

IPAM は、組織のニーズに合わせて使用できます。このセクションでは、IP アドレスを整理する方法の例を示します。

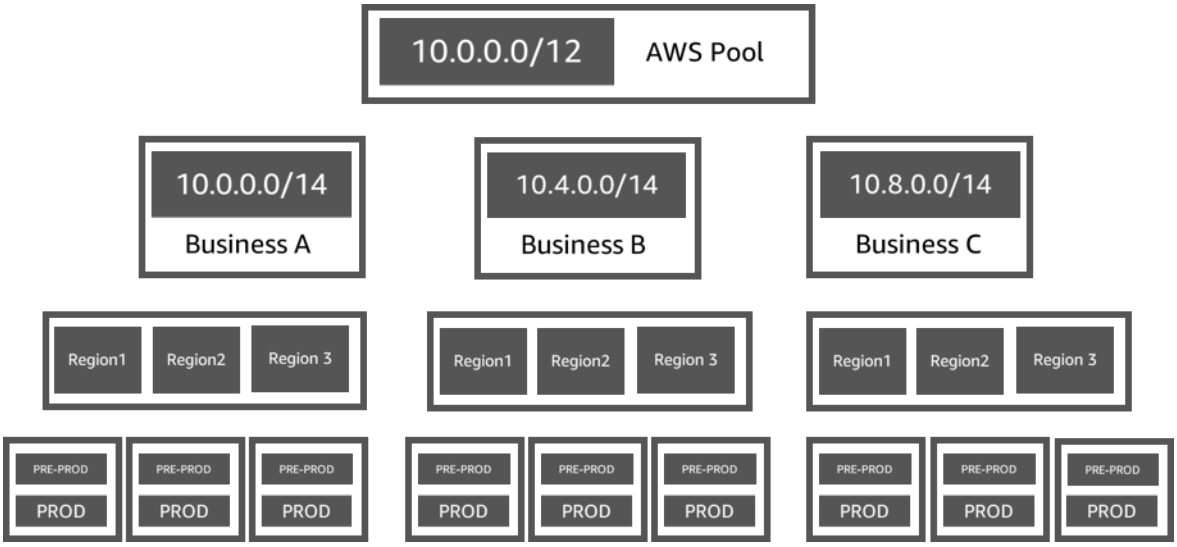
複数の AWS リージョン内の IPv4 プール

次の例に示しているのは、最上位プール内の複数のAWS リージョンの IPAM プールの階層です。各 AWS リージョンプールには、2 つの IPAM 開発プールがあります。1 つは開発リソース用のプールで、もう 1 つは生産リソース用のプールです。



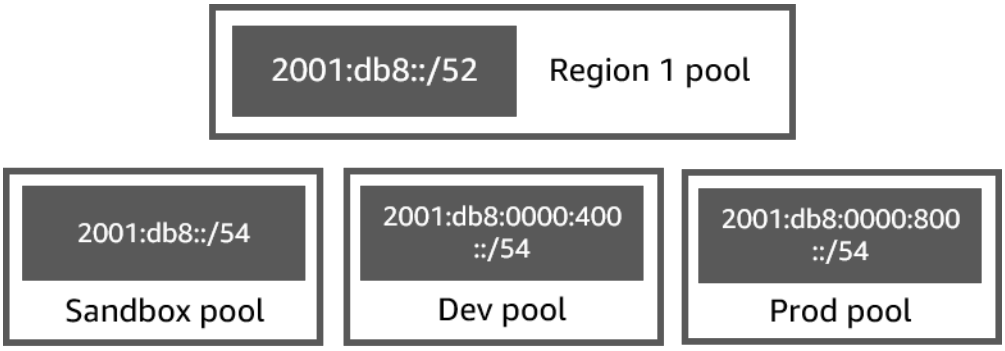
複数の事業部門用の IPv4 プール

次の例に示しているのは、最上位プール内の複数の事業部門用の IPAM プール階層です。各事業部門の各プールには、3 つの AWS リージョンプールが含まれています。各リージョンプールには、2 つの IPAM 開発プールがあります。1 つは本番稼働前リソース用のプールでもう 1 つは本番稼働リソース用のプールです。



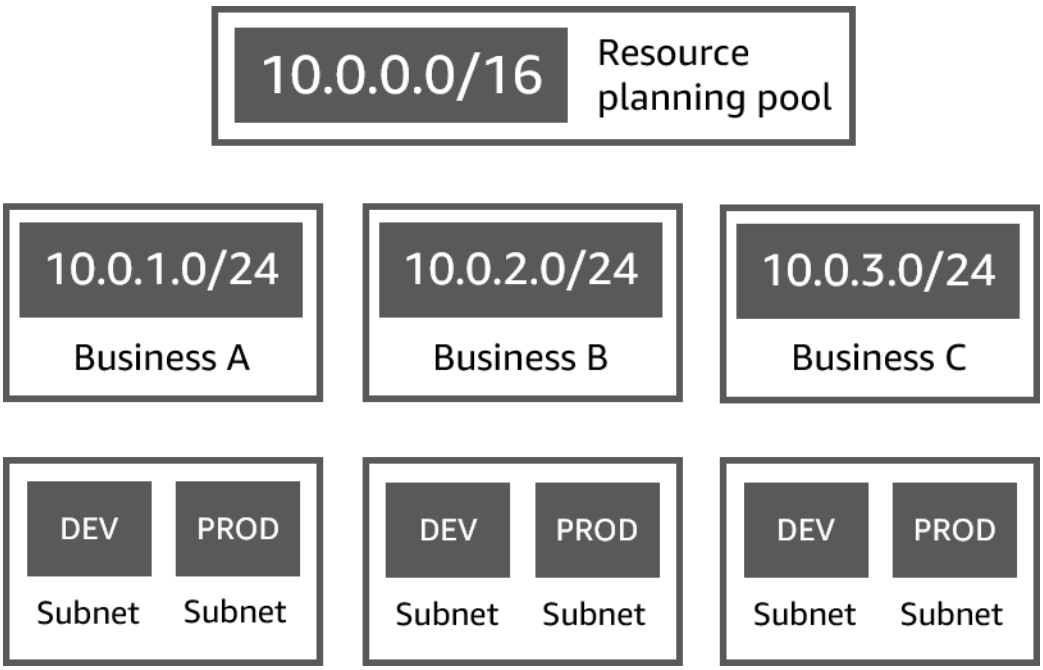
AWS リージョン内の IPv6 プール

以下は、リージョンプール内にある複数の事業部門用の IPAM IPv6 プール階層の例です。各リージョンプール内には、サンドボックスリソース用のプール、開発リソース用のプール、および本番環境リソース用のプールの 3 つの IPAM プールがあります。



複数の事業ライン用のサブネットプール

次の例は、複数の事業ライン用と dev/prod サブネットプール用のリソース計画プール階層を示しています。IPAM を使用したサブネット IP アドレス空間計画の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。



IPv4 プールを作成する

このセクションの手順に従って、IPv4 IPAM プール階層を作成します。

次の例は、このガイドの手順で作成できるプール構造の階層を示しています。このセクションでは、次のような IPv4 IPAM プール階層を作成します。

- AWS リージョン 1 と AWS リージョン 2 で運用されている IPAM
  - プライベートスコープ
    - 最上位プール (10.0.0.0/8)
      - AWS リージョン 2 のリージョンプール (10.0.0.0/16)
        - 開発プール (10.0.0.0/24)
          - VPC の割り当て (10.0.0.0/25)

前述の例で使用されている CIDR は例にすぎません。これらは、トップレベルプール内の各プールがトップレベル CIDR の一部でプロビジョニングされていることを示しています。

内容

トップレベル IPv4 プールを作成する

このセクションの手順に従って、IPv4 トップレベル IPAM プールを作成します。プールを作成するときは、使用するプールの CIDR をプロビジョニングします。次に、そのスペースを割り振りに割り当てます。割り振りとは、IPAM プールから別のIPAM プール、またはリソースへの CIDR の割り当てです。

次の例は、このガイドの手順で作成できるプール構造の階層を示しています。このステップでは、トップレベル IPAM プールを作成します。

- AWS リージョン 1 とAWS リージョン 2 で運用されている IPAM
  - プライベートスコープ
    - 最上位プール (10.0.0.0/8)
      - AWS リージョン 1 のリージョンプール (10.0.0.0/16)
        - 実稼働以外の VPC の開発プール (10.0.0.0/24)
          - VPC の割り当て (10.0.0.0/25)

前述の例で使用されている CIDR は例にすぎません。これらは、トップレベルプール内の各プールがトップレベル CIDR の一部でプロビジョニングされていることを示しています。

IPAM プールの作成時に、IPAM プール内で行われる割り当てのルールを設定できます。

割り当てルールを使用すると、以下を設定できます。

- このプールの CIDR 範囲内で検出された場合、CIDR を IPAM プールに自動的にインポートするかどうか
- プール内の割り当てに必要なネットマスクの長さ
- プール内のリソースに必要なタグ
- プール内のリソースに必要なロケール ロケールは、IPAM プールを割り当てることができるようにする AWS リージョンです。

割り当てルールは、リソースが準拠しているか非準拠かを決定します。コンプライアンスの詳細については、リソースごとに CIDR の使用状況をモニタリングする を参照してください。

> **Important**
>
> 割り当てルールには表示されない追加の暗黙ルールがあります。リソースが、AWS Resource Access Manager (RAM) の共有リソースである IPAM プール内にある場合、リソース所有者は AWS RAM でプリンシパルとして設定されている必要があります。RAM でプールを共有する方法の詳細については、AWS RAM を使用して IPAM プールを共有する を参照してください。

次の例は、割り当てルールを使用して IPAM プールへのアクセスを制御する方法を示しています。

Example

ルーティングとセキュリティのニーズに基づいてプールを作成する場合、特定のリソースのみがプールを使用できるようにしたい場合があります。このような場合、このプールからの CIDR を必要とするリソースには、割り当てルールタグの要件に一致するタグが必要であることを示す割り当てルールを設定できます。例えば、prod タグのある VPC のみが IPAM プールから CIDR を取得できることを示す割り当てルールを設定できます。また、このプールから割り当てられる CIDR は /24 以下であることを示すルールを設定することもできます。この場合、このプールから /24 より大きい CIDR を使用してリソースを作成すると、プールの割り当てルールに違反し、作成が失敗します。CIDR が /24 より大きい既存のリソースには、非準拠としてフラグが付けられます。

> **Important**
>
> このトピックでは、AWS 提供の IP アドレス範囲を使用してトップレベル IPv4 プールを作成する方法を説明します。独自の IPv4 アドレス範囲を AWS に持ち込む (BYOIP) には、前提条件があります。詳細については、「チュートリアル: IP アドレスを IPAM に移行する」を参照してください。

AWS Management Console

プールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. [プールを作成] を選択します。
4. [IPAM スコープ] で、使用するプライベートスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。

   デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。プライベートスコープのプールは IPv4 プールにする必要があります。パブリックスコープのプールは、IPv4 プールまたは IPv6 プールにすることができます。パブリックスコープは、すべてのパブリック空間を対象としています。
5. (オプション) プールの[名前タグ]とプールの説明を入力します。
6. [ソース] で [IPAM 範囲] を選択します。
7. [アドレスファミリー] には [IPv4] を選択します。
8. [リソース計画] で、[範囲内のIP 空間計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
9. [Locale] (ロケール) で、[None] (なし) を選択します。リージョンプールにロケールを設定します。

   ロケールは、この IPAM プールを割り当てることができるようにする AWS リージョンです。例えば、VPC の CIDR は、VPC のリージョンとロケールを共有する IPAM プールからしか割り当てることができません。プールのロケールを選択したら、変更はできないことに注意してください。停止が原因で IPAM のホームリージョンが使用できなくなり、プールの

ロケールが IPAM のホームリージョンと異なる場合でも、プールを使用して IP アドレスを割り当てることができます。

10. (オプション) CIDR なしでプールを作成することもできますが、プールに CIDR をプロビジョニングするまでは、割り振りにそのプールを使用することはできません。CIDR をプロビジョニングするには、[新しい CIDR を追加] を選択します。プールにプロビジョニングする IPv4 CIDR を入力します。独自の IPv4 または IPv6 IP アドレス範囲を AWS に持ち込む (BYOIP) 場合は、前提条件があります。詳細については、「チュートリアル: IP アドレスを IPAM に移行する」を参照してください。
11. このプールのオプションの割り当てルールを選択します。

- [Automatically import discovered resources] (検出されたリソースを自動的にインポートする): このオプションは、[Locale] (ロケール) が [None] (なし) に設定されている場合は選択できません。選択すると、IPAM はこのプールの CIDR 範囲内のリソースを継続的に検索し、自動的に割り当てとして IPAM にインポートします。次の点に注意してください。
  - インポートを成功させるためには、これらのリソースに割り当てられる CIDR がすでに他のリソースに割り当られていてはなりません。
  - IPAM は、プールの割り当てルールに準拠しているかどうかに関係なく CIDR をインポートするため、リソースがインポートされ、その後、非準拠としてマークされる可能性があります。
  - 重複する複数の CIDR を IPAM が検出した場合、IPAM は最大 CIDR のみをインポートします。
  - 一致する CIDR を持つ複数の CIDR を IPAM が検出した場合、IPAM はそれらのうちの 1 つだけをランダムにインポートします。

> ⚠ Warning
>
> - IPAM を作成したら、VPC の作成時、IPAM で割り当てられた CIDR ブロックオプションを選択します。これを選択しなければ、VPC 用に選択した CIDR が IPAM CIDR の割り当てと重複する可能性があります。
> - VPC が IPAM プールにすでに割り当てられている場合、CIDR が重複している VPC を自動的にインポートすることはできません。例えば、10.0.0.0/26 の CIDR が IPAM プールに割り当てられた VPC がある場合、10.0.0.0/23 の CIDR (10.0.0.0/26 CIDR がカバーされる) の VPC はインポートできません。
> - 既存の VPC CIDR 割り当てが IPAM に自動でインポートされるまでにはしばらく時間がかかります。

- [Minimum netmask length] (ネットマスクの最小長): この IPAM プール内の CIDR 割り当てが準拠するために必要なネットマスクの最小長と、プールから割り当てられる最大サイズの CIDR ブロック。ネットマスクの最小長は、ネットマスクの最大長より小さくなければなりません。IPv4 アドレスに使用できるネットマスクの長さは 0 ~ 32 です。IPv6 アドレスに使用できるネットマスクの長さは 0 ~ 128 です。
- [Default netmask length] (デフォルトのネットマスク長): このプールに追加される割り当てのデフォルトのネットマスク長。例えば、このプールにプロビジョニングされる CIDR が **`10.0.0.0/8`** である場合に **16** をここに入力すると、このプールでの新しい割り振りは、いずれもデフォルトで /16 のネットマスク長になります。
- [Maximum netmask length] (ネットマスクの最大長): このプールの CIDR 割り当てに必要なネットマスクの最大長。この値は、プールから割り当てられる最小サイズの CIDR ブロックを示します。
- [Tagging requirements] (タグ付け要件): プールからスペースを割り当てるためにリソースに必要なタグ。スペースを割り当てた後にリソースのタグが変更された場合、またはプールで割り当てのタグ付けルールが変更された場合、リソースは非準拠としてマークされることがあります。
- [ロケール]: このプールの CIDR を使用するリソースに必要なロケール。このロケールが設定されていない、自動的にインポートされたリソースは、非準拠としてマークされます。プールに自動的にインポートされないリソースは、このロケールでない限り、プールからスペースを割り当てることはできません。

> **Note**
>
> 割り当てルールは、そのプール内のマネージドリソースにのみ適用されます。このルールは、プール内のサブプールのリソースには適用されません。

12. (オプション) プールのタグを選択します。
13. [プールを作成] を選択します。
14. 「リージョン IPv4 プールを作成する」を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

IPAM にトップレベルプールを作成または編集するには、次の AWS CLI コマンドを使用します。

1. プールを作成する: create-ipam-pool
2. 作成後にプールを編集して、割り当てルールを変更する: modify-ipam-pool。

リージョン IPv4 プールを作成する

このセクションの手順に従って、トップレベルプール内にリージョンプールを作成します。トップレベルプールのみが必要で、追加のリージョンプールおよび開発プールが不要な場合は、IPAM プールから CIDR を割り当てる に進んでください。

> **Note**
>
> プールの作成プロセスは、パブリックスコープとプライベートスコープで異なります。このセクションでは、プライベートスコープにリージョンプールを作成する手順について説明します。BYOIP および BYOASN のチュートリアルについては、「チュートリアル」を参照してください。

次の例は、このガイドの手順に従って作成するプール構造の階層を示しています。このステップでは、リージョン IPAM プールを作成します。

- AWS リージョン 1 とAWS リージョン 2 で運用されている IPAM
  - プライベートスコープ
    - 最上位プール (10.0.0.0/8)
      - AWS リージョン 1 のリージョンプール (10.0.0.0/16)
        - 実稼働以外の VPC の開発プール (10.0.0.0/24)
          - VPC の割り当て (10.0.0.0/25)

前述の例で使用されている CIDR は例にすぎません。これらは、トップレベルプール内の各プールがトップレベル CIDR の一部でプロビジョニングされていることを示しています。

AWS Management Console

トップレベルプール内にリージョンプールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。

2. ナビゲーションペインで、[プール] を選択します。
3. [プールを作成] を選択します。
4. [IPAM スコープ] で、最上位プールの作成時に使用したものと同じスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
5. (オプション) プールの[名前タグ]とプールの説明を入力します。
6. [ソース] で [IPAM プール] を選択します。次に、前のセクションで作成した最上位プールを選択します。
7. パブリックスコープでこのプールを作成する場合は、[アドレスファミリー] のオプションが表示されます。[IPv4] を選択します。
8. 「リソース計画」で、[h範囲内のプラン IP スペース] は選択したままにします。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
9. プールのロケールを選択します。ロケールを選択すると、プールとそのプールから割り当てられるリソースの間にクロスリージョン依存関係がないことが保証されます。使用可能なオプションは、IPAM を作成したときに選択した運用リージョンによって提供されます。

   ロケールは、この IPAM プールを割り当てることができるようにする AWS リージョンです。例えば、VPC の CIDR は、VPC のリージョンとロケールを共有する IPAM プールからしか割り当てることができません。プールのロケールを選択したら、変更はできないことに注意してください。停止が原因で IPAM のホームリージョンが使用できなくなり、プールのロケールが IPAM のホームリージョンと異なる場合でも、プールを使用して IP アドレスを割り当てることができます。

   > **Note**
   >
   > 無料利用枠でプールを作成する場合、IPAM のホームリージョンに一致するロケールのみを選択できます。すべてのロケールで IP アドレス管理機能を使用するには、アドバンスト枠にアップグレードしてください。

10. パブリックスコープでこのプールを作成する場合は、[サービス] のオプションが表示されます。[EC2 (EIP/VPC)] を選択します。選択したサービスによって、CIDR がアドバタイズ可能になる AWS サービスが決定します。現在、唯一の選択肢は EC2 (EIP/VPC) であり、このプールから割り当てられた CIDR は、Amazon EC2 サービス (Elastic IP アドレスの場合) と Amazon VPC サービス (VPC に関連付けられている CIDR の場合) に対してアドバタイズできるようになります。

11. (オプション) プールにプロビジョニングする CIDR を選択します。CIDR なしでプールを作成することもできますが、CIDR をプロビジョニングするまで、そのプールを割り当てに使用することはできません。プールを編集することで、いつでも CIDR をプールに追加できます。
12. ここでは、トップレベルプールを作成したときと同じ割り当てルールオプションがあります。プールの作成時に使用できるオプションの説明については、トップレベル IPv4 プールを作成する を参照してください。リージョンプールの割り当てルールは、トップレベルプールから継承されません。ここでルールを適用しない場合、プールに割り当てルールは設定されません。
13. (オプション) プールのタグを選択します。
14. プールの設定が完了したら、[Create pool] (プールの作成) を選択します。
15. 「開発 IPv4 プールを作成する」を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

IPAM にリージョンプールを作成するには、次の AWS CLI コマンドを使用します。

1. プールを作成するスコープの ID を取得します: describe-ipam-scopes
2. プールを作成するプールの ID を取得します: describe-ipam-pools。
3. プールを作成します: create-ipam-pool
4. 新しいプールを表示する: describe-ipam-pools

必要に応じて、これらのステップを繰り返して、トップレベルプール内に追加のプールを作成します。

開発 IPv4 プールを作成する

このセクションの手順に従って、リージョンプール内に開発プールを作成します。トップレベルとリージョンのプールのみが必要で、開発プールが不要な場合は、IPAM プールから CIDR を割り当てる に進んでください。

次の例は、このガイドの手順で作成できるプール構造の階層を示しています。このステップでは、開発 IPAM プールを作成します。

- AWS リージョン 1 と AWS リージョン 2 で運用されている IPAM
  - プライベートスコープ
    - 最上位プール (10.0.0.0/8)
      - AWS リージョン 1 のリージョンプール (10.0.0.0/16)
        - 実稼働以外の VPC の開発プール (10.0.0.0/24)
          - VPC の割り当て (10.0.1.0/25)

前述の例で使用されている CIDR は例にすぎません。これらは、トップレベルプール内の各プールがトップレベル CIDR の一部でプロビジョニングされていることを示しています。

AWS Management Console

リージョンプール内に開発プールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. [プールを作成] を選択します。
4. [IPAM スコープ] で、最上位とリージョンのプールの作成時に使用したものと同じスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
5. (オプション) プールの[名前タグ]とプールの説明を入力します。
6. [ソース] で [IPAM プール] を選択します。次に、リージョンプールを選択します。
7. 「リソース計画」で、[範囲内の IP スペース計画] は選択した範囲内のままにします。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
8. (オプション) プールにプロビジョニングする CIDR を選択します。プロビジョニングできるのは、トップレベルのプールにプロビジョニングされた CIDR のみです。CIDR なしでプールを作成することもできますが、CIDR をプロビジョニングするまで、そのプールを割り当てに使用することはできません。プールを編集することで、いつでも CIDR をプールに追加できます。
9. ここでは、トップレベルとリージョンのプールを作成したときと同じ割り当てルールオプションがあります。プールの作成時に使用できるオプションの説明については、トップレベル IPv4 プールを作成する を参照してください。プールの割り当てルールは、階層内のその上位プールから継承されません。ここでルールを適用しない場合、プールに割り当てルールは設定されません。

10. (オプション) プールのタグを選択します。
11. プールの設定が完了したら、[Create pool] (プールの作成) を選択します。
12. 「IPAM プールから CIDR を割り当てる」を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

IPAM にリージョンプールを作成するには、次の AWS CLI コマンドを使用します。

1. プールを作成するスコープの ID を取得します: describe-ipam-scopes
2. プールを作成するプールの ID を取得します: describe-ipam-pools。
3. プールを作成します: create-ipam-pool
4. 新しいプールを表示します: describe-ipam-pools

必要に応じて、これらの手順を繰り返して、リージョンプール内に追加の開発プールを作成します。

IPAM で IPv6 アドレスプールを作成する

AWS は、EC2、VPC、S3 など、多くのサービスで IPv6 接続を提供し、ユーザーが IPv6 のアドレス空間の増加とセキュリティ機能の強化を使用できるようにします。IPv6 は、IPv4 のこの基本的な制限を解決するように設計されました。128 ビットのアドレス空間に移行することで、IPv6 は一意の IP アドレスを大量に提供します。この大規模なアドレス拡張により、スマートフォンや IoT デバイスからクラウドインフラストラクチャまで、コネクテッドテクノロジーの利用を継続的に広めることができます。

さらに、IPAM を使用して、VPC 作成に連続する IPv6 CIDR を使用していることを確認することもできます。連続して割り当てられた CIDR とは、続いて割り当てられた CIDR を意味します。これにより、セキュリティルールとネットワークルールを簡素化できます。IPv6 CIDR は、アクセスコントロールリスト、ルートテーブル、セキュリティグループ、ファイアウォールなどのネットワークおよびセキュリティ構造全体で 1 つのエントリに集約できます。

このセクションの手順に従って、IPAM IPv6 プール階層を作成します。プールを作成するときは、プールが使用する CIDR をプロビジョニングできます。プールは、その CIDR 内のスペースをプール内の割り当てに対して割り当てます。割り当てとは、IPAM プールから別のリソースまたは IPAM プールへの CIDR 割り当てです。

> **Note**
>
> AWS ではパブリック IPv6 アドレス指定とプライベート IPv6 アドレス指定の両方が利用できます。AWS では、AWS からインターネットでアドバタイズされるパブリック IP アドレスは考慮されますが、プライベート IP アドレスは考慮されず、AWS からインターネットでアドバタイズできません。プライベートネットワークで IPv6 をサポートし、このアドレスからインターネットにトラフィックをルーティングするつもりがない場合は、プライベートスコープに IPv6 プールを作成します。パブリックおよびプライベート IPv6 アドレスの詳細については、「Amazon VPC ユーザーガイド」の「IPv6 アドレス」を参照してください。

次の例は、このガイドの手順で作成できるプール構造の階層を示しています。このセクションでは、次のような IPv6 IPAM プール階層を作成します。

- AWS リージョン 1 と AWS リージョン 2 で運用されている IPAM
  - スコープ
    - AWS リージョン 1 内のリージョンプール (2001:db8::/52)
      - 開発プール (2001:db8::/54)
        - VPC の割り振り (2001:db8::/56)

前述の例で使用されている CIDR は例にすぎません。これらは、リージョンプール内の各開発プールがリージョン CIDR の一部を使用してプロビジョニングされていることを示しています。

内容

IPAM でリージョンレベルの IPv6 アドレスプールを作成する

このセクションの手順に従って、IPv6 リージョン IPAM プールを作成します。Amazon 提供の IPv6 CIDR ブロックをプールにプロビジョニングするときは、ロケール (AWS リージョン) が選択されたプールにブロックをプロビジョニングする必要があります。プールを作成するときは、プールが使用する CIDR をプロビジョニングするか、CIDR を後ほど追加することができます。次に、そのスペースを割り振りに割り当てます。割り振りとは、IPAM プールから別のIPAM プール、またはリソースへの CIDR の割り当てです。

次の例は、このガイドの手順で作成できるプール構造の階層を示しています。このステップでは、IPv6 リージョン IPAM プールを作成します。

- AWS リージョン 1 と AWS リージョン 2 で運用されている IPAM
  - スコープ
    - AWS リージョン 1 内のリージョンプール (2001:db8::/52)
      - 開発プール (2001:db8::/54)
        - VPC の割り振り (2001:db8::/56)

前述の例で使用されている CIDR は例にすぎません。これらは、IPv6 リージョンプール内の各プールが IPv6 リージョン CIDR の一部でプロビジョニングされていることを示しています。

IPAM プールの作成時に、IPAM プール内で行われる割り当てのルールを設定できます。

割り当てルールを使用すると、以下を設定できます。

- プール内の割り当てに必要なネットマスクの長さ
- プール内のリソースに必要なタグ
- プール内のリソースに必要なロケール ロケールは、IPAM プールを割り当てることができるようにする AWS リージョンです。

割り当てルールは、リソースが準拠しているか非準拠かを決定します。コンプライアンスの詳細については、リソースごとに CIDR の使用状況をモニタリングする を参照してください。

> **Note**
>
> 割り当てルールには表示されない追加の暗黙ルールがあります。リソースが、AWS Resource Access Manager (RAM) の共有リソースである IPAM プール内にある場合、リソース所有者は AWS RAM でプリンシパルとして設定されている必要があります。RAM でプールを共有する方法の詳細については、AWS RAM を使用して IPAM プールを共有する を参照してください。

次の例は、割り当てルールを使用して IPAM プールへのアクセスを制御する方法を示しています。

Example

ルーティングとセキュリティのニーズに基づいてプールを作成する場合、特定のリソースのみがプールを使用できるようにしたい場合があります。このような場合、このプールからの CIDR を必要とするリソースには、割り当てルールタグの要件に一致するタグが必要であることを示す割り当てルールを設定できます。例えば、prod タグのある VPC のみが IPAM プールから CIDR を取得できることを示す割り当てルールを設定できます。

> **Note**
>
> - このトピックでは、AWS 提供の IP アドレス範囲、またはプライベート IPv6 範囲を使用して、IPv6 リージョンプールを作成する方法について説明します。独自のパブリック IPv4 または IPv6 IP アドレス範囲を AWS に持ち込む (BYOIP) 場合は、前提条件があります。詳細については、「チュートリアル: IP アドレスを IPAM に移行する」を参照してください。
> - プライベートスコープに IPv6 プールを作成する場合は、プライベート IPv6 GUA または ULA 範囲を使用できます。プライベート GUA 範囲を使用するには、まず IPAM で対象オプションを有効にする必要があります (「プライベート IPv6 GUA CIDR のプロビジョニングを有効にする」を参照)。

AWS Management Console

プールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. [プールを作成] を選択します。
4. [IPAM スコープ] で、プライベートスコープまたはパブリックスコープを選択します。プライベートネットワークで IPv6 をサポートし、そのアドレスからインターネットにトラフィックをルーティングするつもりがない場合は、プライベートスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。

   デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。
5. (オプション) プールの[名前タグ]とプールの説明を入力します。
6. [ソース] で [IPAM スコープ] を選択します。

7. [アドレスファミリー] には [IPv6] を選択します。パブリックスコープにこのプールを作成する場合、このプール内のすべての CIDR がパブリックにアドバタイズ可能になります。
8. [リソース計画] で、[範囲内のIP スペースの計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
9. プールの [ロケール] を選択します。Amazon 提供の IPv6 CIDR ブロックをプールにプロビジョニングする場合、ロケール (AWS リージョン) が選択されたプールにブロックをプロビジョニングする必要があります。ロケールを選択すると、プールとそのプールから割り当てられるリソースの間にクロスリージョン依存関係がないことが保証されます。利用可能なオプションは、IPAM を作成したときに選択した運用リージョンによって提供されます。運用リージョンはいつでも追加することができます。

   ロケールは、この IPAM プールを割り当てることができるようにする AWS リージョンです。例えば、VPC の CIDR は、VPC のリージョンとロケールを共有する IPAM プールからしか割り当てることができません。プールのロケールを選択したら、変更はできないことに注意してください。停止が原因で IPAM のホームリージョンが使用できなくなり、プールのロケールが IPAM のホームリージョンと異なる場合でも、プールを使用して IP アドレスを割り当てることができます。

   > **Note**
   >
   > 無料利用枠でプールを作成する場合、IPAM のホームリージョンに一致するロケールのみを選択できます。すべてのロケールで IP アドレス管理機能を使用するには、アドバンスト枠にアップグレードしてください。
10. (任意) パブリックスコープに IPv6 プールを作成する場合、[サービス] で [EC2 (EIP/VPC)] を選択します。選択したサービスによって、CIDR がアドバタイズ可能になる AWS サービスが決定します。現在、唯一の選択肢は EC2 (EIP/VPC) であり、このプールから割り当てられた CIDR は、Amazon EC2 サービス (Elastic IP アドレスの場合) と Amazon VPC サービス (VPC に関連付けられている CIDR の場合) に対してアドバタイズできるようになります。
11. (任意) [パブリック IP ソース] オプションでパブリックスコープに IPv6 プールを作成する場合は、[Amazon 所有] を選択して、AWS によりこのプールの IPv6 アドレス範囲が提供されるようにします。このページの冒頭に記載されているとおり、このトピックでは AWS 提供の IP アドレス範囲を使用して IPv6 リージョンプールを作成する方法を説明します。独自の IPv4 または IPv6 アドレス範囲を AWS に持ち込む (BYOIP) には、前提条件があります。詳細については、「チュートリアル: IP アドレスを IPAM に移行する」を参照してください。

12. (オプション) CIDR なしでプールを作成することもできますが、プールに CIDR をプロビジョニングするまでは、割り振りにそのプールを使用することはできません。CIDR をプロビジョニングするには、次のいずれかを実行します。

    - [Amazon が所有するパブリック IP ソース] を使用してパブリックスコープに IPv6 プールを作成する場合、CIDR をプロビジョニングするために、[プロビジョニングする CIDR] で [Amazon が所有する CIDR を追加] を選択し、CIDR のネットマスクサイズを /40 ~ /52 から選択します。ドロップダウンメニューでネットマスク長を選択するときは、ネットマスク長に加えて、そのネットマスクが表す /56 CIDR の数も表示されます。デフォルトで、リージョンプールには Amazon 提供の IPv6 CIDR ブロックを 1 つ追加できます。デフォルト制限の引き上げに関する情報については、「IPAM のクォータ」を参照してください。
    - プライベートスコープに IPv6 プールを作成する場合は、プライベート IPv6 GUA または ULA 範囲を使用できます。
        - プライベート IPv6 アドレス指定に関する重要な詳細については、「Amazon VPC ユーザーガイド」の「プライベート IPv6 アドレス」を参照してください。
        - プライベート IPv6 ULA 範囲を使用するには、[プロビジョニングする CIDR] で、[ネットマスクで ULA CIDR を追加] を選択してネットマスクサイズを選択するか、[プライベート IPv6 CIDR を入力] を選択して ULA 範囲を入力します。有効な IPv6 ULA スペースは、Amazon の予約範囲 fd00::/16 と重複しない fd00::/8 より下のいずれかです。
        - プライベート IPv6 GUA 範囲を使用するには、まず IPAM で 対象オプションを有効にする必要があります (「プライベート IPv6 GUA CIDR のプロビジョニングを有効にする」を参照)。プライベート IPv6 GUA CIDR を有効にしたら、[プライベート IPv6 CIDR を入力] で IPv6 GUA を入力します。

13. このプールのオプションの割り振りルールを選択します。

    - [Minimum netmask length] (ネットマスクの最小長): この IPAM プール内の CIDR 割り当てが準拠するために必要なネットマスクの最小長と、プールから割り当てられる最大サイズの CIDR ブロック。ネットマスクの最小長は、ネットマスクの最大長より小さくなければなりません。IPv6 アドレスに使用できるネットマスクの長さは 0 ~ 128 です。
    - [Default netmask length] (デフォルトのネットマスク長): このプールに追加される割り当てのデフォルトのネットマスク長。例えば、このプールにプロビジョニングされる CIDR が `2001:db8::/52` である場合に 56 をここに入力すると、このプールでの新しい割り振りは、いずれもデフォルトで /56 のネットマスク長になります。
    - [Maximum netmask length] (ネットマスクの最大長): このプールの CIDR 割り当てに必要なネットマスクの最大長。この値は、プールから割り当てられる最小サイズの CIDR ブロッ

クを示します。例えば、ここに /56 を入力する場合、このプールからの CIDR に割り振ることができる最小ネットマスク長は /56 です。

- [タグ付け要件]: プールからスペースを割り当てるためにリソースに必要なタグ。スペースを割り当てた後にリソースのタグが変更された場合、またはプールで割り当てのタグ付けルールが変更された場合、リソースは非準拠としてマークされることがあります。
- [ロケール]: このプールの CIDR を使用するリソースに必要なロケール。このロケールが設定されていない、自動的にインポートされたリソースは、非準拠としてマークされます。プールに自動的にインポートされないリソースは、このロケールでない限り、プールからスペースを割り当てることはできません。

14. (オプション) プールのタグを選択します。
15. [プールを作成] を選択します。
16. 「IPAM で開発 IPv6 アドレスプールを作成する」を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

IPAM 内で IPv6 リージョンプールを作成、または編集するには、以下の AWS CLI コマンドを使用します。

1. プライベート IPv6 GUA CIDR のプロビジョニングを有効にする場合は、modify-ipam で IPAM を変更し、対象オプションを `enable-private-gua` に入れます。詳細については、「プライベート IPv6 GUA CIDR のプロビジョニングを有効にする」を参照してください。
2. create-ipam-pool でプールを作成します。
3. プールに CIDR をプロビジョニングします: provision-ipam-pool-cidr。
4. 作成後にプールを編集して、割り当てルールを変更する: modify-ipam-pool。

IPAM で開発 IPv6 アドレスプールを作成する

このセクションの手順に従って、IPv6 リージョンプール内に開発プールを作成します。リージョンプールのみが必要で、開発プールは必要ない場合は、「IPAM プールから CIDR を割り当てる」に進んでください。

次の例は、このガイドの手順で作成できるプール構造の階層を示しています。このステップでは、開発 IPAM プールを作成します。

- AWS リージョン 1 と AWS リージョン 2 で運用されている IPAM
  - 範囲
    - AWS リージョン 1 内のリージョンプール (2001:db8::/52)
      - 開発プール (2001:db8::/54)
        - VPC の割り振り (2001:db8::/56)

前述の例で使用されている CIDR は例にすぎません。これらは、トップレベルプール内の各プールがトップレベル CIDR の一部でプロビジョニングされていることを示しています。

AWS Management Console

IPv6 リージョンプール内に開発プールを作成する

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. [プールを作成] を選択します。
4. [IPAM スコープ] で、スコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
5. (オプション) プールの[名前タグ]とプールの説明を入力します。
6. [ソース] で [IPAM プール] を選択します。次に、[ソースプール] で、IPv6 リージョンプールを選択します。
7. 「リソース計画」で、「範囲内のプラン IP スペース」は選択したままにします。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
8. (オプション) プールにプロビジョニングする CIDR を選択します。プロビジョニングできるのは、トップレベルのプールにプロビジョニングされた CIDR のみです。CIDR なしでプールを作成することもできますが、CIDR をプロビジョニングするまで、そのプールを割り当てに使用することはできません。プールを編集することで、いつでも CIDR をプールに追加できます。
9. ここには、IPv6 プールを作成したときと同じ割り振りルールオプションがあります。プールの作成時に使用できるオプションの説明については、IPAM でリージョンレベルの IPv6 アドレスプールを作成する を参照してください。プールの割り当てルールは、階層内のその上位プールから継承されません。ここでルールを適用しない場合、プールに割り当てルールは設定されません。

10. (オプション) プールのタグを選択します。
11. プールの設定が完了したら、[Create pool] (プールの作成) を選択します。
12. 「IPAM プールから CIDR を割り当てる」を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

IPAM に IPv6 リージョンプールを作成するには、以下の AWS CLI コマンドを使用します。

1. プールを作成するスコープの ID を取得します: describe-ipam-scopes
2. プールを作成するプールの ID を取得します: describe-ipam-pools。
3. プールを作成します: create-ipam-pool
4. 新しいプールを表示します: describe-ipam-pools

必要に応じてこれらの手順を繰り返し、IPv6 リージョンプール内に追加の開発プールを作成します。

IPAM プールから CIDR を割り当てる

IPAM の重要な機能の 1 つは、IP アドレス空間を割り当てて管理する機能です。VPC を作成する際には、その VPC で使用できる IP アドレスの範囲を定義する IP アドレス CIDR ブロックを指定する必要があります。IPAM は、IP アドレスインベントリ全体のグローバルビューを提供することでこのプロセスを簡素化し、複数の VPC で IP プレフィックスを戦略的に割り当てて再利用できるようにします。

このアドレス空間の割り当ては、ルーティングの競合や接続の問題を引き起こす可能性のある、重複する IP 範囲がないようにするために重要です。また、IPAM を使用すると、将来の VPC 拡張のために IP アドレス空間を予約できるため、後で複雑なリナンバリングを行う必要がなくなります。

このセクションの手順に従って、IPAM プールからリソースに CIDR を割り当てます。

> **Note**
>
> プロビジョンおよび割り当てという用語は、このユーザーガイドと IPAM コンソール全体で使用されています。プロビジョンは、CIDR を IPAM プールに追加するときに使用されます。割り当ては、IPAM プールの CIDR をリソースに関連付けるときに使用されます。

以下の方法で IPAM プールから CIDR を割り当てることができます。

- Amazon VPC など、IPAM と統合されている AWS サービスを使用し、CIDR に IPAM プールを使用するオプションを選択します。IPAM によって、プール内に割り当てが自動的に作成されます。
- IPAM プール内の CIDR を手動で割り当て、後で Amazon VPC などの IPAM と統合された AWS サービスで使用できるように予約します。

このセクションでは、IPAM と統合された AWS サービスを使用して IPAM プール CIDR をプロビジョニングする方法と、IP アドレス空間を手動で予約する方法の両方のオプションについて説明します。

内容

IPAM プール CIDR を使用する VPC を作成する

Amazon Virtual Private Cloud (Amazon VPC) を使用すると、論理的に隔離されている定義済みの仮想ネットワーク内で AWS リソースを起動できます。仮想ネットワークは、お客様自身のデータセンターで運用されていた従来のネットワークによく似ていますが、AWS のスケーラブルなインフラストラクチャを使用できるというメリットがあります。

仮想プライベートクラウド (VPC) は、AWS アカウント専用の仮想ネットワークです。VPC は、AWS クラウドの他の仮想ネットワークから論理的に切り離されています。VPC の IP アドレス範囲を指定して、サブネットを追加し、ゲートウェイを追加して、セキュリティグループを関連付けます。

Amazon VPC ユーザーガイドの「VPC を作成する」の手順に従います。VPC の CIDR を選択する手順に達すると、IPAM プールから CIDR を使用するオプションが表示されます。

VPC を作成するときに IPAM プールを使用するオプションを選択した場合、AWS によって IPAM プールに CIDR が割り当てられます。IPAM コンソールの [コンテンツ] ペインでプールを選択し、そのプールの [リソース] タブを表示して、IPAM での割り当てを表示できます。

> **Note**
>
> VPC の作成など、AWS CLI の使用方法の詳細については、Amazon VPC IP Address Manager のチュートリアル セクションを参照してください。

CIDR をプールに手動で割り当てて IP アドレス空間を予約する

このセクションの手順に従って、CIDR をプールに手動で割り当てます。これは、後で使用するために、IPAM プール内の CIDR を予約するために行う場合があります。IPAM プール内のスペースを予約して、オンプレミスネットワークを表すこともできます。IPAM がその予約を管理し、オンプレミス IP スペースと重複する CIDR がある場合はそれを示します。

AWS Management Console

CIDR を手動で割り当てるには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Pools] (プール) を選択します。
3. デフォルトでは、デフォルトのプライベートスコープが選択されます。デフォルトのプライベートスコープを使用しない場合は、コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、「IPAM の仕組み」を参照してください。
4. コンテンツペインで、[pool] (プール) を選択します。
5. [Actions] (アクション)、[Create custom allocation] (カスタム割り当ての作成) を順に選択します。
6. 割り当てる特定の CIDR (IPv4 には `10.0.0.0/24`、IPv6 には `2001:db8::/52` など) を追加するか、ネットマスクの長さ (IPv4 には `/24`、IPv6 には `/52` など) だけを選択してサイズ別に CIDR 追加するかを選択します。
7. [Allocate] (割り当て) を選択します。
8. IPAM で割り当てを表示するには、ナビゲーションペインで、[Pools] (プール) を選択し、プールの [割り当て] タブを表示します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

以下の AWS CLI コマンドを使用して、CIDR をプールに手動で割り当てます。

1. 割り当てを作成する IPAM プールの ID を取得します: describe-ipam-pools。
2. 割り当ての作成: allocate-ipam-pool-cidr。
3. 割り当ての表示: get-ipam-pool-allocations。

手動で割り当てられた CIDR をリリースするには、「割り当ての解除」を参照してください。

IPAM で IP アドレス空間を管理する

このセクションのタスクはオプションです。このセクションは、IPAM の操作に関連する手順をまとめたものであることに留意してください。手順はアルファベット順に並べられています。

IPAM アカウントを委任している場合は、このセクションのタスクを完了するには、タスクは IPAM 管理者が完了する必要があります。

IPAM で IP アドレス空間を管理するには、このセクションのステップに従います。

内容

IPAM を使用してプレフィックスリストの更新を自動化する

マネージドプレフィックスリストは、個々の IP アドレスを指定する代わりに、セキュリティグループルールとルートテーブルで参照できる CIDR ブロックのセットです。例えば、10.1.0.0/16、10.2.0.0/16、および 10.3.0.0/16 用に個別のセキュリティグループルールを作成する代わりに、3 つの CIDR すべてを含む 1 つのプレフィックスリストを作成し、1 つのルールで参照できます。

ユーザー定義変数には次の 2 種類があります。

- カスタマーマネージドプレフィックスリスト: 定義および管理する IP 範囲
- AWS マネージドプレフィックスリスト: AWS サービス (S3 や CloudFront など) の IP 範囲

この IPAM 機能は、CIDR エントリをネットワークの変更と同期させることで、カスタマーマネージドプレフィックスリストの管理を自動化します。

これによって解決される問題

自動化しないと、ネットワークチームはインフラストラクチャが変更されたときにプレフィックスリストを手動で更新し、環境とリージョン全体で一貫したプレフィックスリストを維持するのにかなりの時間を費やします。

IPAM は、プレフィックスリストを自動的に入力するルールを作成できるようにすることで、この問題を解決します。IPAM プールから CIDR を参照するか、実際の AWS リソースに基づいてルールを作成するという 2 つのアプローチを使用できます。作成するルールは、例えば、「env=prod とタグ付けされたすべての VPC を含める」、「us-east-1 のすべてのサブネットを含める」、「アカウント 123456789 が所有するすべての Elastic IP アドレスを含める」などです。これらのリソースを追加または削除すると、IPAM は CIDR を使用して自動的にプレフィックスリストを更新します。

仕組み

プレフィックスリストに含める IP アドレスを IPAM に指示するルールを作成します。例えば、「env=prod とタグ付けされたすべての VPC CIDR を含める」などです。本番稼働用 VPC を追加または削除すると、IPAM は自動的にプレフィックスリストを更新します。

どのような場合に使用するか

- セキュリティグループ: 「env=prod とタグ付けされたすべての VPC を含める」というルールを作成すると、新しく本番稼働用 VPC を追加するときに、これらはセキュリティグループルールで自動的に許可されます
- マルチリージョン: 複数のリージョンに同じ IPAM ルールをデプロイすると、CIDR エントリを手動でコピーしなくても同じプレフィックスリストが保持されます
- 動的インフラストラクチャ: VPC またはサブネットを作成/削除すると、手動で更新することなく、その CIDR がプレフィックスリストに自動的に追加/削除されます

前提条件

開始する前に、以下を確認してください。

- アドバンスト階層が有効になっている IPAM
- カスタマーマネージドプレフィックスリスト (またはセットアップ時に作成)
- IPAM および EC2 プレフィックスリストオペレーションの IAM アクセス許可

セットアップステップ

ステップ 1: IPAM プレフィックスリストリゾルバーを作成する

IPAM プレフィックスリストリゾルバーを作成して、プレフィックスリストに含める CIDR を定義します。

AWS Management Console

IPAM プレフィックスリストリゾルバーを作成するには

1. IPAM コンソールを開きます。
2. ナビゲーションペインで、[プレフィックスリストリゾルバー] を選択します。
3. [プレフィックスリストリゾルバーを作成] をクリックします。
4. [ステップ 1: リゾルバーの詳細を設定する] で、以下を選択します。
   - IPAM: IPAM インスタンス
   - アドレスファミリー: IPv4 または IPv6

- 名前タグ - オプション: わかりやすい名前
- 説明 - オプション: 説明
- タグ: リソースタグ

5. [次へ] を選択します。
6. [ステップ 2: ルールを設定する] で、[ルールを追加] を選択します。最大 99 個のルールを追加できます。

> **Important**
>
> CIDR 選択ルールなしでプレフィックスリストリゾルバーを作成できますが、ルールを追加するまで空のバージョン (CIDR が含まれていない) が生成されます。

7. 以下のルールタイプのいずれかを選択します。

- 静的 CIDR: 変更されない CIDR の固定リスト (リージョン間でレプリケートされる手動リストなど)
- IPAM プール CIDR: CIDR (IPAM 本番稼働用プールからのすべての CIDR など)

  このオプションを選択する場合は、以下を選択する必要があります。

  - IPAM スコープ: リソースを検索する IPAM スコープを選択します。
  - 条件:
    - プロパティ
      - IPAM プール ID: リソースを含む IPAM プールを選択する
      - CIDR (10.24.34.0/23 など)
    - オペレーション: Equals/Not equals
    - 値: 条件に一致する値
- スコープリソース CIDR: IPAM スコープ内の VPC、サブネット、EIP などの AWS リソースからの CIDR

  このオプションを選択する場合は、以下を選択する必要があります。

  - IPAM スコープ: リソースを検索する IPAM スコープを選択します。
  - リソースタイプ: VPC やサブネットなどのリソースを選択します。
  - 条件:
    - プロパティ:

- リソース ID: リソースの一意の ID (vpc-1234567890abcdef0 など)
- リソース所有者 (111122223333 など)
- リソースリージョン (us-east-1 など)
- リソースタグ (キー: name、値: dev-vpc-1 など)
- CIDR (10.24.34.0/23 など)

- オペレーション: Equals/Not equals
- 値: 条件に一致する値

8. [次へ] を選択します。
9. [検証と作成] を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

次の AWS CLI コマンドを使用して、IPAM プレフィックスリストリゾルバーを作成します。

- create-ipam-prefix-list-resolver コマンドを使用して、返されたリゾルバー ID をステップ 2 のために保存します。

ステップ 2: プレフィックスリストに接続するリゾルバーターゲットを作成する

リゾルバーターゲットを作成して、リゾルバーを既存のプレフィックスリストにリンクします。ステップ 1 で返されたリゾルバー ID を使用します。

AWS Management Console

IPAM プレフィックスリストリゾルバーターゲットを作成するには

1. IPAM コンソールで、[プレフィックスリストリゾルバー] を選択します。
2. ステップ 1 で作成したリゾルバーを選択します。
3. [リゾルバーの詳細] ページで、[ターゲット] タブを選択します。
4. [ターゲットの作成] を選択します。
5. 次のようにターゲットを設定します。

- リージョン: 既存のマネージドプレフィックスリストが存在するリージョン、または作成するリージョンを選択します。
- プレフィックスリスト: 既存のマネージドプレフィックスリストを選択するか、新しいプレフィックスリストを作成します。

6. [必要なバージョン] で、次のいずれかを選択します。

- 常に最新バージョンを追跡する: プレフィックスリストを手動による介入なしでインフラストラクチャの変更に対して最新の状態に保つ場合は、これを選択して自動更新します。
- 特定のバージョンを追跡する: 予測可能で制御された更新が必要で、プレフィックスリストの変更を手動で承認する場合は、これを選択して安定性を確保します。

7. [ターゲットの作成] を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

次の AWS CLI コマンドを使用して、IPAM プレフィックスリストリゾルバーターゲットを作成します。

- ステップ 1 のリゾルバー ID と既存のプレフィックスリスト ID を使用して create-ipam-prefix-list-resolver-target コマンドを使用します。

IPAM は、ルールに基づいてプレフィックスリストを自動的に更新するようになりました。プレフィックスリストには、条件に一致する CIDR が入力されます。

ステップ 3: バージョンと同期をモニタリングする

プレフィックスリストリゾルバーとターゲットを作成すると、プレフィックスリストリゾルバーはルールに基づいて CIDR バージョンを生成し、ターゲットはそれらの CIDR をリゾルバーから特定のマネージドプレフィックスリストに同期します。各バージョンは、その時点でルールに一致した CIDR のスナップショットです。バージョン番号は、インフラストラクチャの変更によって CIDR リストが変更されるたびに増加します。

バージョンの例:

初期状態 (バージョン 1)

本番環境:

- vpc-prod-web (10.1.0.0/16) - env=prod タグ付き
- vpc-prod-db (10.2.0.0/16) - env=prod タグ付き

リゾルバールール: env=prod とタグ付けされたすべての VPC を含める

バージョン 1 CIDR: 10.1.0.0/16、10.2.0.0/16

インフラストラクチャの変更 (バージョン 2)

新しい VPC が追加されました。

- vpc-prod-api (10.3.0.0/16) - env=prod タグ付き

IPAM は変更を自動的に検出し、新しいバージョンを作成します。

バージョン 2 CIDR: 10.1.0.0/16、10.2.0.0/16、10.3.0.0/16

このセクションでは、AWS コンソールまたは AWS CLI でバージョンの作成をモニタリングし、AWS CLI で同期の成功をモニタリングする方法について説明します。

また、バージョンとプレフィックスのリストサイズの制限内に収まるように CIDR 選択ルールを再評価して調整する必要がある可能性があるため、障害メトリクスに CloudWatch アラームを設定することをお勧めします。IPAM プレフィックスリストに関連する CloudWatch メトリクスのリストについては、「IPAM プレフィックスリストリゾルバーメトリクス」を参照してください。

AWS Management Console

作成されたバージョンを表示し、ターゲット同期をモニタリングするには

1. IPAM コンソールで、[プレフィックスリストリゾルバー] を選択します。
2. ステップ 1 で作成したリゾルバーを選択します。
3. [ドメインの詳細] ページで、[バージョン] タブを選択します。ここでは、リゾルバーによって作成されたすべてのバージョンと、そのバージョンのすべての CIDR が表示されます。
4. リゾルバーの詳細ページで、[モニタリング] タブを選択します。このビューでは、IPAM プレフィックスリストリゾルバーメトリクス はグラフ形式で表示されます。
   - プレフィックスリストリゾルバーのバージョン作成の成功
   - プレフィックスリストリゾルバーのバージョン作成の失敗

5. [モニタリング] タブから、[プレフィックスリストリゾルバーのバージョン作成のアラームを作成] を選択して CloudWatch アラームを設定することもできます。アラームがメトリクスに部分的に設定された状態で CloudWatch コンソールが表示されます。アラームの作成を完了する方法の詳細については、「Amazon CloudWatch ユーザーガイド」の「静的しきい値に基づいて CloudWatch アラームを作成する」を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

バージョンと同期をモニタリングするには、次の AWS CLI コマンドを使用します。

1. get-ipam-prefix-list-resolver-version-entries コマンドを使用して、リゾルバーによって作成された最新バージョンを表示します。
2. describe-ipam-prefix-list-resolver-targets コマンドを使用して、リゾルバーのターゲット同期ステータスをモニタリングします。

モニタリングコマンドには、以下が表示されます。

- state - 現在の同期状態 (create-complete、modify-complete など)
- lastSyncedVersion - 最後に正常に同期されたバージョン
- desiredVersion - 同期先のターゲットバージョン
- stateMessage - 同期が失敗した場合のエラーの詳細

> **Important**
>
> ロールバックのワークフローをサポートするために、IPAM はターゲットごとに以前の 10 個のプレフィックスリストリゾルバーバージョンのコピーを保持します。このしきい値よりも古く、7 日間参照されていないバージョンは削除されます。

ステップ 4: (オプション) IPAM プレフィックスリストの同期を有効および無効にする

マネージドプレフィックスリストが IPAM プレフィックスリストターゲットとして設定されていて、IPAM プレフィックスリストリゾルバーターゲットにアクセスするためのアクセス許可を必要と

せずにプレフィックスリストを変更する場合は、マネージドプレフィックスリストを変更し、IPAM プレフィックスリストリゾルバーとの同期を無効にすることができます。無効にすると、プレフィックスリスト CIDR は自動的に更新されず、変更を加えることができます。有効にすると、プレフィックスリスト CIDR は、関連付けられたリゾルバーの CIDR 選択ルールに基づいて自動的に更新されます。

VPC CIDR のモニタリング状態を変更する

このセクションのステップに従って、VPC CIDR のモニタリング状態を変更します。IPAM で VPC を管理またはモニタリングせず、VPC に割り当てられた CIDR を使用できるようにする場合は、VPC CIDR をモニタリング対象から無視対象に変更できます。IPAM で VPC CIDR を管理またはモニタリングする場合は、VPC CIDR を無視対象からモニタリング対象に変更できます。

> **Note**
>
> - パブリックスコープ内の VPC CIDR を無視することはできません。
> - CIDR を無視した場合でも、引き続き CIDR 内のアクティブ IP アドレスに対して課金されます。詳細については、「IPAM の料金」を参照してください。
> - CIDR を無視した場合でも、CIDR 内の IP アドレスの履歴を表示できます。詳細については、「IP アドレス履歴の表示」を参照してください。

VPC CIDR のモニタリング状態を、モニタリング対象または無視対象に変更できます。

- モニタリング対象: VPC CIDR は IPAM によって検出され、他の CIDR との重複および割り当てルールへの準拠についてモニタリングされています。
- 無視: VPC CIDR はモニタリングの対象外として選択されています。無視された VPC CIDR は、他の CIDR との重複または割り当てルールへの準拠について評価されません。VPC CIDR が無視されるように選択されると、IPAM プールから VPC CIDR に割り当てられた空間はすべてプールに返され、VPC CIDR が自動インポートを介して再度インポートされることはありません (自動インポートの割り当てルールがプールで設定されている場合)。

AWS Management Console

VPC に割り当てられた CIDR のモニタリングステータスを変更するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。

2. ナビゲーションペインで、[リソース] を選択します。
3. コンテンツペインの上部にあるドロップダウンメニューから、使用するプライベートスコープを選択します。
4. コンテンツペインで、VPC を選択して VPC の詳細を表示します。
5. [VPC CIDR] で、VPC に割り当てられた CIDR のいずれかを選択し、[アクション]、[無視としてマーク] または [無視のマークを解除] の順に選択します。
6. [無視対象としてマーク] または [無視対象のマークを解除する] を選択します。

Command line

次の AWS CLI コマンドを使用して、VPC CIDR のモニタリング状態を変更します。

1. スコープ ID を取得します。describe-ipam-scopes
2. VPC CIDR の現在のモニタリング状態を表示します。get-ipam-resource-cidrs
3. VPC CIDR の状態を変更します。modify-ipam-resource-cidr
4. VPC CIDR の新しいモニタリング状態を表示します。get-ipam-resource-cidrs

追加のスコープを作成する

このセクションの手順に従って、追加のスコープを作成します。

スコープは IPAM 内の最上位のコンテナです。IPAM を作成すると、IPAM によって 2 つのデフォルトスコープが作成されます。各スコープは、単一のネットワークの IP スペースを表します。プライベートスコープは、すべてのプライベート空間を対象としています。パブリックスコープは、すべてのパブリック空間を対象としています。スコープを使用すると、IP アドレスの重複や競合を引き起こすことなく、接続されていない複数のネットワーク間で IP アドレスを再利用できます。

IPAM を作成すると、デフォルトのスコープ (1 つのプライベートスコープと 1 つのパブリックスコープ) が自動的に作成されます。プライベートスコープは追加で作成できます。パブリックスコープは追加で作成できません。

複数の切断されたプライベートネットワークをサポートする必要がある場合は、追加のプライベートスコープを作成できます。追加のプライベートスコープを使用すると、プールを作成し、同じ IP 領域を使用するリソースを管理できます。

> **Important**
>
> IPAM がプライベート IPv4 CIDR または プライベート IPv6 CIDR を持つリソースを検出すると、リソース CIDR はデフォルトのプライベートスコープにインポートされ、作成した追加のプライベートスコープに表示されなくなります。CIDR は、デフォルトのプライベートスコープから別のプライベートスコープに移動できます。詳細については、「スコープ間で VPC CIDR を移動する」を参照してください。

AWS Management Console

追加のプライベートスコープを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Scopes] (スコープ) を選択します。
3. [Create scope] (スコープの作成) を選択します。
4. スコープを追加する IPAM を選択します。
5. スコープの説明を追加します。
6. [Create scope] (スコープの作成) を選択します。
7. IPAM でスコープを表示するには、ナビゲーションペインで[Scopes] (スコープ) を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

以下の AWS CLI コマンドを使用して追加のプライベートスコープを作成します。

1. 現在のスコープを表示する: describe-ipam-scopes
2. 新しいプライベートスコープを作成する: create-ipam-scope
3. 現在のスコープを表示して新しいスコープを表示する: describe-ipam-scopes

IPAM を削除する

不要になった場合、IP アドレス管理を再構築する必要がある場合、または新しい IPAM 設定で新しく開始する場合は、IPAM を削除することが考えられます。IPAM の削除は、IP アドレス管理を簡素化したり、変化するビジネス要件や運用要件に対応したりするのに役立ちます。

IPAM を削除するには、このセクションのステップに従います。既存の IPAM を削除するのではなく、デフォルトの IPAM 数を増やす方法については、IPAM のクォータ を参照してください。

> **Note**
>
> IPAM を削除すると、CIDR の履歴データを含む、IPAM に関連付けられているモニタリング対象データがすべて削除されます。

AWS Management Console

IPAM を削除するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[IPAMs] (IPAM) を選択します。
3. コンテンツペインで、IPAM を選択します。
4. [Actions] (アクション) で、[Delete IPAM] (IPAM の削除) を選択します。
5. 次のいずれかを行います。
   - [Cascade delete] (カスケード削除) を選択して、IPAM、プライベートスコープ、プライベートスコープ内のプール、およびプライベートスコープ内のプールのすべての割り振りを削除します。パブリックスコープにプールがある場合、このオプションを使用して IPAM を削除することはできません。このオプションを使用する場合、IPAM は次の処理を実行します。
     - プライベートスコープのプール内の VPC リソース (VPC など) に割り振られた CIDR の割り振りを解除します。

> **Note**
>
> このオプションを有効にしても、VPC リソースは削除されません。リソースに関連付けられた CIDR は IPAM プールから割り振られなくなりますが、CIDR 自体は変更されません。

- プライベートスコープ内の IPAM プールにプロビジョニングされたすべての IPv4 CIDR のプロビジョニングを解除します。
- プライベートスコープ内のすべての IPAM プールを削除します。
- IPAM 内のデフォルトではないすべてのプライベートスコープを削除します。
- デフォルトのパブリックスコープとプライベートスコープ、および IPAM を削除します。

- [Cascade delete] (カスケード削除) のチェックボックスを選択しない場合は、IPAM を削除する前に、次の手順を実行する必要があります。
  - IPAM プール内の割り当てを解放します。詳細については、「割り当ての解除」を参照してください。
  - IPAM 内のプールにプロビジョニングされた CIDR のプロビジョニングを解除します。詳細については、「プールから CIDR のプロビジョニングを解除するには」を参照してください。
  - デフォルト以外の追加のスコープを削除します。詳細については、「スコープを削除する」を参照してください。
  - IPAM プールを削除します。詳細については、「プールを削除する」を参照してください。

6. **delete** と入力し、[削除] を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

IPAM を削除するには、次の AWS CLI コマンドを使用します。

1. 現在の IPAM を表示する: describe-ipams
2. IPAM を削除する: delete-ipam
3. 更新された IPAM を表示する: describe-ipams

新しい IPAM を作成する方法については、IPAM を作成する を参照してください。

プールを削除する

AWS の IPAM プールは、特定の AWS 環境または組織内で割り当ておよび管理できる、定義された IP アドレスの範囲を表します。プールは、IP アドレス空間の整理、自動 IP アドレス管理の有効化、クラウドインフラストラクチャ全体での IP アドレスガバナンスポリシーの強制に使用されます。

IPAM プールを削除して、未使用または不要な IP アドレス空間を削除し、他の目的で再利用することもできます。IP アドレスプール内に割り当てがある場合、IP アドレスプールを削除することはできません。プールを削除するには、最初に割り当てを解放し、プールから CIDR のプロビジョニングを解除するには を行う必要があります。

IPAM プールを削除するには、このセクションのステップに従います。

AWS Management Console

プールを削除するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Pools] (プール) を選択します。
3. コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組み を参照してください。
4. コンテンツペインで、CIDR を削除するプールを選択します。
5. [Actions] (アクション) で、[Delete Pool] (プールの削除) を選択します。
6. **`delete`** と入力し、[Delete] (削除) を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

プールを削除するには、次の AWS CLI コマンドを使用します。

1. プールを表示し、IPAM プール ID を取得する: describe-ipam-pools
2. プールを削除する: delete-ipam-pool
3. プールを表示する: describe-ipam-pools

新しいプールを作成する方法については、トップレベル IPv4 プールを作成する を参照してください。

スコープを削除する

ネットワークを再構築したり、リージョンを統合したり、IP アドレスの割り当てを調整したりするなど、IPAM スコープが意図する目的にそぐわなくなった場合は、IPAM スコープを削除することが考えられます。未使用のスコープの削除は、IPAM 設定を効率化したり、AWS 内の IP アドレス管理を最適化したりするのに役立ちます。

> **Note**
>
> 次のいずれかに該当する場合には、スコープを削除できません。
>
> - スコープがデフォルトのスコープである。IPAM を作成すると、2 つのデフォルトスコープ (パブリックスコープが 1 つ、プライベートスコープが 1 つ) が自動的に作成され、それらは削除できません。スコープがデフォルトのスコープであるかどうかを確認するには、スコープの詳細でスコープタイプを確認してください。
> - スコープに 1 つ以上のプールがある。スコープを削除する前に、プールを削除する必要があります。

AWS Management Console

スコープを削除する

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Scopes] (スコープ) を選択します。
3. コンテンツペインで、削除するスコープを選択します。
4. [Actions] (アクション) で、[Delete Scope] (スコープの削除) を選択します。
5. **`delete`** と入力し、[Delete] (削除) を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

スコープを削除するには、次の AWS CLI コマンドを使用します。

1. スコープを表示する: describe-ipam-scopes
2. スコープを削除する: delete-ipam-scope
3. 更新されたスコープを表示する: describe-ipam-scopes

新しいスコープを作成する方法については、追加のスコープを作成する を参照してください。IPAM を削除する方法については、IPAM を削除する を参照してください。

プールから CIDR のプロビジョニングを解除するには

プール CIDR のプロビジョニングを解除して、IP アドレス空間を解放したり、IP アドレス管理を簡素化したりできるほか、ネットワーク変更に備え、コンプライアンス要件を満たすこともできます。プール CIDR のプロビジョニングを解除すると、未使用の IP 空間が再利用され、将来使用できるようになる一方で、IPAM 内の IP アドレス割り当てをより適切に制御および最適化できます。プール内に割り当てがある場合、CIDR のプロビジョニングを解除することはできません。割り当てを削除するには、the section called “割り当ての解除” を参照してください。

IPAM プールの CIDR のプロビジョニングを解除するには、このセクションのステップに従います。すべてのプール CIDR のプロビジョニングを解除すると、そのプールを割り当てに使用できなくなります。割り当てにプールを使用するには、まずプールに新しい CIDR をプロビジョニングする必要があります。

AWS Management Console

プール CIDR のプロビジョニングを解除するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Pools] (プール) を選択します。
3. コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
4. コンテンツペインで、プロビジョニングを解除する CIDR を選択します。
5. [CIDRs] (CIDR) タブを選択します。
6. 1 つまたは複数のCIDR を選択し、[Deprovision CIDRs] (CIDR のプロビジョニング解除) を選択します。
7. [Deprovision CIDR] (CIDR のプロビジョニング解除) を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

プール CIDR のプロビジョニングを解除するには、次の AWS CLI コマンドを使用します。

1. IPAM プール ID を取得する: describe-ipam-pools
2. 現在のプールの CIDR を表示する: get-ipam-pool-cidrs
3. CIDR のプロビジョニングを解除する: deprovision-ipam-pool-cidr
4. 更新された CIDR を表示する: get-ipam-pool-cidrs

プールに新しい CIDR をプロビジョニングするには、プールから CIDR のプロビジョニングを解除するには を参照してください。プールを削除する場合は、プールを削除する を参照してください。

IPAM プールを編集する

プールを編集して、次のいずれかを実行できます。

- プールの割り当てルールを変更する。割り当てルールの詳細については、トップレベル IPv4 プールを作成するを参照してください。
- プールの名前、説明、または他のメタデータを変更して、IPAM 内でより良く整理および可視化できるようにする。
- 検出されたリソースの自動インポートなどのプールオプションを変更して、IPAM の自動 IP アドレス管理を最適化する。

IPAM プールを編集するには、このセクションのステップに従います。

AWS Management Console

プールを編集するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Pools] (プール) を選択します。
3. デフォルトでは、デフォルトのプライベートスコープが選択されます。デフォルトのプライベートスコープを使用しない場合は、コンテンツペインの上部にあるドロップダウンメ

ニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。

4. コンテンツペインで、CIDR を編集するプールを選択します。
5. [Actions] (アクション)、[Edit] (編集) の順に選択します。
6. プールに必要な変更を加えます。プールの設定オプションの詳細については、トップレベル IPv4 プールを作成するを参照してください。
7. [更新] を選択します。

Command line

プールを編集するには、次の AWS CLI コマンドを使用します。

1. IPAM プール ID を取得する: describe-ipam-pools
2. プールを変更する: modify-ipam-pool

コスト配分を有効にする

コスト配分を有効にすると、アクティブな IP アドレスの料金を IPAM 所有者ではなく IP アドレスを使用しているアカウントに分配します。これは、IPAM の委任管理者が IPAM を使用して IP アドレスを一元管理し、各アカウントが各自の使用量に責任を持っていて、手動による請求計算が不要になっている大規模組織にとって有用です。

コスト配分オプションは、IPAM を作成する、または Metering モードで IPAM を変更するときに使用できます。ここでは、次のようになります:

- IPAM 所有者 (デフォルト): IPAM を所有する AWS アカウントは、IPAM で管理されているすべてのアクティブな IP アドレスに対して課金されます。
- リソース所有者: IP アドレスを所有する AWS アカウントは、アクティブな IP アドレスに対して課金されます。

要件

- お使いの IPAM は AWS Organizations と統合する必要があります。
- IPAM は、お使いの AWS Organization の委任 IPAM 管理者によって作成されている必要があります。

- IPAM のホームリージョンは、デフォルトで有効になっているリージョンである必要があります。オプトインリージョンにすることはできません。

課金の仕組み

- 組織内で IP アドレスの料金を分配できますが、すべての IPAM 料金は AWS Organizations 一括請求を用いて組織の支払者アカウントにまとめられます。
- コスト配分が有効になっている場合、組織のメンバーアカウントは、そのアカウント請求書に個々の IPAM の使用状況と料金を表示できます。
- IPAM ARN は、コスト分散が有効になっている場合に個々のアカウント請求書に表示され、リソース所有者は IPAM のアクティブな IP 使用量を追跡できます。AWS Data Exportsを使用する場合、IPAM 料金は、一括請求書と個別のアカウント請求書の両方で、関連する IPAM ARN と表示されます。
- 委任管理者の組織内のアカウントのみが、所有するリソースの料金を受け取ることができます。組織外の IP アドレスのコストは、IPAM 所有者に請求されます。

時間制限

- コスト配分を有効にしてからオプトアウトするまでに 24 時間かかります。24 時間経過後、7 日間は設定を変更することはできません。7 日後にコスト配分を無効にすることができます。

VPC IPAM と Infoblox インフラストラクチャの統合

Amazon VPC IPAM と Infoblox の統合は、AWS VPC IP Address Manager (IPAM) を Infoblox と接続し、クラウドネイティブ AWS 機能を取得しながら、既存の Infoblox ワークフローを通じて AWS IP アドレスを管理できるようにします。

この統合は、重複する IP 管理システムを回避するというエンタープライズの一般的な課題を解決します。新しいツールを学習し、AWS とオンプレミスネットワークの個別のプロセスを維持する代わりに、Infoblox を VPC IPAM スコープの管理機関として指定し、使い慣れた Infoblox インターフェイスをすべての IP アドレスオペレーションに引き続き使用できます。

統合プロセスの概要

以下のステップでは、統合プロセス全体の概要を示します。

1. IPAM スコープを設定する (このドキュメントで説明): Amazon VPC IPAM 委任管理者は、Infoblox を外部権限として使用するように新しいスコープを作成するか、既存のスコープを変更します。
2. Infoblox を設定する (このドキュメントの外部で説明):「次のステップ」を参照してください。
3. 最上位プールを作成する: Amazon VPC IPAM 委任管理者は、Infoblox にリンクされたスコープにプールを作成します。プールは CIDR が割り当てられていない状態で始まります。
4. 外部機関から CIDR をプロビジョニングする: Amazon VPC IPAM 委任管理者がプールの CIDR をプロビジョニングします。使用可能な CIDR を指定せずにリクエスト (Infoblox が許可された範囲から選択) することも、特定の CIDR を指定してリクエスト (Infoblox が可用性に基づいて承認または拒否) することもできます。IPAM は Infoblox と自動的に連携し、承認された CIDR を取得してプロビジョニングします。
5. 標準の IPAM オペレーションを続行する: 標準の Amazon VPC IPAM 手順を使用して、割り当てられた CIDR から子プールと VPC を作成します。

この統合を使用するタイミング

オンプレミスのネットワーク管理に Infoblox を既に使用または使用する予定があり、個別のシステムを維持せずに既存の IP 管理プラクティスを AWS に拡張する場合は、この統合を使用します。

前提条件

この統合を設定する前に、以下を確認してください。

- VPC IPAM Advanced Tier: AWS アカウントで有効になっている。詳細については、「IPAM 階層を変更する」を参照してください。
- 必要な IAM アクセス許可: 以下に記載
- Infoblox リソース識別子: Infoblox 管理者から提供されたもの

Infoblox の IAM ロール

Infoblox プリンシパルが引き受ける IAM ロールを作成するか、既存のロールを使用します。ロールには以下のアクセス許可が必要です。

- `ec2:DescribeIpamPools`
- `ec2:DescribeIpams`
- `ec2:DescribeIpamScopes`

- `ec2:GetIpamPoolAllocations`
- `ec2:GetIpamPoolCidrs`
- `ec2:GetIpamResourceCidrs`

これらのアクセス許可を IAM ロールまたはポリシーに追加する方法については、「IAM ユーザーガイド」の「IAM ID のアクセス許可の追加および削除」を参照してください。

> **Note**
>
> Infoblox では、この統合を有効にするために必要なこれらのアクセス許可に加えて、VPC IPAM 検出のアクセス許可が必要になる場合があります。

VPC IPAM で Infoblox 統合を設定する

AWS VPC IPAM コンソールまたは AWS CLI でスコープを作成または変更するときに、Infoblox 統合を有効にできます。

> **Important**
>
> Infoblox 統合は、パブリックスコープではなく、プライベートスコープでのみ使用できます。

Infoblox 統合による新しいスコープの作成

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、[IPAM] を選択し、次に [スコープ] を選択します。
3. [Create scope] (スコープの作成) を選択します。
4. [スコープの設定] で、以下の操作を行います。
   - [IPAM ID] は自動的に入力されます。
   - (オプション) [名前タグ] に、スコープの名前を入力します。
   - (オプション) [説明] に、ルールの説明を入力します。
5. [スコープ権限] で、[Infoblox IPAM] を選択します。
6. [Infoblox リソース識別子] には、Infoblox リソース識別子を `<version>.identity.account.<entity_realm>.<entity_id>` の形式で入力します。

7. 情報ボックスに表示される必要な IAM アクセス許可があることを確認します。
8. [Create scope] (スコープの作成) を選択します。

これに関連する AWS CLI コマンドは create-ipam-scope です。

既存のスコープの変更

既存のスコープのスコープ権限を [Amazon VPC IPAM] から [Infoblox IPAM] に変更するには、スコープ設定を編集し、前の手順と同じ設定ステップに従います。

これに関連する AWS CLI コマンドは modify-ipam-scope です。

次のステップ

これで、統合に必要な Amazon VPC IPAM 設定は完了です。スコープ権限を設定したら、スコープ内に最上位の IPAM プールを作成できます。詳細については、「トップレベル IPv4 プールを作成する」を参照してください。

また、統合には、Infoblox ソースプールの設定、検出ジョブのステータスの検証、Infoblox が管理するプライベートスコープの設定、Amazon VPC IPAM の Infoblox 管理の有効化、Infoblox 統合または Infoblox ポータルから直接プールを作成する必要があります。

統合の Infoblox 側の詳細については、Infoblox ドキュメントの「AWS IPAM Integration User Guide」を参照してください。

プライベート IPv6 GUA CIDR のプロビジョニングを有効にする

プライベートネットワークで IPv6 をサポートし、そのアドレスからインターネットにトラフィックをルーティングするつもりがない場合は、プライベート IPv6 ULA または GUA 範囲をプライベートスコープの IPAM プールにプロビジョニングできます。

プライベート IPv6 アドレス指定に関する重要な詳細については、「Amazon VPC ユーザーガイド」の「プライベート IPv6 アドレス」を参照してください。

プライベート IPv6 アドレスには 2 つのタイプがあります。

- IPv6 ULA 範囲: RFC4193 で定義されている IPv6 アドレス。このアドレス範囲は常に「fc」または「fd」で始まり、簡単に識別できます。有効な IPv6 ULA スペースは、Amazon の予約範囲 fd00::/16 と重複しない fd00::/8 より下のいずれかです。

- IPv6 GUA 範囲: RFC3587 で定義されている IPv6 アドレス。IPv6 GUA 範囲をプライベート IPv6 アドレスとして使用するオプションはデフォルトで無効になっているため、使用する前に有効にする必要があります。

IPv6 ULA アドレス範囲を使用するには、IPAM プールに CIDR をプロビジョニングするときに IPv6 オプションを選択し、IPv6 ULA 範囲を入力します。ただし、独自の IPv6 GUA 範囲をプライベート IPv6 アドレスとして使用するには、まずこのセクションのステップを完了する必要があります。このオプションはデフォルトでは無効になっています。

> **Note**
>
> - プライベート IPv6 GUA 範囲を使用するときは、独自に所有する IPv6 GUA 範囲を使用する必要があります。
> - IPAM は、IPv6 ULA および GUA アドレスを持つリソースを検出し、プールをモニタリングして、IPv6 ULA および GUA アドレス空間が重複していないかを確認します。
> - プライベート IPv6 アドレスを持つリソースからインターネットに接続する場合、それは可能ですが、そのためにはパブリック IPv6 アドレスを持つ別のサブネットのリソースを介してトラフィックをルーティングする必要があります。
> - VPC にプライベート IPv6 GUA 範囲が割り当てられている場合、同じ VPC 内のプライベート IPv6 GUA スペースと重複するパブリック IPv6 GUA スペースを使用することはできません。
> - プライベート IPv6 ULA および GUA アドレス範囲を持つリソース間の通信がサポートされています (Direct Connect 間、VPC ピアリング 間、Transit Gateway 間、VPN 接続間など)。
> - プライベート GUA IPv6 範囲を、パブリックにアドバタイズされた IPv6 GUA 範囲に変換することはできません。

AWS Management Console

プライベート IPv6 GUA CIDR のプロビジョニングを有効にするには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[IPAM] を選択します。
3. 使用する IPAM を選択して、[アクション]、[編集] の順に選択します。

4. [プライベート IPv6 GUA CIDR] で、[プライベート IPv6 IPAM プールへの GUA CIDR スペースのプロビジョニングを有効にする] を選択します。
5. [Save changes] (変更の保存) をクリックします。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

次の AWS CLI コマンドを使用して、プライベート IPv6 GUA CIDR のプロビジョニングを有効にします。

1. describe-ipams で現在の IPAM を表示する
2. modify-ipam で IPAM を変更し、対象オプションを `enable-private-gua` に入れます。

プライベート IPv6 GUA CIDR をプロビジョニングするオプションを有効にすると、プライベート IPv6 GUA CIDR をプールにプロビジョニングできます。詳細については、「CIDR をプールにプロビジョニングする」を参照してください。

SCP を使用して VPC 作成に IPAM の使用を強制する

> **Note**
>
> このセクションは、IPAM と AWS Organizations の統合を有効にしている場合にのみ適用されます。詳細については、「IPAM を AWS Organizations 内のアカウントと統合する」を参照してください。

このセクションでは、AWS Organizations でサービスコントロールポリシーを作成する方法について説明します。ここでは、組織のメンバーが VPC を作成する際に IPAM を使用する必要があります。サービスコントロールポリシー (SCP) は、組織のアクセス許可を管理できる組織ポリシーの一種です。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。

VPC の作成時に IPAM の使用を強制する

VPC の作成時に、組織のメンバーに IPAM を使用するよう義務付けるには、このセクションの手順に従います。

SCP を作成して VPC の作成に IPAM を使用するように制限するには

1. AWS Organizations ユーザーガイドの「サービスコントロールポリシーの作成」のステップに従って、JSON エディターに以下のテキストを入力してください。

   JSON

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

2. 組織内の 1 つ以上の組織単位にポリシーをアタッチします。詳細については、AWS Organizations ユーザーガイドの「ポリシーのアタッチ」と「ポリシーのデタッチ」を参照してください。

VPC の作成時に IPAM プールの使用を強制する

VPC の作成時に、組織のメンバーに特定の IPAM プールを使用するよう義務付けるには、このセクションの手順に従います。

SCP を作成して VPC の作成に IPAM プールを使用するように制限するには

1. AWS Organizations ユーザーガイドの「サービスコントロールポリシーの作成」のステップに従って、JSON エディターに以下のテキストを入力してください。

   JSON

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

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

2. サンプルの値 `ipam-pool-0123456789abcdefg` を、ユーザーを制限したい IPv4 プール ID に変更します。
3. 組織内の 1 つ以上の組織単位にポリシーをアタッチします。詳細については、AWS Organizations ユーザーガイドの「ポリシーのアタッチ」と「ポリシーのデタッチ」を参照してください。

特定の OU リスト以外のすべての OU に IPAM を適用する

このセクションのステップに従い、特定の組織単位 (OU) のリストを除くすべての OU に IPAM を適用します。このセクションで説明するポリシーは、組織内の OU (`aws:PrincipalOrgPaths` で指定した OU を除く) に、IPAM を使用して VPC を作成および拡張することを要求しています。リストにある OU は、VPC の作成時に IPAM を使用するか、IP アドレスの範囲を手動で指定することができます。

SCP を作成し、特定の OU リストを除くすべての OU に IPAM を適用するには

1. AWS Organizations ユーザーガイドの「サービスコントロールポリシーの作成」のステップに従って、JSON エディターに以下のテキストを入力してください。

   JSON

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

```
        "ec2:Ipv4IpamPoolId": "true"
               },
         "ForAnyValue:StringNotLike": {
             "aws:PrincipalOrgPaths": [
                 "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/",
                 "o-a1b2c3d4e5/r-ab12/ou-ab13-22222222/ou-ab13-33333333/"
             ]
                }
            }
     }]
}
```

2. サンプルの値 (o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/ など) を削除し、IPAM を使用するオプション (必須ではない) を付与する OU の、AWS Organizations エンティティパスを追加します。エンティティパスの詳細については、IAM ユーザーガイドの「AWS Organizations エンティティパスを理解する」および「aws: PrincipalOrgPaths」を参照してください。
3. ポリシーを組織のルートにアタッチします。詳細については、AWS Organizations ユーザーガイドの「ポリシーのアタッチ」と「ポリシーのデタッチ」を参照してください。

IPAM から組織単位を除外する

IPAM が AWS Organizations と統合されている場合は、組織単位 (OU) を IPAM による管理から除外できます。OU を除外すると、IPAM はその OU のアカウントの IP アドレスを管理しなくなります。この機能により、IPAM をより柔軟に使用できます。

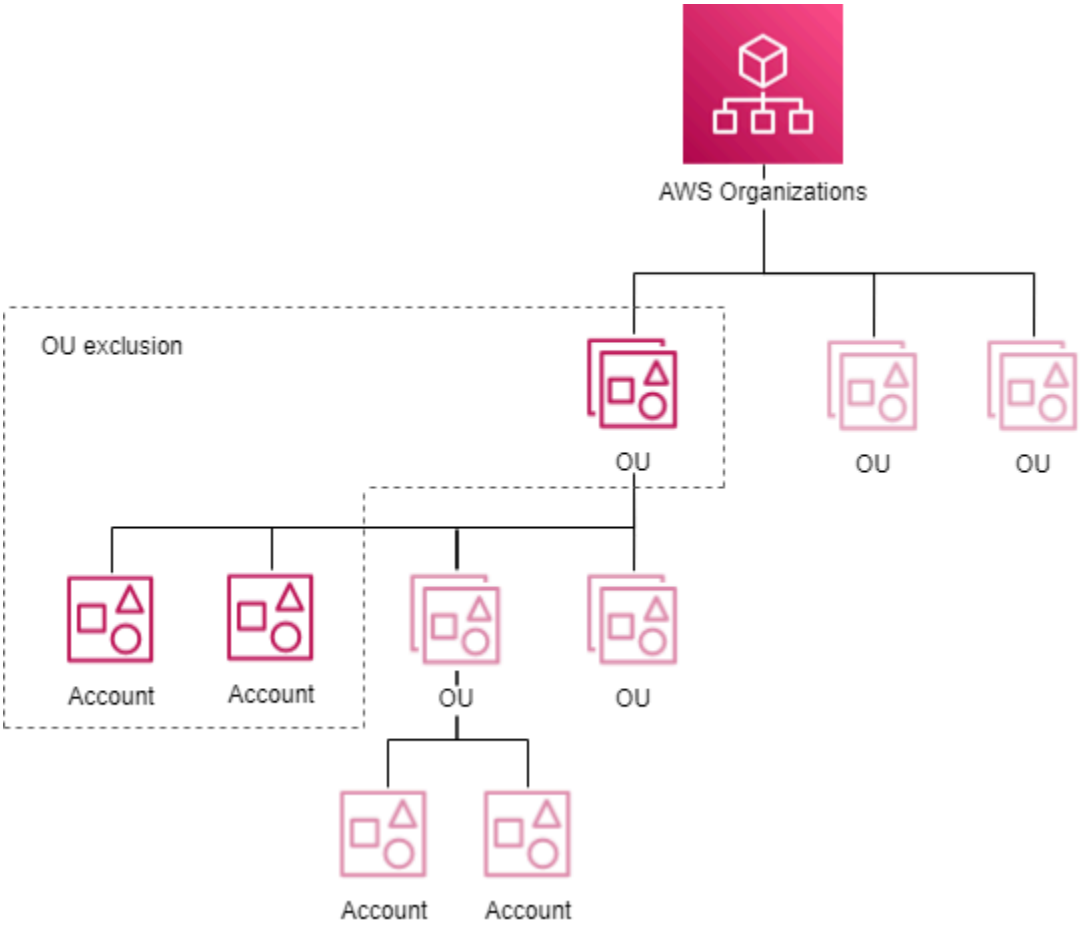
OU の除外は、次の方法で使用できます:

- ビジネスの特定の部分のために IPAM を有効にする: AWS Organizations に複数のビジネスユニットまたは子会社がある場合は、IPAM を必要とするビジネスユニットまたは子会社のためにのみ使用できるようになりました。
- サンドボックスアカウントが分離された状態を維持する: IPAM からサンドボックスアカウントを除外し、IP 管理のために本当に重要なアカウントにのみ焦点を当てることができます。

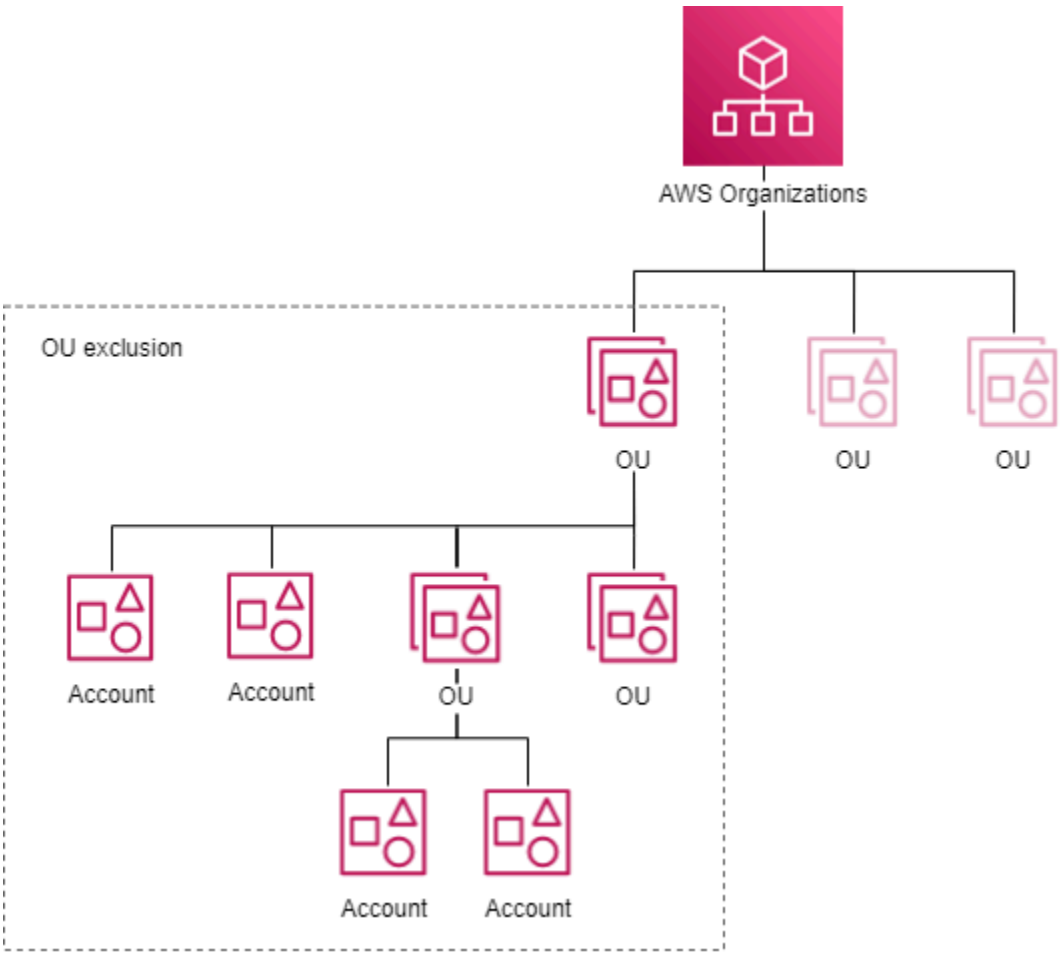
OU の除外の仕組み

このセクションの図は、IPAM での OU の除外の追加に関する 2 つの異なるユースケースを示しています。

最初の図は、組織単位 (OU) の除外を親 OU にのみ追加した場合の影響を示しています。結果として、IPAM は親 OU のアカウントの IP アドレスを管理しません。IPAM は、除外に含まれない他の OU のアカウントの IP アドレスを管理します。



2 番目の図は、組織単位 (OU) の除外を親 OU およびすべての子 OU に追加した場合の影響を示しています。結果として、IPAM は親 OU のアカウントや子 OU のアカウントの IP アドレスを管理しません。IPAM は、除外に含まれない OU のアカウントの IP アドレスを管理します。



OU の除外を追加または削除する

OU の除外を追加または削除するには、このセクションのステップを実行します。

> **Note**
>
> - 委任された IPAM 管理者アカウントは、除外された OU 内であっても除外されません。
> - OU の除外を追加するには、IPAM を AWS Organizations と統合する必要があります。Organization には OU が含まれている必要があります。
> - OU の除外を表示、追加、または削除するには、委任された IPAM 管理者である必要があります。
> - 最近作成された組織単位を IPAM が検出するには時間がかかります。
> - リソース検出ごとに追加できる除外の数には、デフォルトのクォータがあります。詳細については、「IPAM のクォータ」の「リソース検出あたりの組織単位の除外」を参照してください。

- リソース検出を別のアカウントと共有する場合、そのアカウントでは、リソース検出所有者の Organization の組織 ID、ルート ID、組織単位 ID などの情報を含む OU の除外を確認できます。

AWS Management Console

OU の除外を追加または削除するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで [リソース検出] を選択します。
3. デフォルトのリソース検出を選択します。
4. [編集] を選択します。
5. [組織単位の除外] で、次を実行します:
   - OU の除外を追加するには:
     - OU とそのすべての子 OU を除外する場合:
       - テーブルで OU を見つけ、チェックボックスをオンにします。すべての子 OUが自動的に選択されます。
     - 親 OU アカウントのみを除外する場合:
       - テーブルで OU を見つけ、チェックボックスをオンにします。すべての子 OUが自動的に選択されます。すべての子 OU の選択を解除します。
     - あるいは、[アクション] 列を使用して、親 OU のみ、または親 OU と子 OU を選択できます。
       - [すべての子 OU を選択]: 除外にすべての子 OU を含めます。OU を選択すると、その OU が画面に追加されます。各 OU には、OU の除外の ID とエンティティパスが含まれます。
       - [この OU のみを選択]: 除外にこの OU のみを含めます。OU を選択すると、その OU が画面に追加されます。各 OU には、OU の除外の ID とエンティティパスが含まれます。
       - [OU エンティティパスをコピー]: 必要に応じて、使用する Organization エンティティパスをコピーします。
     - AWS Organizations エンティティパスが既にわかっている場合、またはそれを構築する場合:

- [組織単位の除外を入力] を選択し、OU の除外のエンティティパスを入力します。/ で区切られた AWS Organizations ID を使用して、OU のパスを構築します。パスの末尾を /* にして、すべての子 OU を含めます。
  - 例 1
    - 子 OU へのパス: o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/
    - この例では、o-a1b2c3d4e5 は組織 ID、r-f6g7h8i9j0example はルート ID、ou-ghi0-awsccccc は OU ID、ou-jkl0-awsddddd は子 OU ID です。
    - IPAM は子 OU のアカウントの IP アドレスを管理しません。
  - 例 2
    - すべての子 OU が除外の一部となるパス: o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*
    - この例では、IPAM は OU (ou-ghi0-awsccccc) のアカウント、または OU の子である OU のアカウントの IP アドレスを管理しません。
- OU の除外を削除するには:
  - 既に追加されている OU の横にある [X] を選択します。OU ID の後の /* は、それが親 OU であり、子 OU が OU の除外の一部であることを示します。

6. [Save changes] (変更の保存) をクリックします。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

1. 次のステップのために、describe-ipam-resource-discoveries を使用して、リソース検出の詳細を表示してデフォルトのリソース検出の ID を取得します。

   入力:

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

   出力:

   ```
   {
   ```

```
    "IpamResourceDiscoveries": [

        {

            "OwnerId": "111122223333",

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

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

            "OperatingRegions": [

                {

                    "RegionName": "us-east-1"

                },

                {

                    "RegionName": "us-west-1"

                },

                {

                    "RegionName": "us-west-2"

                }

            ],

            "IsDefault": true,

            "State": "modify-complete",

            "Tags": []

        }

    ]
```

```
}
```

2. modify-ipam-resource-discovery と `--add-organizational-unit-exclusions` または `--remove-organizational-unit-exclusions` オプションを使用して、リソース検出から組織単位の除外を追加または削除します。AWS Organizations エンティティパスを入力する必要があります。/ で区切られた AWS Organizations ID を使用して、OU のパスを構築します。パスの末尾を /* にして、すべての子 OU を含めます。追加または削除パラメータに同じエンティティ パスを複数回含めることはできません。

   - 例 1
     - 子 OU へのパス: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
     - この例では、`o-a1b2c3d4e5` は組織 ID、`r-f6g7h8i9j0example` はルート ID、`ou-ghi0-awsccccc` は OU ID、`ou-jkl0-awsddddd` は子 OU ID です。
     - IPAM は子 OU のアカウントの IP アドレスを管理しません。
   - 例 2
     - すべての子 OU が除外の一部となるパス: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
     - この例では、IPAM は OU (`ou-ghi0-awsccccc`) のアカウント、または OU の子である OU のアカウントの IP アドレスを管理しません。

   > **Note**
   >
   > 結果として得られる除外設定の集合は「重複」してはいけません。つまり、複数の OU 除外が同一の OU を除外してはいけません。
   > 重複しないエンティティパスの例:
   >
   > - Path 1 ="o-1/r-1/ou-1/"
   > - Path 2 ="o-1/r-1/ou-1/ou-2/"
   >
   > Path 1 は ou-1 のアカウントのみを除外し、Path 2 は ou-2 のアカウントのみを除外するため、これらのパスは重複しません。
   > エンティティパスの重複の例:
   >
   > - Path 1 ="o-1/r-1/ou-1/*"

- Path 2 ="o-1/r-1/ou-1/ou-2/"

Path 1 は "o-1/r-1/ou-1/" と "o-1/r-1/ou-1/ou-2/"の両方を表し、"o-1/r-1/ou-1/ou-2/" は Path 2 と重複するため、これらのパスは重複します。

入力:

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

出力:

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

IPAM 階層を変更する

IPAM には無料利用枠とアドバンス利用枠の 2 つの階層があります。Amazon VPC IP Address Manager のアドバンストティアに切り替えると、IP アドレス管理をより詳細に制御できます。これは、ネットワークの複雑さが増すにつれてより多くの恩恵をもたらすことができるため、ユーザーは IP アドレス空間をより良く最適化および管理できます。無料利用枠で利用できる機能とアドバンス利用枠に関連するコストの詳細については、「Amazon VPC の料金」の [IPAM] タブを参照してください。

> **Note**
>
> アドバンス利用枠から無料利用枠に切り替える前に、次のことを行う必要があります。
>
> - プライベート範囲プールを削除します。
> - IPAM 内のデフォルト以外のすべてのプライベート範囲を削除します。
> - IPAM ホームリージョンとロケールが異なるプールを削除します。
> - デフォルト以外ののリソース検出アソシエーションを削除します。
> - IPAM 以外のアカウントへのプール割り当てを削除します。

AWS Management Console

IPAM 階層を変更するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[IPAMs] (IPAM) を選択します。
3. コンテンツペインで、IPAM を選択します。
4. [Actions] (アクション)、[Edit] (編集) の順に選択します。

> **Note**
>
> 無料利用枠に加入している場合、[IPAM の推定アクティブ IP 数の合計は...] と表示されます。
> アクティブな IP 数の合計はアドバンスト階層に切り替えた場合に課金される IPAM 内のアクティブな IP アドレスの数です。アクティブ IP アドレスは、EC2 インスタンスなどのリソースにアタッチされた Elastic Network Interface (ENI) に関連付けられた IP アドレスまたはプレフィックスとして定義されます。

- このメトリクスは、無料利用枠のお客様にのみご利用いただけます。
- IPAM が AWS Organizations と統合されている場合、アクティブな IP 数はすべての組織アカウントをカバーします。
- アクティブな IP 数の内訳を IP タイプ (パブリック/プライベート) またはクラス (IPv4/IPv6) 別に表示することはできません。
- IPAM は、モニタリング対象アカウントが所有する ENI からの IP のみをカウントします。共有サブネットの数は不正確である可能性があります。サブネット所有者または ENI 所有者が IPAM によってカバーされていない場合、IP アドレスは除外されます。

5. IPAM に使用する [IPAM 階層] を選択します。
6. [Save changes] (変更の保存) をクリックします。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

次の AWS CLI コマンドを使用して IPAM 階層を表示および変更します。

1. 現在の IPAM を表示する: describe-ipams
2. IPAM 階層の変更: modify-ipam
3. 更新された IPAM を表示する: describe-ipams

IPAM 操作リージョンの変更

運用リージョンとは、IPAM が IP アドレス CIDR の管理を許可されている AWS リージョンのことです。IPAM は、運用リージョンとして選択された AWS リージョンのリソースのみを検出および監視します。

IPAM に運用リージョンを追加すると、複数の AWS リージョンにわたって IP アドレス空間を管理できます。これにより、IP アドレスの使用率が改善され、リージョンレベルのセグメンテーションが可能になり、地理的に分散されたインフラストラクチャをサポートできます。IPAM のリージョンレベルのスコープを拡張すると、IP アドレス管理全体の柔軟性が向上し、コントロールが強化されます。

AWS Management Console

IPAM 操作リージョンを変更するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[IPAMs] (IPAM) を選択します。
3. コンテンツペインで、IPAM を選択します。
4. [Actions] (アクション)、[Edit] (編集) の順に選択します。
5. [IPAM 設定] で、IPAM に使用する操作リージョンを選択します。
6. [Save changes] (変更の保存) をクリックします。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

次の AWS CLI コマンドを使用して、IPAM 操作リージョンを表示および変更します。

1. 現在の IPAM を表示する: describe-ipams
2. IPAM 操作リージョンの追加または削除: modify-ipam
3. 更新された IPAM を表示する: describe-ipams

CIDR をプールにプロビジョニングする

CIDR をプールにプロビジョニングするには、このセクションのステップに従います。プールの作成時に既に CIDR をプロビジョニングしている場合、プールの割り当て容量が残りわずかな場合は、追加の CIDR のプロビジョニングが必要になる場合があります。プールの使用状況を監視するには、IPAM ダッシュボードで CIDR の使用状況をモニタリングする を参照してください。

> **Note**
>
> このユーザーガイドと IPAM コンソールでは、全体を通じてプロビジョンおよび割り振りという用語が使用されています。プロビジョンは、CIDR を IPAM プールに追加するときに使用されます。割り振りは、IPAM プールからの CIDR を VPC または Elastic IP アドレスに関連付けるときに使用されます。

AWS Management Console

CIDR をプールにプロビジョニングするには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Pools] (プール) を選択します。
3. デフォルトでは、デフォルトのプライベートスコープが選択されます。デフォルトのプライベートスコープを使用しない場合は、コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
4. コンテンツペインで、CIDR を追加するプールを選択します。
5. [Actions] (アクション) > [Provision CIDRs] (CIDR のプロビジョニング) を選択します。
6. 次のいずれかを行います。

   - CIDR をパブリックスコープのプールにプロビジョニングする場合は、[ネットマスク] を入力します。
   - CIDR をプライベートスコープの IPv4 プールにプロビジョニングする場合は、[CIDR] を入力します。
   - CIDR をプライベートスコープの IPv6 プールにプロビジョニングする場合は、次の点に注意してください。
     - プライベート IPv6 アドレス指定に関する重要な詳細については、「Amazon VPC ユーザーガイド」の「プライベート IPv6 アドレス」を参照してください。
     - プライベート IPv6 ULA 範囲を使用するには、[プロビジョニングする CIDR] で、[ネットマスクで ULA CIDR を追加] を選択してネットマスクサイズを選択するか、[プライベート IPv6 CIDR を入力] を選択して ULA 範囲を入力します。プライベート IPv6 ULA の有効範囲は、fd80::/9 以降の /9 ~ /60 です。
     - プライベート IPv6 GUA 範囲を使用するには、まず IPAM で 対象オプションを有効にする必要があります (「プライベート IPv6 GUA CIDR のプロビジョニングを有効にする」を参照)。プライベート IPv6 GUA CIDR を有効にしたら、[プライベート IPv6 CIDR を入力] で IPv6 GUA を入力します。

> **Note**
>
> - デフォルトで、リージョンプールには 1 つの Amazon 提供の IPv6 CIDR ブロックを追加できます。デフォルト制限の引き上げに関する情報については、「IPAM のクォータ」を参照してください。
> - プロビジョニングする CIDR がスコープ内で利用可能である。
> - プール内のプールに CIDR をプロビジョニングする場合は、プロビジョニングする CIDR スペースがそのプールで使用可能である。

7. [プロビジョニング] を選択します。
8. IPAM で CIDR を表示するには、ナビゲーションペインで、[Pools] (プール) を選択し、プールの [CIDRs] (CIDR) タブを表示します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

CIDR をプールにプロビジョニングするには、次の AWS CLI コマンドを使用します。

1. IPAM プールの ID を取得: describe-ipam-pools
2. プールにプロビジョニングされた CIDR を取得: get-ipam-pool-cidrs
3. プールに新しい CIDR をプロビジョニング: provision-ipam-pool-cidr
4. プールにプロビジョニングされた CIDR を取得し、新しい CIDR を表示: get-ipam-pool-cidrs

スコープ間で VPC CIDR を移動する

CIDR をスコープ間で移行することで、IP アドレスの割り当てを最適化し、リージョン別に整理するとともに、懸念を分離して、コンプライアンスを強制し、インフラストラクチャの変更に適応できます。この柔軟性により、ワークロードの進化に合わせて IP アドレス空間を効率的に管理できます。

あるスコープから別のスコープに VPC CIDR を移動する場合は、このセクションのステップに従ってください。

Important

- VPC CIDR のみを移動できます。VPC CIDR を移動すると、VPC のサブネット CIDR も自動的に移動されます。
- VPC CIDR の移動は、あるプライベートスコープから別のプライベートスコープにのみ行うことができます。VPC CIDR をパブリックスコープからプライベートスコープに移動したり、プライベートスコープからパブリックスコープに移動したりすることはできません。
- 同じ AWS アカウントが両方のスコープを持っている必要があります。
- プライベートスコープのプールから VPC CIDR が現在割り当てられている場合、移動リクエストは成功しますが、現在のプールから VPC CIDR 割り当てを解除するまで、VPC CIDR は移動されません。割り当ての解除の詳細については、「割り当ての解除」を参照してください。

AWS Management Console

VPC に割り当てられた CIDR を移動するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[リソース] を選択します。
3. コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。
4. コンテンツペインで、VPC を選択し、VPC の詳細を表示します。
5. [VPC CIDRs] (VPC CIDR) で、リソースに割り当てられた CIDR の 1 つを選択し、[Actions] (アクション)、[Move CIDR to different scope] (CIDR を別のスコープに移動) を順に選択します。
6. VPC CIDR の移動先のスコープを選択します。
7. [Move CIDR to different scope] (CIDR を別のスコープに移動) を選択します。

Command line

VPC CIDR を移動するには、次の AWS CLI コマンドを使用します。

1. 現在のスコープ内の VPC CIDR を取得: get-ipam-resource-cidrs

2. VPC CIDR を移動: modify-ipam-resource-cidr
3. 他のスコープ内の VPC CIDR を取得: get-ipam-resource-cidrs

IPAM ポリシーを使用してパブリック IPv4 割り当て戦略を定義する

IPAM ポリシーは、IPAM プールからのパブリック IPv4 アドレスを AWS リソースに割り当てる方法を定義する一連のルールです。各ルールは、サービスが IP アドレスを取得するために使用する IPAM プールに AWS サービスをマッピングします。1 つのポリシーに複数のルールを設定し、複数の AWS リージョンに適用できます。IPAM プールのアドレスが不足している場合、サービスは Amazon が提供する IP アドレスにフォールバックします。ポリシーは、AWS Organizations 内の個々の AWS アカウントまたはエンティティに適用できます。Bring-Your-Own-IP (BYOIP) を導入すると、AWS パブリック IPv4 のコストを削減できます。

IPAM ポリシーを使用するタイミング

IPAM ポリシーを使用して以下を行います。

- BYOIP アドレスを使用してパブリック IPv4 コストを削減する
- AWS リソースが使用する IP プールを一元的に制御する
- 組織全体で一貫した IP 割り当てを確保する

仕組み

IPAM ポリシーが強制されたアカウントでパブリック IP アドレスを必要とする AWS リソースを作成する場合:

- IPAM はポリシールールを順番にチェックします。
- ルールがリソースタイプと一致する場合、IPAM は指定されたプールから IP を割り当てます。
- プールが空で、オーバーフローが有効になっている場合、Amazon は IP アドレスを提供します。
- 一致するルールがない場合、デフォルトの動作が適用されます。

サポートされているサービスとリソース

IPAM ポリシーを作成して、IPAM プールからのパブリック IPv4 アドレスを以下の AWS サービスとリソースに割り当てる方法を定義できます。

- Elastic IP アドレス (EIP)
- Application Load Balancers (ALB)
- Amazon Relational Database Service (RDS)
- リージョン NAT ゲートウェイ

> **Important**
>
> AWS リソースを作成するときに特定の IPAM プールまたは EIP 割り当て ID を選択すると IPAM ポリシーが上書きされます。

前提条件

- アドバンスト階層が有効になっている委任管理者アカウントの IPAM
- IPv4 アドレスを持つパブリック IPAM プール
- IPAM および EC2 オペレーションの IAM アクセス許可

用語

IPAM ポリシー

IPAM ポリシーは、IPAM プールからのパブリック IPv4 アドレスを AWS リソースに割り当てる方法を定義する一連のルールです。各ルールは、サービスが IP アドレスを取得するために使用する IPAM プールに AWS サービスをマッピングします。1 つのポリシーに複数のルールを設定し、複数の AWS リージョンに適用できます。IPAM プールのアドレスが不足している場合、サービスは Amazon が提供する IP アドレスにフォールバックします。ポリシーは、AWS Organizations 内の個々の AWS アカウントまたはエンティティに適用できます。ポリシーは、AWS Organizations 内の個々の AWS アカウントまたはエンティティに適用できます。

割り当てルール

AWS リソースタイプを特定の IPAM プールにマッピングする IPAM ポリシー内のオプション設定。ルールが定義されていない場合、リソースタイプはデフォルトで Amazon が提供する IP アドレスを使用します。

ターゲット

IPAM ポリシーを適用できる AWS Organization 内の個々の AWS アカウントまたはエンティティ。

ステップ 1: IPAM ポリシーを作成する

AWS コンソールを使用する:

AWS コンソールを使用して IPAM ポリシーを作成するには、以下のステップに従います。

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. 左のナビゲーションペインの [ポリシー] を選択します。
3. [Create policy (ポリシーの作成)] を選択します。
4. ポリシーの [名前] を入力します (オプション)。
5. このポリシーに関連付ける [IPAM] を選択します。
6. (オプション) タグを追加します。
7. [Create policy] (ポリシーの作成) を選択します。

AWS CLI の使用

create-ipam-policy コマンドを使用します。

ステップ 2: 割り当てルールを追加する

ポリシーを作成したら、IP アドレスの割り当て方法を定義する割り当てルールを追加する必要があります。

AWS コンソールを使用する:

AWS コンソールを使用して割り当てルールを追加するには、以下のステップに従います。

1. 左のナビゲーションペインの [ポリシー] を選択します。
2. 前のステップで作成したポリシーを選択します。
3. ポリシーの詳細ページで、[割り当てルール] タブを選択します。
4. [割り当てルールの作成] を選択します。
5. [サービスの設定] を設定します。

   - [ロケール]: このポリシーを適用する AWS リージョン (us-east-1) またはローカルゾーンを選択します。
   - リソースタイプ: このポリシーの AWS サービスまたはリソースタイプ (リージョン別可用性モードの Elastic IP アドレス、RDS データベースインスタンス、Application Load Balancer、または NAT ゲートウェイ) を選択します。

6. [ルールの設定] を設定します。
   - [IPAM プール]: IP アドレスを提供する IPAM プールを選択します。
   - プールの詳細 (ロケール、パブリック IP ソース、使用可能なスペース、使用可能な CIDR 範囲) を確認します。
7. (オプション) 追加のルールを作成するには、[新しいルールを追加] を選択します。
8. [割り当てルールの作成] を選択します。

AWS CLI の使用

modify-ipam-policy-allocation-rules コマンドを使用します。

ステップ 3: ポリシーを有効にする

このポリシーを使用するアカウントを指定します。

AWS コンソールを使用する:

AWS コンソールを使用してポリシーを有効にするには、以下のステップに従います。

1. ポリシーの詳細ページで、[ターゲット] タブを選択します。
2. [ポリシーターゲットの管理] を選択します。
3. 次のいずれかを行います。
   - 単一アカウントで使用する (IPAM が AWS Organizations と統合されていない) 場合は、[アカウントで有効にする] を選択します。
   - AWS Organizations と統合された IPAM の場合 (委任管理者の場合):
     - [組織構造] セクションで、このポリシーを適用するアカウントまたは組織単位を選択します。
     - 各ターゲットの [有効] チェックボックスをオンにします。
     - [Save changes] (変更の保存) をクリックします。
     - 重要: このポリシーを有効にすると、選択したアカウントまたは組織単位のアクティブな IPAM ポリシーが置き換えられます。

AWS CLI の使用

セットアップに基づいて enable-ipam-policy コマンドを使用します。

単一アカウントで使用する (IPAM が AWS Organizations と統合されていない) 場合:

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

AWS Organizations と統合された IPAM の場合 (委任管理者の場合)、AWS Organization 内のアカウントをターゲットとするポリシーを設定します。

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

AWS Organizations と統合された IPAM の場合 (委任管理者の場合)、組織単位をターゲットとするポリシーを設定します。

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

> **Important**
>
> このポリシーを有効にすると、選択したアカウントまたは組織単位のアクティブな IPAM ポリシーが置き換えられます。

ステップ 4: ポリシーをテストする

いずれかのターゲットアカウントで、設定したタイプの新しいリソース (EIP など) を作成します。リソースは、IPAM プールの IP アドレスを自動的に使用します。

> **Important**
>
> AWS リソースを作成するときに特定の IPAM プールまたは EIP 割り当て ID を選択すると IPAM ポリシーが上書きされます。

ステップ 5: 使用状況をモニタリングする

コンソールで IPAM プールを確認して、リソースに割り当てられた IP アドレスを確認します。

割り当ての解除

プールを削除する場合は、プールの割り当ての解除が必要な場合があります。割り当てとは、IPAM プールから別のリソースまたは IPAM プールへの CIDR 割り当てです。

プールに CIDR がプロビジョニングされている場合はプールを削除できません。また、CIDR がリソースに割り当てられている場合は CIDR のプロビジョニングを解除できません。

Note

- 手動割り当てを解放するには、このセクションの手順を使用するか、ReleaseIpamPoolAllocation API を呼び出します。
- プライベートスコープ内の割り当てを解放するには、リソース CIDR を無視または削除する必要があります。(詳しくは、「VPC CIDR のモニタリング状態を変更する」を参照してください。) しばらくすると、Amazon VPC IPAM がユーザーに代わって自動的に割り当てを解放します。

  Example

  例

  プライベートスコープに VPC CIDR を使用している場合、割り当てを解放するには、VPC CIDR を無視するか、削除する必要があります。しばらくすると、Amazon VPC IPAM は IPAM プールから自動的に VPC CIDR の割り当てを解放します。
- パブリックスコープで割り当てを解放するには、リソース CIDR を削除する必要があります。パブリックリソース CIDR を無視することはできません。詳細については、AWS CLI のみを使用した IPAM への自分のパブリック IPv4 CIDR の取り込み の「クリーンアップ」、または AWS CLI のみを使用した IPAM への IPv6 CIDR の取り込み の「クリーンアップ」を参照してください。しばらくすると、Amazon VPC IPAM がユーザーに代わって自動的に割り当てを解放します。

Amazon VPC IPAM がお客様に代わって割り当てを解放するには、すべてのアカウント権限が、単一アカウント使用または複数アカウント使用のいずれかに適切に設定されている必要があります。

IPAM によって管理されている CIDR を解放すると、Amazon VPC IPAM は CIDR を IPAM プールにリサイクルします。アドバンスト枠で IPAM を使用している場合、CIDR が以後の割り当てに使用できるようになるまでに数分かかります。無料利用枠で IPAM を使用している場合、CIDR が以後の割り当てに使用できるまでに最大 48 時間かかります。プールと割り当ての詳細については、IPAM の仕組み を参照してください。

AWS Management Console

プールの割り当てを解除するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Pools] (プール) を選択します。
3. コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組み を参照してください。
4. コンテンツペインで、割り当てが含まれているプールを選択します。
5. [Allocations] (割り当て) タブを選択します。
6. 1 つまたは複数の割り当てを選択します。割り当ては、リソースタイプによって以下のように識別できます。
   - custom: カスタム割り当て。
   - vpc: VPC 割り当て。
   - ipam-pool: IPAM プール割り当て。
   - ec2-public-ipv4-pool: パブリック IPv4 プール割り当て。
   - [サブネット]: サブネットの割り当て。
7. [Actions] (アクション)、[Release custom allocation] (カスタム割り当ての解除) を順に選択します。
8. [Deallocate CIDR] (CIDR の割り当て解除) を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

プールの割り当てを解除するには、次の AWS CLI コマンドを使用します。

1. IPAM プール ID を取得: describe-ipam-pools

2. プール内の現在の割り当てを表示: get-ipam-pool-allocations
3. 割り当てを解除: release-ipam-pool-allocation
4. 更新された割り当てを表示: get-ipam-pool-allocations

新しい割り当てを追加するには、IPAM プールから CIDR を割り当てる を参照してください。割り当てを解除した後にプールを削除するには、最初に プールから CIDR のプロビジョニングを解除するには を実行する必要があります。

AWS RAM を使用して IPAM プールを共有する

このセクションでは、AWS Resource Access Manager (RAM) を使用して IPAM プールを共有するためのステップを説明します。IPAM プールを RAM で共有している場合、「プリンシパル」はプールからの CIDR をそれぞれのアカウントの AWS リソース (VPC など) に割り当てることができます。プリンシパルとは、RAM の概念であり、AWS Organizations の AWS アカウント、IAM ロール、組織単位を意味します。詳しくは、AWS RAM ユーザーガイドの AWS リソースの共有をご覧ください。

Note

- IPAM プールを AWS RAM と共有できるのは、IPAM と AWS Organizations を統合している場合のみです。詳細については、「IPAM を AWS Organizations 内のアカウントと統合する」を参照してください。単一アカウントの IPAM ユーザーの場合、IPAM プールを AWS RAM と共有することはできません。
- AWS RAM で AWS Organizations でのリソース共有を有効にする必要があります。詳細については、AWS RAM ユーザーガイドの AWS Organizations 内でリソース共有を有効にするを参照してください。
- RAM 共有は、IPAM のホーム AWS リージョンでのみ使用できます。IPAM プールのリージョンではなく、IPAM がある AWS リージョンに共有を作成する必要があります。
- IPAM プールリソース共有を作成および削除するアカウントには、その IAM ロールにアタッチされている IAM ポリシーで次のアクセス許可が必要です。
  - `ec2:PutResourcePolicy`
  - `ec2:DeleteResourcePolicy`
- 複数の IPAM プールを RAM 共有に追加できます。
- IPAM プールは AWS Organization 外の任意の AWS アカウントと共有できますが、IPAM が Organization 外のアカウントの IP アドレスをモニタリングするのは、アカウント所有

者が IPAM を組織外のアカウントに統合する の説明に従って委任 IPAM 管理者とリソース検出を共有するプロセスを実行した場合のみです。

AWS Management Console

RAM を使用して IPAM プールを共有するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Pools] (プール) を選択します。
3. デフォルトでは、デフォルトのプライベートスコープが選択されます。デフォルトのプライベートスコープを使用しない場合は、コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組み を参照してください。
4. コンテンツペインで、共有したいプールを選択し、[Actions] (アクション) > [View details] (詳細を表示) を選択します。
5. [Resource sharing] (リソース共有) で [Create resource share] (リソース共有の作成) を選択します。その結果、AWS RAM コンソールが開きます。共有プールは AWS RAM 上に作成します。
6. [リソースの共有の作成] を選択します。
7. 共有リソースの [Name] (名前) を追加します。
8. [Select resource type] (リソースタイプの選択) で [IPAM pools] (IPAM プール) を選択し、1 つ以上の IPAM プールを選択します。
9. [次へ] を選択します。
10. リソース共有の許可の 1 つを選択します。

    - AWSRAMDefaultPermissionsIpamPool: プリンシパルが共有 IPAM プール内の CIDR および割り当てを表示し、プール内の CIDR の割り当て/割り当て解除できるようにするには、この許可を選択します。
    - AWSRAMPermissionIpamPoolByoipCidrImport: プリンシパルが共有 IPAM プールに BYOIP CIDR をインポートできるようにするには、この許可を選択します。この許可が必要になるのは、既存の BYOIP CIDR があり、それらを IPAM にインポートしてプリンシパルと共有する場合のみです。IPAM への BYOIP CIDR の転送の詳細については、チュートリアル: BYOIP IPv4 CIDR を IPAM に転送する を参照してください。

11. このリソースへのアクセスを許可するプリンシパルを選択します。プリンシパルが既存の BYOIP CIDR をこの共有 IPAM プールにインポートする場合は、BYOIP CIDR 所有者アカウントをプリンシパルとして追加します。
12. リソース共有オプションと共有先のプリンシパルを確認し、[Create] (作成) を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。そこには、コマンドの実行時に使用できるオプションの詳細な説明があります。

RAM を使用して IPAM プールを共有するには、次の AWS CLI コマンドを使用します。

1. IPAM の ARN を取得: describe-ipam-pools
2. リソース共有を作成: create-resource-share
3. リソース共有を表示: get-resource-share

RAM でリソース共有を作成した結果、他のプリンシパルは、IPAM プールを使用してリソースに CIDR を割り当てることができるようになりました。プリンシパルによって作成されたリソースのモニタリングの詳細については、リソースごとに CIDR の使用状況をモニタリングする を参照してください。VPC を作成し、共有 IPAM プールの CIDR を割り当てる方法の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」を参照してください。

リソース検出を使用する

リソース検出は、リソース検出を所有するアカウントに属するリソースを IPAM が管理およびモニタリングできるようにする IPAM コンポーネントです。これにより、IPAM はワークロード全体における IP アドレスの使用状況の最新インベントリを維持することができ、IP アドレスの管理と計画が容易になります。

リソース検出は、IPAM の作成時にデフォルトで作成されます。IPAM とは別個にリソース検出を作成して、別のアカウントまたは組織が所有する IPAM に統合することもできます。リソース検出所有者が組織の委任管理者である場合、IPAM はその組織のすべてのメンバーのリソースを監視します。

> **Note**
>
> リソース検出の作成、共有、および関連付けは、IPAM を組織外のアカウントに統合するプロセスの一環です (「IPAM を組織外のアカウントに統合する」を参照)。IPAM を作成して、

それを組織外のアカウントに統合しない場合は、リソース検出を作成、共有、または関連付ける必要はありません。

このセクションは、リソース検出の操作に関連する手順をまとめたものであることに留意してください。

内容

別の IPAM と統合するリソース検出を作成する

このセクションでは、リソース検出の作成方法を説明します。リソース検出は、IPAM の作成時にデフォルトで作成されます。リソース検出のリージョンあたりのデフォルトクォータは 1 です。IPAM クォータの詳細については、「IPAM のクォータ」を参照してください。

Note

リソース検出の作成、共有、および関連付けは、IPAM を組織外のアカウントに統合するプロセスの一環です (「IPAM を組織外のアカウントに統合する」を参照)。IPAM を作成して、それを組織外のアカウントに統合しない場合は、リソース検出を作成、共有、または関連付ける必要はありません。

IPAM を組織外のアカウントに統合している場合、このステップは、セカンダリ組織の管理者アカウントが完了する必要がある必須のステップです。このプロセスに関与する役割の詳細については、「プロセスの概要」を参照してください。

AWS Management Console

リソース検出を作成する

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで [リソース検出] を選択します。
3. [リソース検出を作成] を選択します。
4. [Amazon VPC IP Address Manager がソースアカウントから IPAM 委任アカウントにデータをレプリケートすることを許可します] を選択します。このオプションを選択しなければ、リソース検出を作成することはできません。
5. (オプション) リソース検出に [名前] タグを追加します。タグとは、AWS リソースに割り当てるラベルです。各タグはキーとオプションの値で構成されます。タグを使用して、リソースを検索してフィルタリングしたり、AWS コストを追跡したりできます。
6. (オプション) 説明を入力します。
7. [運用リージョン] で、リソースが検出される AWS リージョンを選択します。現在のリージョンが、運用リージョンの 1 つとして自動的に設定されます。運用リージョン `us-east-1` 内の IPAM と共有できるようにリソース検出を作成している場合は、ここで `us-east-1` を選択するようにしてください。運用リージョンを忘れた場合は、後ほどこのページに戻って、リソース検出の設定を編集することができます。

   > **Note**
   >
   > ほとんどの場合、リソース検出には IPAM と同じ運用リージョンを使用する必要があります。そうしなければ、その 1 つのリージョンのみでリソース検出が行われることになります。

8. (オプション) プール用の追加の [タグ] を選択します。
9. [作成] を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

- リソース検出を作成する: create-ipam-resource-discovery

リソース検出の詳細を表示する

AWS IPAM でリソース検出の詳細を表示すると、次のような有益なインサイトが得られます。

- インポートされた特定の AWS リソースと、それに関連付けられた IP アドレスの割り当ての特定。
- リソース検出プロセスのステータスと進行状況のモニタリング。
- IPAM と検出されたリソースの間の問題または齟齬のトラブルシューティング。
- IP アドレスの使用状況と傾向の分析。

この情報は、IP アドレス管理を最適化し、IPAM と実際のリソースデプロイ間の整合性を確保するのに役立ちます。

AWS Management Console

リソース検出の詳細を表示する

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで [リソース検出] を選択します。
3. リソース検出を選択します。
4. [リソース検出の詳細] で、リソース検出に関連する詳細を確認します。これには、リソース検出がデフォルトかどうかを示す [デフォルト] などがあります。デフォルトのリソース検出は、IPAM を作成したときに自動的に作成されたリソース検出です。
5. このタブで、リソース検出の詳細を確認します。

    - [検出されたリソース] – リソース検出で監視されているリソース。IPAM は、VPC、パブリック IPv4 プール、VPC サブネット、および Elastic IP アドレスのリソースタイプからの CIDR を監視します。
        - [名前 (リソース ID)] – リソース検出 ID。
        - [割り当てられた IP] – 使用されている IP アドレススペースの割合。小数を割合 (%) に変換するには、小数に 100 を掛けます。次の点に注意してください。
            - リソースが VPC の場合、これはサブネット CIDR が使用している VPC 内の IP アドレス空間の割合になります。
            - リソースがサブネットで、サブネットに IPv4 CIDR がプロビジョニングされている場合、これは使用中のサブネット内の IPv4 アドレス空間の割合です。サブネットに IPv6 CIDR がプロビジョニングされている場合、使用中の IPv6 アドレス空間の割合

は表示されません。使用中の IPv6 アドレス空間の割合は、現在のところ計算できません。

- リソースがパブリック IPv4 プールの場合、これはプール内の IP アドレス空間のうち、Elastic IP アドレス (EIP) に割り振られた空間の割合になります。

- [CIDR] – リソース CIDR。
- [リージョン] – リソースリージョン。
- [所有者 ID] – リソース所有者 ID。
- [サンプル時間] – 最後に成功したリソース検出の時間。

- [検出されたアカウント]: リソース検出の監視対象となっている AWS アカウント。IPAM を AWS Organizations に統合した場合は、組織内のすべてのアカウントが検出されたアカウントになります。
  - [アカウント ID] – アカウント ID。
  - [リージョン] – アカウント情報の取得元である AWS リージョン。
  - [前回検出を試みた日時] – 最後に試行されたリソース検出の時間。
  - [前回発見に成功した日時] – 最後に成功したリソース検出の時間。
  - [ステータス] – リソース検出が失敗した理由。
- [運用リージョン] – リソース検出の運用リージョン。
- [リソース共有] – リソース検出が共有されている場合、リソース共有 ARN のリストが表示されます。
  - [リソース共有 ARN] – リソース共有 ARN。
  - [ステータス] – リソース共有の現在のステータス。可能な値は以下のとおりです。
    - [アクティブ] – リソース共有がアクティブで利用可能です。
    - [削除済み] – リソース共有が削除されており、使用できなくなっています。
    - [保留中] – リソース共有の承諾を求める招待への応答を待っています。
  - [作成日] – リソース共有が作成された日時。
- [タグ] – タグとは、ユーザーが AWS リソースに割り当てるラベルです。各タグはキーとオプションの値で構成されます。タグを使用して、リソースを検索してフィルタリングしたり、AWS コストを追跡したりできます。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

- リソース検出の詳細を表示する: describe-ipam-resource-discoveries

リソース検出を別の AWS アカウントと共有する

このセクションの手順に従って、AWS Resource Access Manager を使用してリソース検出を共有します。AWS RAM の詳細については、「AWS RAM ユーザーガイド」の「AWS リソースの共有」を参照してください。

> **Note**
>
> リソース検出の作成、共有、および関連付けは、IPAM を組織外のアカウントに統合するプロセスの一環です (「IPAM を組織外のアカウントに統合する」を参照)。IPAM を作成して、それを組織外のアカウントに統合しない場合は、リソース検出を作成、共有、または関連付ける必要はありません。

組織外のアカウントを監視する IPAM アカウントを作成すると、セカンダリ組織の管理者アカウントは AWS RAM を使用して、そのリソース検出をプライマリ組織の IPAM アカウントと共有します。プライマリ組織の IPAM アカウントがリソース検出をその IPAM に関連付ける前に、まずリソース検出をプライマリ組織の IPAM アカウントと共有する必要があります。このプロセスに関与する役割の詳細については、「プロセスの概要」を参照してください。

> **Note**
>
> - リソース検出を共有するために AWS RAM を使用してリソース検出を作成するときは、プライマリ組織の IPAM のホームリージョン内にリソース共有を作成する必要があります。
> - リソース検出用のリソース共有を作成および削除するアカウントでは、IAM ポリシーに以下の許可が必要です。
>   - ec2:PutResourcePolicy
>   - ec2:DeleteResourcePolicy
> - リソース検出を別のアカウントと共有する場合、そのアカウントはリソース検出の OU 除外を確認できます。これには、リソース検出所有者の組織の組織 ID、ルート ID、組織単位 ID などの情報が含まれます。

IPAM を組織外のアカウントに統合している場合、このステップは、セカンダリ組織の管理者アカウントが完了する必要がある必須のステップです。

AWS Management Console

リソース検出を共有する

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで [リソース検出] を選択します。
3. [リソース共有]」タブを選択します。
4. [リソースの共有の作成] を選択します。AWS RAM コンソールが開きます。リソース共有はここで作成します。
5. AWS RAM コンソールで、[設定] を選択します。
6. [AWS Organizations との共有を有効にする] を選択してから [設定の保存] を選択します。
7. [リソースの共有の作成] を選択します。
8. 共有リソースの [名前] を追加します。
9. [リソースタイプを選択] で [IPAM リソース検出]] を選択し、リソース検出を選択します。
10. [次へ] を選択します。
11. [許可を関連付ける] では、このリソース共有へのアクセス権を付与されるプリンシパルに対して有効化されるデフォルトの許可を確認できます。
    - AWSRAMPermissionIpamResourceDiscovery
    - この許可で可能になるアクション:
      - ec2:AssociateIpamResourceDiscovery
      - ec2:GetIpamDiscoveredAccounts
      - ec2:GetIpamDiscoveredPublicAddresses
      - ec2:GetIpamDiscoveredResourceCidrs
12. 共有リソースへのアクセスが許可されるプリンシパルを指定します。[プリンシパル] でプライマリ組織の IPAM アカウントを選択してから、[追加] を選択します。
13. [次へ] を選択します。
14. リソース共有オプションと、共有先のプリンシパルを確認します。確認後、[リソースの共有の作成] を選択します。

15. リソース検出の共有後は、プライマリ組織の IPAM アカウントがその共有を承諾してから、それを IPAM に関連付ける必要があります。詳細については、「リソース検出を IPAM に関連付ける」を参照してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

1. リソース共有を作成する: create-resource-share
2. リソース共有を表示: get-resource-share

リソース検出を IPAM に関連付ける

このセクションでは、リソース検出を IPAM に関連付ける方法を説明します。リソース検出を IPAM に関連付けると、この IPAM が、リソース検出で検出されたすべてのリソース CIDR とアカウントを監視します。IPAM を作成するときは、IPAM 用のデフォルトリソース検出が作成され、IPAM に自動的に関連付けられます。

リソース検出の関連付けのデフォルトクォータは 5 個です。詳細については (このクォータの調整方法を含む)、「IPAM のクォータ」を参照してください。

> **Note**
>
> リソース検出の作成、共有、および関連付けは、IPAM を組織外のアカウントに統合するプロセスの一環です (「IPAM を組織外のアカウントに統合する」を参照)。IPAM を作成して、それを組織外のアカウントに統合しない場合は、リソース検出を作成、共有、または関連付ける必要はありません。

IPAM を組織外のアカウントに統合している場合、このステップは、プライマリ組織の IPAM アカウントが完了する必要がある必須のステップです。このプロセスに関与する役割の詳細については、「プロセスの概要」を参照してください。

AWS Management Console

リソース検出を関連付ける

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。

2. ナビゲーションペインで、[IPAM] を選択します。
3. [関連付けられた検出] を選択してから、[リソース検出を関連付ける] を選択します。
4. [IPAM リソース検出] で、[セカンダリ組織の管理者アカウント] が共有したリソース検出を選択します。
5. [関連付ける] を選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

- リソース検出を関連付ける: associate-ipam-resource-discovery

リソース検出の関連付けを解除する

このセクションでは、IPAM からリソース検出との関連付けを解除する方法を説明します。IPAM からリソース検出との関連付けを解除すると、IPAM はリソース検出で検出されたすべてのリソース CIDR とアカウントを監視しなくなります。

> **Note**
>
> デフォルトのリソース検出の関連付けを解除することはできません。デフォルトのリソース検出の関連付けは、IPAM の作成時に自動的に作成される関連付けですが、IPAM を削除すると、デフォルトのリソース検出の関連付けも削除されます。

このステップは、プライマリ組織の IPAM アカウントが完了する必要があります。このプロセスに関与する役割の詳細については、「プロセスの概要」を参照してください。

AWS Management Console

リソース検出の関連付けを解除する

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[IPAM] を選択します。
3. [関連付けられた検出] を選択してから、[リソース検出の関連付けを解除] を選択します。

4. [IPAM リソース検出] で、[セカンダリ組織の管理者アカウント] が共有したリソース検出を選択します。
5. [関連付け解除] を選択してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

- リソース検出の関連付けを解除する: disassociate-ipam-resource-discovery

リソース検出を削除する

このセクションでは、リソース検出を削除する方法を説明します。

> **Note**
> デフォルトのリソース検出を削除することはできません。デフォルトのリソース検出は、IPAM の作成時に自動的に作成されるリソース検出ですが、IPAM を削除すると、デフォルトのリソース検出も削除されます。

このステップは、セカンダリ組織の管理者アカウントが完了する必要があります。このプロセスに関与する役割の詳細については、「プロセスの概要」を参照してください。

AWS Management Console

リソース検出を削除する

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで [リソース検出] を選択します。
3. リソース検出を選択し、[アクション] > [リソース検出を削除] の順に選択します。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

- リソース検出を削除する: delete-ipam-resource-discovery

IPAM での IP アドレス使用状況の追跡

Amazon VPC IP Address Manager は、IP アドレスの使用状況を追跡する機能があり、複雑なネットワーク環境を管理するすべてのユーザーにメリットをもたらします。IPAM は、AWS 全体の IP アドレスの割り当て、使用状況、消費の傾向を可視化します。これは、未使用または非効率的に使用されている IP アドレスを特定し、アドレス空間を最適化して、潜在的な IP アドレスの枯渇を防ぐのに役立ちます。

IPAM は、CIDR、スコープ、IPAM レベルで IP アドレスの使用状況を追跡し、詳細なレポートと分析を提供します。これは、大規模なデプロイ、マルチアカウント設定、進化するネットワーク要件にとって重要です。

IPAM の使用状況の追跡を活用することで、十分な情報に基づいた意思決定を行い、IP アドレス管理を改善し、IP リソースを効率的に使用できるようになります。

> **Note**
>
> このセクションの設定はオプションです。IPAM アカウントを委任している場合は、このセクションのタスクを完了するには、タスクは IPAM アカウントで完了する必要があります。

内容

IPAM ダッシュボードで CIDR の使用状況をモニタリングする

Amazon VPC IP Address Manager の IPAM ダッシュボードでは、いくつかの主要なシナリオで CIDR の使用状況をモニタリングできます。

- 未使用の IP アドレス空間または使用率の低い IP アドレス空間を特定する: ダッシュボードは CIDR の使用状況に関する可視性を提供するため、ユーザーは再利用または再割り当てできる使用可能なキャパシティを持つ CIDR を識別できます。

- IP アドレス管理を最適化する: CIDR の使用状況を詳細に追跡することで、変化するビジネスおよびインフラストラクチャの要件を満たすための IP アドレスブロックの拡張、縮小、再割り当てについて、十分な情報に基づいた意思決定を行うことができます。
- IP アドレスの枯渇を防ぐ: CIDR の使用状況のモニタリングは、IP アドレス空間を追加で取得する必要があるかもしれない時期を予測するのに役立ちます。これにより、IP アドレスの枯渇によるサービスの中断をプロアクティブに計画したり、回避したりできます。
- コンプライアンスとガバナンスを実現する: IPAM ダッシュボードは、IP アドレス管理に関する規制要件または社内ポリシーを満たすために、IP アドレスの使用パターンを明らかにするのに役立ちます。
- ネットワークに関する問題をトラブルシューティングする: CIDR の詳細な使用状況データは、ネットワーク接続の問題やリソースの競合の根本原因を特定するのに役立ちます。

IPAM ダッシュボードを通じて CIDR の使用状況を詳細にモニタリングすることで、AWS 内の IP アドレス管理の効率、回復力、コンプライアンスを強化できます。

AWS Management Console

IPAM ダッシュボードで CIDR の使用状況をモニタリングするには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、ダッシュボードを選択します。
3. デフォルトでは、ダッシュボードを表示すると、デフォルトのプライベートスコープが選択されます。デフォルトのプライベートスコープを使用しない場合は、コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
4. ダッシュボードには、スコープ内の IPAM プールと CIDR の概要が表示されます。ウィジェットを追加、削除、サイズ変更、移動してダッシュボードをカスタマイズできます。

    - [Scope] (スコープ): このスコープの詳細。スコープは IPAM 内の最上位のコンテナです。IPAM には 2 つのデフォルトスコープが含まれています。1 つはプライベート、もう 1 つはパブリックです。各スコープは、単一のネットワークの IP 空間を表します。プライベートスコープは複数保持できますが、パブリックスコープは 1 つに限られます。
        - [Scope ID] (スコープ ID): このスコープのID。
        - [Scope type] (スコープタイプ): スコープのタイプ。
        - [IPAM ID]: スコープが属している IPAM の ID。

    - [このスコープ内の IPAM プール]: スコープが属している IPAM の ID。
    - [このスコープ内のネットワークリソースを表示]: IPAM コンソールの [リソース] セクションに移動します。
    - [このスコープ内の IP アドレスの履歴を検索]: IPAM コンソールの [IP 履歴の検索] セクションに移動します。
- [リソース CIDR タイプ]: スコープ内のリソース CIDR のタイプ。
    - [サブネット]: サブネットの CIDR の数。
    - [VPC]: VPC の CIDR の数。
    - [EIP]: Elastic IP アドレスの CIDR の数。
    - [パブリック IPv4 プール]: パブリック IPv4 プールの CIDR の数。
- [管理状態]: CIDR の管理状態。
    - [Unmanaged CIDRs] (アンマネージド CIDR): このスコープ内のアンマネージドリソースのリソース CIDR の数。
    - [Ignored CIDRs] (無視された CIDR): スコープ内の IPAM によるモニタリングから除外するように選択したリソース CIDR の数。無視されたリソースは、スコープ内での重複またはコンプライアンスについて評価されません。リソースが無視されるように選択されると、IPAM プールからリソースに割り当てられたスペースはすべてプールに返され、リソースは自動インポートを介して再度インポートされません (自動インポートの割り当てルールがプールに設定されている場合)。
    - [Managed CIDRs] (マネージド CIDR): スコープ内の IPAM プールから割り当てられた、管理可能なリソース (VPC またはパブリック IPv4 プール) のリソース CIDR の数。
- [重複するリソース CIDR]: 重複する CIDR と重複しない CIDR の数。CIDR が重複していると、VPC のルーティングに誤りが生じる恐れがあります。
    - [Overlapping CIDRs] (重複しているCIDR): このスコープ内の IPAM プール内で現時点で重複しているリソース CIDR の数。CIDR が重複していると、VPC のルーティングに誤りが生じる恐れがあります。
    - [重複しない CIDR]: このスコープ内の IPAM プール内で重複しないリソース CIDR の数。
- [準拠リソース CIDR]: 準拠リソース CIDR の数。
    - [Compliant CIDR] (準拠 CIDR): スコープ内の IPAM プールの割り当てルールに準拠しているリソース CIDR の数。
    - [Noncompliant CIDRs] (非準拠 CIDR): スコープ内の IPAM プールの割り当てルールに準拠していないリソース CIDR の数。

- [重複ステータス]: 時間の経過と共に重複する CIDR の数。
  - [OverlappingResourceCidrs]: このスコープ内の IPAM プール内で重複しているリソース CIDR の数。CIDR が重複していると、VPC のルーティングに誤りが生じる恐れがあります。
- [コンプライアンスステータス]: 時間の経過と共にスコープ内の IPAM プールの割り振りルールに準拠する CIDR と準拠しない CIDR の数。
  - [CompliantResourceCidrs]: 割り振りルールに準拠しているリソース CIDR の数。
  - [NoncompliantResourceCidrs]: 割り振りルールに準拠していないリソース CIDR の数。
- [VPC の使用率]: IP 使用率が最も高い、または最も低い VPC (IPv4 および IPv6) です。この情報を使用すると、IP 使用率のしきい値を超えた場合に警告する Amazon CloudWatch アラームを設定できます。詳細については、「IPAM リソース使用率メトリクス」を参照してください。
- [サブネットの使用率]: IP 使用率が最も高い、または最も低いサブネット (IPv4 のみ) です。この情報を使用すると、使用率の低いリソースを残すか削除するかを決定できます。詳細については、「IPAM リソース使用率メトリクス」を参照してください。
- [最も多くの IP が割り当てられている VPC]: サブネットに割り振られた IP アドレス空間の割合が最も高い VPC。これは、VPC に追加の IP アドレス空間をプロビジョニングする必要があるかどうかを示すのに役立ちます。
- [最も多くの IP が割り当てられているサブネット]: リソースに割り振られた IP アドレス空間の割合が最も高いサブネット。これは、サブネットに追加の IP アドレス空間をプロビジョニングする必要があるかどうかを示すのに役立ちます。
- [プールの割り当て]: 時間の経過と共にスコープ内のリソースおよび手動割り振りに割り当てられた IP スペースの割合。
- [プールの割り振り]: 時間の経過と共にスコープ内の他のプールに割り振られたプールの IP スペースの割合。

Command line

ダッシュボードに表示される情報は、Amazon CloudWatch に保存されているメトリクスから取得されます。Amazon CloudWatch に保存されたメトリクスの詳細については、「Amazon CloudWatch で IPAM をモニタリングする」を参照してください。AWS CLI リファレンスの Amazon CloudWatch オプションを使用して、IPAM プールおよびスコープ内の割り当てのメトリクスを表示します。

プール用にプロビジョニングされた CIDR がほぼ完全に割り当てられている場合は、追加の CIDR をプロビジョニングすることが必要な場合があります。(詳しくは、「CIDR をプールにプロビジョニングする」を参照してください。)

リソースごとに CIDR の使用状況をモニタリングする

Amazon VPC IP Address Manager の [リソース] ビューでは、AWS リソース全体の IP アドレスの使用状況の概要を一元的に把握できます。これにより、IP アドレスを消費しているリソースを迅速に特定し、アドレス割り当ての傾向を追跡して、進化するインフラストラクチャとビジネスニーズに合わせて IP アドレス管理を最適化できます。

IPAM では、リソースとは、IP アドレスまたは CIDR ブロックが割り当てられている AWS サービスエンティティのことです。IPAM は一部のリソースを管理しますが、他のリソースについてはモニタリングのみを行うため、この 2 つの違いを理解することが重要です。

- マネージドリソース: マネージドリソースには、IPAM プールから CIDR が割り当てられています。IPAM は、CIDR をモニタリングして、他の CIDR との IP アドレスの重複がないかどうかを確認します。また、プールの割り当てルールに対する CIDR のコンプライアンスをモニタリングします。IPAM では、次のタイプのリソースの管理がサポートされています。
  - Elastic IP アドレス
  - パブリック IPv4 プール

    > **Note**
    >
    > パブリック IPv4 プールと IPAM プールは、別個の AWS リソースによって管理されます。パブリック IPv4 プールは、パブリック所有の CIDR を Elastic IP アドレスに変換できるようにする単一のアカウントリソースです。IPAM プールは、パブリック空間をパブリック IPv4 プールに割り当てるために使用できます。

  - VPC
- モニタリング対象リソース: リソースが IPAM によってモニタリングされている場合、リソースは IPAM によって検出され、AWS CLI で `get-ipam-resource-cidrs` を使用したとき、またはナビゲーションペインの [Resources] (リソース) を表示したときに、リソースの CIDR に関する詳細が表示されます。IPAM は、次のリソースのモニタリングをサポートしています。
  - Elastic IP アドレス
  - パブリック IPv4 プール
  - VPC

- VPC サブネット

AWS Management Console

リソースごとに CIDR の使用状況をモニタリングするには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[リソース] を選択します。
3. コンテンツペインの上部にある IP ドロップダウンメニューから、使用する IP アドレスプロトコル (IPv4 または IPv6) を選択します。
4. コンテンツペインの上部にあるスコープドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
5. リソース CIDR マップを使用すると、スコープ内の使用可能な IP アドレス空間、割り当てられた IP アドレス空間、重複する IP アドレス空間を確認できます。

   - [使用可能]: IP アドレス範囲を割り当てることができます。
   - [準拠していて重複しない]: IP アドレス範囲は IPAM によって管理されるリソースに割り当てられます。
   - 占有中: IP アドレス範囲がリソースに割り当てられます。
   - 重複: IP アドレス範囲が複数のリソースに割り当てられていて、重複しています。
   - 非準拠: IP アドレス範囲が準拠していません。IP アドレス範囲を使用しているリソースが、プールに設定されている割り当てルールに準拠していません。

   CIDR マップで、マップの下部にある IP アドレスブロックを選択すると、リソースがより小さな CIDR ブロックで表示されます。マップの上部にある IP アドレスブロックを選択すると、リソースがより大きな CIDR ブロックで表示されます。
6. この表には、スコープ内のリソースに関する次の詳細が表示されます。

   - 名前 (リソース ID): リソースの名前とリソース ID です。
   - CIDR: リソースに関連付けられている CIDR。
   - 管理ステータス: リソースのステータス。
     - マネージド： リソースには、IPAM プールから割り当てられた CIDR があり、IPAM によって、CIDR の重複がないかどうか、およびプール割り当てルールへのコンプライアンスをモニタリングされています。

  - アンマネージド: リソースには、IPAM プールから割り当てられた CIDR がなく、IPAM によって、CIDR の重複がないかどうか、およびプール割り当てルールへのコンプライアンスをモニタリングされていません。CIDR は重複について監視されます。
  - 無視: リソースはモニタリングの対象外として選択されています。無視されたリソースは、重複または割り当てルールへのコンプライアンスについて評価されません。リソースが無視されるように選択されると、IPAM プールからリソースに割り当てられたスペースはすべてプールに返され、リソースは自動インポートを介して再度インポートされません (自動インポートの割り当てルールがプールに設定されている場合)。
  - [-]: このリソースは、IPAM が管理できるリソースタイプではありません。
- コンプライアンスのステータス: CIDR のコンプライアンスのステータス。
  - 準拠: マネージドリソースは、IPAM プールの割り当てルールに準拠しています。
  - [Noncompliant] (非準拠): リソース CIDR は、IPAM プールの 1 つ以上の割り当てルールに準拠していません。

    Example

    VPC に IPAM プールのネットマスク長パラメータを満たさない CIDR がある場合、またはリソースが IPAM プールと同じ AWS リージョンにない場合、非準拠としてフラグが設定されます。
  - [UnManaged] (アンマネージド): リソースには、IPAM プールから割り当てられた CIDR がなく、IPAM によって、CIDR の重複がないかどうか、およびプール割り当てルールへのコンプライアンスが監視されていません。CIDR は重複について監視されます。
  - 無視: リソースはモニタリングの対象外として選択されています。無視されたリソースは、重複または割り当てルールへのコンプライアンスについて評価されません。リソースが無視されるように選択されると、IPAM プールからリソースに割り当てられたスペースはすべてプールに返され、リソースは自動インポートを介して再度インポートされません (自動インポートの割り当てルールがプールに設定されている場合)。
  - [-]: このリソースは、IPAM が管理できるリソースタイプではありません。
- 重複ステータス: CIDR の重複ステータス。
  - 重複していない: リソース CIDR は同じスコープ内の別の CIDR と重複していません。
  - 重複している: リソース CIDR は同じスコープ内の別の CIDR と重複しています。リソース CIDR が重複している場合は、手動割り当てと重複している可能性があることに注意してください。
  - 無視: リソースはモニタリングの対象外として選択されています。無視されたリソースは、IPAM では、重複または割り当てルールへのコンプライアンスについて評価されま

せん。リソースが無視されるように選択されると、IPAM プールからリソースに割り当てられたスペースはすべてプールに返され、リソースは自動インポートを介して再度インポートされません (自動インポートの割り当てルールがプールに設定されている場合)。

  - [-]: このリソースは、IPAM が管理できるリソースタイプではありません。
- [割り当てられた IP]: リソースが VPC である場合、これはサブネット CIDR が使用している VPC 内の IP アドレススペースの割合です。リソースがサブネットで、サブネットに IPv4 CIDR がプロビジョニングされている場合、これは使用中のサブネット内の IPv4 アドレス空間の割合です。サブネットに IPv6 CIDR がプロビジョニングされている場合、使用中の IPv6 アドレス空間の割合は表示されません。使用中の IPv6 アドレス空間の割合は、現在のところ計算できません。リソースがパブリック IPv4 プールの場合、これはプール内の IP アドレス空間のうち、Elastic IP アドレス (EIP) に割り振られた空間の割合になります。
- [Region] (リージョン): リソースの AWS リージョン。
- [Owner ID] (所有者 ID): このリソースを作成したユーザーの AWS アカウント ID。
- [リソースタイプ]: リソースが VPC、サブネット、Elastic IP アドレス、パブリック IPv4 プールのいずれであるか。
- プール ID: リソースが存在する IPAM プールの ID。

7. [リソースをフィルタする] を使用して、VPC ID やコンプライアンスステータスなどの列プロパティでリソーステーブルをフィルタリングします。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳細な説明が記載されています。

リソース別に CIDR の使用状況をモニタリングするには、次の AWS CLI コマンドを使用します。

1. スコープ ID を取得する: describe-ipam-scopes
2. リソース情報をリクエストする: get-ipam-resource-cidrs

Amazon CloudWatch で IPAM をモニタリングする

IPAM では、IP アドレス使用とリソース使用率に関連するメトリクス (IPAM プールで使用可能な IP アドレス空間や、割り当てルールに準拠しているリソース CIDR の数など) が IPAM のホームリージョン内の `AWS/IPAM` Amazon CloudWatch 名前空間に自動的に保存されます。

IPAM を CloudWatch と統合することで、AWS 内の IP アドレス管理をモニタリング、分析、最適化する機能が強化されます。

ユースケースを以下に示します。

- IP アドレスの使用状況の傾向の追跡: CloudWatch は CIDR プールの使用状況、スコープの割り当て、および他の IPAM メトリクスをモニタリングできるため、IP アドレスが枯渇する潜在的なリスクをプロアクティブに特定できます。
- 使用状況ベースのアラートの設定: CIDR の使用状況が事前定義されたしきい値に達したときに通知するように CloudWatch アラームを設定して、適時の介入と最適化を実現できます。
- IPAM イベントのモニタリング: CloudWatch は、CIDR の割り当て、割り当ての解除、スコープの変更などの IPAM 関連のイベントをキャプチャして分析し、IP アドレス管理アクティビティを可視化できます。
- カスタムダッシュボードの生成: IPAM データと他の AWS メトリクスを組み合わせることで、包括的なダッシュボードを作成して、関連するインフラストラクチャやパフォーマンス指標とともに IP アドレスのランドスケープを視覚化および分析できます。

内容

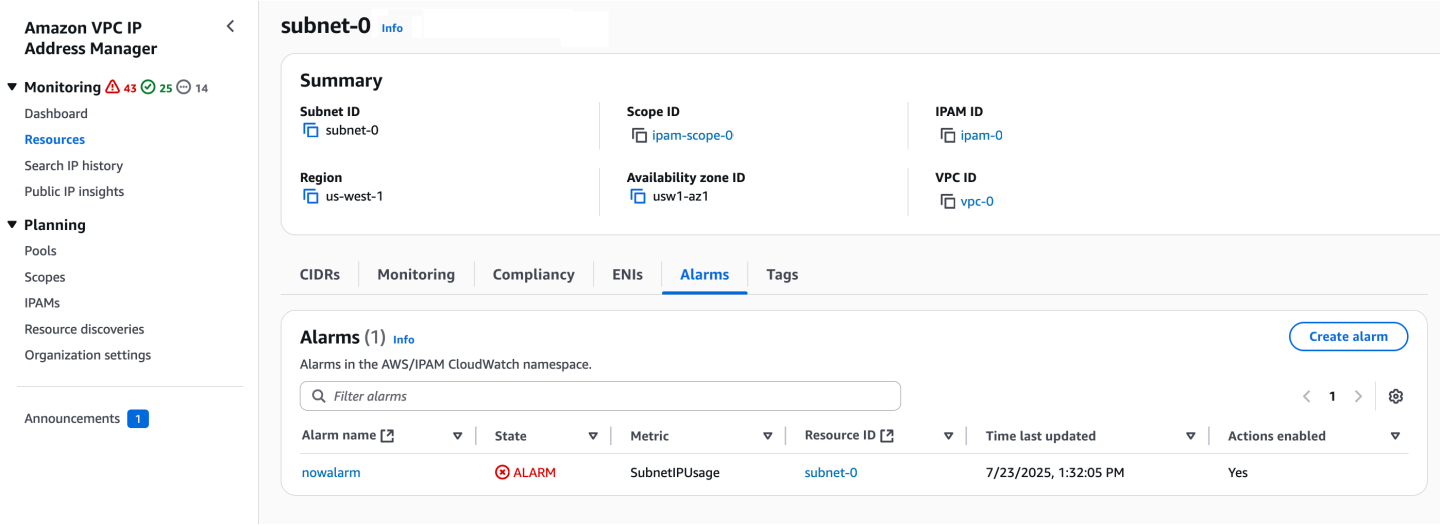
IPAM コンソールからアラームを管理する

Amazon CloudWatch アラームの作成と管理は、IPAM コンソールから直接実行できます。INSUFFICIENT_DATA または ALARM 状態になっている IPAM メトリクス または IPAM リソース使用率メトリクス のアラームは、コンソール上部に警告バーとして表示、および左側にあるナビゲーションの [モニタリング] の横にビジュアルインジケータとして表示されます。

特定のリソースのアラームを管理するには、[リソース] を選択してから、VPC、サブネット、またはプールを選択します。リソースの詳細ページが開いたら、[アラーム] タブを選択します。

[アラーム] タブには、選択したリソースに関連付けられているすべての CloudWatch アラームが表示されます。このタブから、アラーム詳細の表示や現行状態の監視を行い、アラーム設定オプションにアクセスすることができます。タブには、表示しているリソースに関連する AWS/IPAM 名前空間からのアラームが表示されます。

以下のスクリーンショットは、IPAM コンソールのアラーム管理インターフェイスの画像です。



[アラーム] タブでは、IPAM のホームリージョン内の AWS/IPAM Amazon CloudWatch 名前空間にある CloudWatch アラームの詳しい概要を確認できます。

- アラーム名: ユーザー定義の CloudWatch アラーム名です。
- 状態: CloudWatch アラームの現在の状態です。
  - ALARM: メトリクスが定義されたしきい値を超えています。
  - OK: メトリクスは定義されたしきい値内です。
  - INSUFFICIENT_DATA: アラーム状態を判断するのに十分なデータがありません。
- メトリクス: アラームが監視している特定の CloudWatch メトリクスです。
- リソース ID: アラームが監視している AWS リソースの一意識別子です。
- 最終更新日時: アラーム状態が最後に変更または評価された日時です。
- アクション有効: アラームに対して CloudWatch アクションが有効化されているかどうかを示します。
  - はい: 条件が満たされたときにアラームが設定されたアクションをトリガーできます。
  - いいえ: アラームが監視を行っていますが、アクションは実行していません。

さらに、VPC、サブネット、またはプールの [モニタリング] タブで使用率グラフを確認している場合は、リソース使用率のアラームを作成するオプションを選択できます。選択すると、リソースとメトリクスの詳細が事前に入力されている CloudWatch コンソールにリダイレクトされます。コンソールからアラームのしきい値を設定できます。例えば、使用率が特定の割合に達したときに通知を受けるなどです。

IPAM メトリクス

IPAM は IPAM、プール、およびスコープに関するデータを Amazon CloudWatch に発行します。これらのメトリックを使用して、アドレスプールが枯渇に近づいているか、リソースがプールに設定された割り当てルールに準拠していない場合に、IP アドレス管理プールのアラームを作成できます。Amazon CloudWatch を使用したアラームの作成と通知の設定は、このセクションの範囲外です。詳細については、『Amazon CloudWatch ユーザーガイド』の「Amazon CloudWatch アラームの使用」を参照してください。

IPAM が Amazon CloudWatch に送信するメトリクスとディメンションを以下に示します。

IPAM メトリクス

AWS/IPAM 名前空間には、次の IPAM メトリクスが含まれます。

メトリクス名	説明
TotalActiveIpCount	アクティブな IP 数の合計はアドバンスト階層に切り替えた場合に課金される IPAM 内のアクティブな IP アドレスの数です。アクティブ IP アドレスは、EC2 インスタンスなどのリソースにアタッチされた Elastic Network Interface (ENI) に関連付けられた IP アドレスまたはプレフィックスとして定義されます。 • このメトリクスは、無料利用枠のお客様にのみご利用いただけます。 • IPAM が AWS Organizations と統合されている場合、アクティブな IP 数はすべての組織アカウントをカバーします。 • アクティブな IP 数の内訳を IP タイプ (パブリック/プライベート) またはクラス (IPv4/IPv6) 別に表示することはできません。 • IPAM は、モニタリング対象アカウントが所有する ENI からの IP のみをカウントします。共有サブネットの数は不正確で

メトリクス名	説明
	ある可能性があります。サブネット所有者または ENI 所有者が IPAM によってカバーされていない場合、IP アドレスは除外されます。

IPAM プールのメトリクス

AWS/IPAM 名前空間には、IPAM の次のプールメトリクスが含まれます。

メトリクス名	説明
CompliantResourceCidrs	IPAM プールの割り振りルールに準拠するマネージドリソース CIDR の数。割り当てルールの詳細については、トップレベル IPv4 プールを作成するを参照してください。
NoncompliantResourceCidrs	IPAM プールの割り振りルールに準拠していないマネージドリソース CIDR の数。割り当てルールの詳細については、トップレベル IPv4 プールを作成するを参照してください。
PercentAllocated	他のプールに割り振られたプールの IP スペースのパーセンテージ (%)。
PercentAssigned	リソースに割り振られているプールの IP スペースの割合 (手動割り振り)。
PercentAvailable	他のプールまたはリソースに割り振られていないプールの IP スペースの割合。

IPAM スコープのメトリクス

AWS/IPAM 名前空間には、IPAM の次のスコープメトリクスが含まれます。

メトリクス名	説明
CompliantResourceCidrs	スコープ内の IPAM プールの割り振りルールに準拠しているリソース CIDR の数。

メトリクス名	説明
ManagedResourceCidrs	スコープ内の IPAM プールから割り振られた、管理可能なリソース (VPC またはパブリック IPv4 プール) のリソース CIDR の数。
NoncompliantResourceCidrs	スコープ内の IPAM プールの割り振りルールに準拠していないリソース CIDR の数。
OverlappingResourceCidrs	スコープ内で重複しているリソース CIDR の数です。
UnmanagedResourceCidrs	管理可能なリソースに現在関連付けられているが、IPAM によって管理されていないスコープ内のリソース CIDR の数。

IPAM パブリック IP メトリクス

AWS/IPAM 名前空間には、IPAM の次のパブリック IP メトリクスが含まれます。

メトリクス名	説明
AmazonOwnedContigIPs	IPAM が所有する Amazon 提供の連続したパブリック IPv4 プールにプロビジョニングされる、CIDR 内の IP アドレスの数。
AllocatedAmazonOwnedContigIPs	Amazon 提供の連続したパブリック IPv4 プール CIDR ブロックから割り当てられた IP アドレスの数。
UnallocatedAmazonOwnedContigIPs	IPAM が所有する Amazon 提供の連続したパブリック IPv4 プール CIDR ブロック内の IP アドレスの数。
AssociatedAmazonOwnedContigIPs	Elastic Network Interface に関連付けられている Amazon 提供の連続したパブリック IPv4 プール CIDR ブロックから割り当てられた Elastic IP アドレスの数。
UnassociatedAmazonOwnedContigIPs	Elastic Network Interface に関連付けられていない Amazon 提供の連続したパブリック IPv4 プール CIDR ブロックから割り当てられた Elastic IP アドレスの数。

IPAM プレフィックスリストリゾルバーメトリクス

IPAM プレフィックスリストリゾルバールールを、バージョンとプレフィックスリストのサイズの制限内に維持するために再評価して調整する必要がある可能性があるため、障害メトリクスに CloudWatch アラームを設定することをお勧めします。

メトリクス名	説明
IpamPrefixListResolverSyncFailure	プレフィックスリストリゾルバーがターゲットとの同期に失敗しました。これは、「プレフィックスリストリゾルバーのバージョンあたりの CIDR エントリ数」などのクォータを超えた場合、ターゲットプレフィックスリストが見つからない場合、またはターゲットマネージドプレフィックスリストで同期が無効になっている場合に発生する可能性があります。
IpamPrefixListResolverSyncSuccess	プレフィックスリストリゾルバーがターゲットと正常に同期されました。
IpamPrefixListResolverVersionCreationSuccess	バージョンの作成に成功しました。
IpamPrefixListResolverVersionCreationFailure	バージョンの作成に失敗しました。これは、「プレフィックスリストリゾルバーのバージョンあたりの CIDR エントリ数」のクォータに達した場合に発生する可能性があります。

メトリクスディメンション

IPAM メトリクスをフィルタリングするには、次のディメンションを使用します。

ディメンション	説明
AddressFamily	リソース CIDR (IPv4 または IPv6) の IP アドレスファミリー。
Locale	IPAM プールを割り振ることができるようにする AWS リージョン。
PoolID	プールの ID。

ディメンション	説明
ScopeID	スコープの ID。

Amazon CloudWatch で VPC をモニタリングする方法については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPC の CloudWatch メトリクス」を参照してください。

IPAM リソース使用率メトリクス

IPAM は、IPAM が監視するリソースの IP 使用率メトリクスを Amazon CloudWatch に発行します。これらのリソースには次のものが含まれます。

- VPC (IPv4 と IPv6)
- サブネット (IPv4)
- パブリック IPv4 プール

IPAM は、IP アドレスファミリー (IPv4 または IPv6) ごとに IP 使用率のメトリクスを個別に計算して発行します。リソースの IP 使用率は、同じアドレスファミリーのすべての CIDR をまたいで計算されます。

IPAM は、リソースタイプとアドレスファミリーの組み合わせごとに、3 つのルールを使用して、発行するメトリクスを決定します。

- IP 使用率が最も高いリソースを最大 50 件。この情報を使用すると、IP 使用率のしきい値を超えた場合に警告するアラームを設定できます。
- IP 使用率が最も低いリソースを最大 50 件。この情報を使用すると、使用率の低いリソースを残すか削除するかを決定できます。
- その他のリソースを最大 50 件。この情報を使用すると、使用率の高いグループまたは低い使用率グループでは取得されないリソースの IP 使用率を一貫して追跡できます。
  - IPAM プールから割り当てられた CIDR を含む VPC を最大 50 件 (CIDR ブロックの合計サイズで優先順位を付ける)。
  - IPAM プールから割り当てられた CIDR が VPC に含まれるサブネットを最大 50 件 (CIDR ブロックの合計サイズで優先順位を付ける)。
  - IPAM プールから割り当てられた CIDR を含むパブリック IPv4 プールを最大 50 件 (CIDR ブロックの合計サイズで優先順位を付ける)。

各ルールを適用した後、各リソースタイプについてメトリクスが集約され、同じメトリクス名で発行されます。メトリクス名とそのディメンションの詳細については、以下を参照してください。

> **Important**
>
> リソースタイプ、アドレスファミリー、ルールの組み合わせにはそれぞれ固有の制限があります。各制限のデフォルト値は 50 です。「AWS 全般のリファレンス」の「AWS サービスクォータ」で説明されているように、AWS サポートセンターに連絡して、これらの制限を調整できます。

Example例

例えば、IPAM が VPC 2,500 件とサブネット 10,000 件を監視していて、そのすべてが IPv4 と IPv6 の CIDR を使用しているとします。IPAM は以下の IP 使用率メトリクスを発行します。

- VPC の IPv4 IP 使用率を最大 150 件。これには以下が含まれます。
  - IPv4 IP 使用率が最も高い VPC 50 件
  - IPv4 の使用率が最も低い VPC 50 件
  - IPAM プールから割り当てられた IPv4 CIDR を含む VPC 最大50 件
- VPC IPv6 の使用率に関するメトリクスを最大 150 件。これには以下が含まれます。
  - IPv6 IP 使用率が最も高い VPC 50 件
  - IPv6 使用率が最も低い VPC 50 件
  - IPAM プールから割り当てられた IPv6 CIDR を含む VPC 最大50 件
- サブネット IPv4 の使用率に関するメトリクスを最大 150 件。これには以下が含まれます。
  - IPv4 IP 使用率が最も高いサブネット 50 件
  - IPv4 IP 使用率が最も低いサブネット 50 件
  - IPAM プールから割り当てられた IPv4 CIDR が VPC に含まれるサブネット最大 50 件

VPC メトリクス

VPC メトリクスの名前と説明を以下に示します。

メトリクス名	説明
VpcIPUsage	VPC のサブネット内における CIDR の対象となる IP の合計を、VPC 内における CIDR の対象となる IP の合計で割ったものです。これは、同じ IPAM スコープ内のすべての VPC CIDR をまたいで、IPv4 CIDR と IPv6 CIDR について別々に計算されます。

VPC メトリクスのフィルタリングに使用できるディメンションを以下に示します。

ディメンション	説明
AddressFamily	リソース CIDR (IPv4 または IPv6) の IP アドレスファミリー。
OwnerID	VPC 所有者の ID。
リージョン	VPC がある AWS リージョン。
ScopeID	VPC が属する IPAM スコープの ID。
VpcID	VPC の ID。

サブネットメトリクス

サブネットメトリクスの名前と説明を以下に示します。

メトリクス名	説明
SubnetIPUsage	アクティブな IP の数をサブネットの IPv4 CIDR の合計 IP 数で割ったものです。

サブネットメトリクスのフィルタリングに使用できるディメンションを以下に示します。

ディメンション	説明
AddressFamily	リソース CIDR (IPv4 のみ) の IP アドレスファミリー。

ディメンション	説明
OwnerID	サブネットの所有者の ID。
リージョン	サブネットがある AWS リージョン。
ScopeID	サブネットが属する IPAM スコープの ID。
SubnetID	サブネットの ID。
VpcID	サブネットが属する VPC の ID。

パブリック IPv4 プールのメトリクス

パブリック IPv4 プールのメトリクスの名前と説明を以下に示します。

メトリクス名	説明
PublicIPv4PoolIPUsage	パブリック IPv4 プールからの EIP の数をプール内の IP の合計で割ったもの。

パブリック IPv4 プールのメトリクスのフィルタリングに使用できるディメンションを以下に示します。

ディメンション	説明
OwnerID	パブリック IPv4 プール所有者の ID
PublicIPv4PoolID	パブリック IPv4 プールの ID
リージョン	パブリック IPv4 プールがある AWS リージョン
ScopeID	パブリック IPv4 プールが属する IPAM スコープの ID

Public IP Insights メトリクス

Public IP Insightsメトリクスの名前と説明は以下のとおりです。

メトリクス名	説明
AmazonOwnedElasticIPs	AWS アカウント内のリソースにプロビジョニング済み、または割り当てられた Amazon 所有の Elastic IP アドレス数。
AssociatedAmazonOwnedElasticIPs	AWS アカウント内の リソースに関連付けられた Amazon 所有の Elastic IP アドレス数。
AssociatedBringYourOwnIPs	Bring your own IP addresses (BYOIP) を使用して AWS に持ち込み、アカウント内のリソースに関連付けたパブリック IPv4 アドレスの数。
BringYourOwnIPs	Bring your own IP addresses (BYOIP) を使用して AWS に持ち込んだパブリック IPv4 アドレスの数。
EC2PublicIPs	インスタンスがデフォルトサブネットまたはパブリック IPv4 アドレスを自動的に割り当てるように設定されたサブネットに起動されたときに、EC2 インスタンスに割り当てられたパブリック IPv4 アドレスの数。
ServiceManagedBringYourOwnIPs	AWS サービスによってプロビジョニングおよび管理されている Bring your own IP addresses (BYOIP) を使用して AWS に持ち込んだパブリック IPv4 アドレスの数。
ServiceManagedIPs	AWS サービスによりプロビジョニングおよび管理されたパブリック IP アドレスの数。
UnassociatedAmazonOwnedElasticIPs	AWS アカウントのリソースにプロビジョニングしていない、Amazon 所有の Elastic IP アドレスの数。
UnassociatedBringYourOwnIPs	Bring your own IP addresses (BYOIP) を使用して AWS に持ち込んだパブリック IPv4 アドレスで、アカウント内のどのリソースにも関連付けられていないアドレスの数。

Public IP Insights のメトリクスのフィルタリングに使用できるディメンションを以下に示します。

ディメンション	説明
IpamId	VPC が属する IPAM の ID。
リージョン	パブリック IPv4 プールがある AWS リージョン。

アラーム作成のクイックヒント

IP アドレスの使用率が高いリソースの Amazon CloudWatch アラームをすばやく作成するには、CloudWatch コンソールを開き、[メトリクス]、[すべてのメトリクス] を選択し、[クエリ] タブを選択し、[名前空間] の `AWS/IPAM > VPC IP Usage Metrics`、`AWS/IPAM > Subnet IP Usage Metrics`、`AWS/IPAM > Public IPv4 Pool IP Usage Metrics` のいずれかを選択し、[メトリクス名] の `MAX(VpcIPUsage)`、`MAX(SubnetIPUsage)`、`MAX(PublicIPv4PoolIPUsage)` のいずれかを選択し、[アラームを作成] を選択します。詳細については、「Amazon CloudWatch ユーザーガイド」の「Metrics Insights クエリでアラームを作成する」を参照してください。

IP アドレス履歴の表示

IPAM スコープ内の IP アドレスまたは CIDR の履歴を表示するには、このセクションのステップに従います。履歴データを使用して、ネットワークセキュリティおよびルーティングポリシーを分析および監査できます。IPAM は、IP アドレス監視データを最大 3 年間自動的に保持します。

IP 履歴データを使用して、次のタイプのリソースの IP アドレスまたは CIDR のステータス変更を検索できます。

- VPC
- VPC サブネット
- Elastic IP アドレス
- EC2 インスタンス
- インスタンスにアタッチされた EC2 ネットワークインターフェイス

Important

IPAM はインスタンスにアタッチされた Amazon EC2 インスタンスまたは EC2 ネットワークインターフェイスを監視しませんが、IP 履歴検索機能を使用して EC2 インスタンスおよびネットワークインターフェイス CIDR 上の履歴データを検索できます。

Note

- ある IPAM スコープから別のスコープにリソースを移動すると、前の履歴レコードが終了し、新しい履歴レコードが新しいスコープの下に作成されます。詳細については、「スコープ間で VPC CIDR を移動する」を参照してください。
- IPAM によって監視されていない AWS アカウントにリソースを削除または転送すると、そのリソースに関連する新しい履歴は表示されなくなり、IPAM はリソースを監視しなくなります。ただし、リソースの IP アドレスは引き続き検索可能です。
- IPAM を組織外のアカウントに統合する の場合、IPAM 所有者はそのアカウントが所有するすべてのリソース CIDR の IP アドレス履歴を確認できます。

AWS Management Console

CIDR の履歴を表示するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで [IP 履歴の検索] をクリックします。
3. IPv4 または IPv6 IP アドレス、または CIDR を入力します。これは、リソースの指定の CIDR である必要があります。
4. IPAM スコープ ID を選択します。
5. 日付 / 時刻の範囲を選択します。
6. VPC で結果をフィルタリングするには、VPC ID を入力します。CIDR が複数の VPC に表示される場合は、このオプションを使用します。
7. [検索] を選択してください。

Command line

このセクションのコマンドは、AWS CLI コマンドリファレンスに関連しています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

- CIDR の履歴を表示: get-ipam-address-history

AWS CLI を使用して IP アドレスの使用状況を分析および監査する方法の事例については、チュートリアル: AWS CLI を使用して IP アドレス履歴を表示するを参照してください。

検索結果は、次の列にまとめられています。

- [Sampled end time] (サンプル終了時間): IPAM スコープ内のリソースと CIDR 関連付けの終了時刻をサンプリングします。変更は定期的なスナップショットで取得されるため、終了時刻がこの特定の時刻より前に発生している場合があります。
- [Sampled start time] (サンプル開始時間): IPAM スコープ内のリソースと CIDR 関連付けの終了時刻をサンプリングします。変更は定期的なスナップショットで取得されるため、開始時刻がこの特定の時刻より前に発生している場合があります。

  Example

  サンプル開始時間とサンプル終了時間の下に表示される時間を説明するために、ユースケースの例を見てみましょう。

  午後 2 時に、CIDR 10.0.0.0/16 で VPC が作成されました。午後 3 時に、CIDR 10.0.0.0/8 で IPAM と IPAM プールを作成し、自動インポートオプションを選択して、IPAM が 10.0.0.0/8 IP アドレス範囲内にあるすべての CIDR を検出してインポートできるようにします。IPAM は定期的なスナップショットで CIDR に対する変更をピックアップするため、午後 3 時 5 分までは既存の VPC CIDR を検出しません。IP 履歴検索機能を使用してこの VPC の ID を検索すると、VPC のサンプル開始時刻は午後 3 時 5 分になります。これは、IPAM で検出された時間であり、VPC を作成した時間である午後 2 時ではありません。ここで、午後 5 時に VPC を削除するとします。VPC が削除されると、VPC に割り当てられた CIDR 10.0.0.0/16 が IPAM プールにリサイクルされます。IPAM は午後 5 時 5 分に定期的なスナップショットを取得し、変更を取得します。IP 履歴検索機能を使用してこの VPC の ID を検索すると、VPC の CIDR のサンプル終了時間は午後 5 時 5 分になります。これは、VPC が削除された時間である午後 5 時ではありません。
- [Resource ID] (リソース ID): リソースが CIDR に関連付けられたときに生成された ID。
- [Name] (名前): リソースの名前 (該当する場合)。

- [Compliance status] (コンプライアンスのステータス): CIDR のコンプライアンスのステータス。
  - 準拠: マネージドリソースは、IPAM プールの割り当てルールに準拠しています。
  - [Noncompliant] (非準拠): リソース CIDR は、IPAM プールの 1 つ以上の割り当てルールに準拠していません。

    Example

    VPC に IPAM プールのネットマスク長パラメータを満たさない CIDR がある場合、またはリソースが IPAM プールと同じ AWS リージョンにない場合、非準拠としてフラグが設定されます。
  - [UnManaged] (アンマネージド): リソースには、IPAM プールから割り当てられた CIDR がなく、IPAM によって、CIDR の重複がないかどうか、およびプール割り当てルールへのコンプライアンスが監視されていません。CIDR は重複について監視されます。
  - [Ignored] (無視): マネージドリソースは、モニタリング対象から除外されるように選択されています。無視されたリソースは、重複または割り当てルールへのコンプライアンスについて評価されません。リソースが無視されるように選択されると、IPAM プールからリソースに割り当てられたスペースはすべてプールに返され、リソースは自動インポートを介して再度インポートされません (自動インポートの割り当てルールがプールに設定されている場合)。
  - [-]: このリソースは、IPAM が監視または管理できるリソースのタイプではありません。
- [Overlap status] (重複ステータス): CIDR の重複ステータス。
  - 重複していない: リソース CIDR は同じスコープ内の別の CIDR と重複していません。
  - 重複している: リソース CIDR は同じスコープ内の別の CIDR と重複しています。リソース CIDR が重複している場合は、手動割り当てと重複している可能性があることに注意してください。
  - [Ignored] (無視): マネージドリソースは、監視対象から除外されるように選択されています。無視されたリソースは、IPAM では、重複または割り当てルールへのコンプライアンスについて評価されません。リソースが無視されるように選択されると、IPAM プールからリソースに割り当てられたスペースはすべてプールに返され、リソースは自動インポートを介して再度インポートされません (自動インポートの割り当てルールがプールに設定されている場合)。
  - [-]: このリソースは、IPAM がモニタリングまたは管理できるリソースのタイプではありません。
- リソースタイプ
  - [vpc]: CIDR は VPC に関連付けられています。
  - [subnet] (サブネット): CIDR は VPC サブネットに関連付けられています。

  - [EIP]: CIDR は Elastic IP アドレスに関連付けられています。
  - [instance] (インスタンス): CIDR は EC2 インスタンスに関連付けられています。
  - [network-interface] (ネットワークインターフェイス): CIDR はネットワークインターフェイスに関連付けられています。
- VPC ID: このリソースが属する VPC の ID (該当する場合)。
- [Region] (リージョン): このリソースの AWS リージョン。
- [Owner ID] (所有者 ID): このリソースを作成したユーザーの AWS アカウント ID (該当する場合)。

Public IP Insights を確認する

[Public IP Insights] を使用すると、次が確認できます。

- IPAM がAWS 組織内のアカウントと統合されている場合は、AWS 組織全体のすべての AWS リージョンのサービスで使用されているすべてのパブリック IPv4 アドレスを表示できます。
- IPAM が 1 つのアカウントに統合されている場合は、アカウント内のすべての AWS リージョンのサービスで使用されているすべてのパブリック IPv4 アドレスを表示できます。

パブリック IPv4 アドレスは、インターネットからルーティング可能な IPv4 アドレスです。インターネットから IPv4 経由でリソースに直接アクセスするには、パブリック IPv4 アドレスが必要です。

> **Note**
>
> AWS は、実行中のインスタンスに関連付けられているパブリック IPv4 アドレスや Elastic IP アドレスを含めたすべてのパブリック IPv4 アドレスの料金を請求します。詳細については「Amazon VPC の料金」ページにあるパブリック IPv4 アドレスタブを参照してください。

以下のパブリック IPv4 アドレスタイプに関するインサイトを確認できます。

- Elastic IP アドレス (EIP): Amazon が提供する静的なパブリック IPv4 アドレスであり、EC2 インスタンス、Elastic Network Interface、または AWS リソースと関連付けることができます。
- EC2 パブリック IPv4 アドレス: Amazon が EC2 インスタンスに割り当てるパブリック IPv4 アドレスです (デフォルトのサブネットで EC2 インスタンスが起動された場合、またはパブリック

IPv4 アドレスを自動的に割り当てるように設定されたサブネットでインスタンスが起動された場合)。

- BYOIPv4 アドレス: Bring-Your-Own-IP (BYOIP) 機能により AWS に持ち込む IPv4 アドレス範囲のパブリック IPv4 アドレスです。
- サービスマネージド IPv4 アドレス: AWS サービスにより自動的に AWS リソースにプロビジョニングされて管理されるパブリック IPv4 アドレスです。例えば、Amazon ECS、Amazon RDS、Amazon WorkSpaces のパブリック IPv4 アドレスなどです。

Public IP Insights では、このリージョンのサービスで使用されている、すべてのパブリック IPv4 アドレスが表示されます。これらのインサイトを利用して、パブリック IPv4 アドレスの使用状況を特定し、未使用の Elastic IP アドレスを解放するための推奨事項を確認できます。

- パブリック IP タイプ: タイプ別に整理されたパブリック IPv4 アドレスの数です。
  - Amazon 所有 EIP: AWS アカウントのリソースにプロビジョニングした、または割り当てた Elastic IP アドレスアカウントです。
  - EC2 パブリック IP: デフォルトサブネット、またはパブリック IPv4 アドレスを自動的に割り当てるように設定されたサブネットでインスタンスを起動したときに EC2 インスタンスに割り当てられるパブリック IPv4 アドレスです。
  - BYOIP: Bring-Your-Own-IP (BYOIP) 機能により AWS に持ち込むパブリック IPv4 アドレスです。
  - サービスマネージド IP: AWS サービスによりプロビジョニングされて管理されるパブリック IPv4 アドレスです。
  - サービスマネージド BYOIP: AWS に提供され、AWS サービスによって管理されるパブリック IPv4 アドレス。
  - Amazon 所有の連続した EIP: Amazon 提供の連続したパブリック IPv4 IPAM プールから割り当てられた Elastic IP アドレス。
- EIP 使用状況: 使用方法別に整理された Elastic IP アドレスの数です。
  - 関連付けられた Amazon 所有 EIP: AWS アカウントでプロビジョニングした Elastic IP アドレスであり、EC2 インスタンス、ネットワークインターフェイス、または AWS リソースに関連付けたものです。
  - 関連付けられた BYOIP: BYOIP により AWS に持ち込んだパブリック IPv4 アドレスであり、ネットワークインターフェイスに関連付けたものです。
  - 関連付けられていない Amazon 所有 EIP: AWS アカウントでプロビジョニングした Elastic IP アドレスであるものの、ネットワークインターフェイスには関連付けていないものです。

  - 関連付けられていない BYOIP: BYOIP により AWS に持ち込んだパブリック IPv4 アドレスであるものの、ネットワークインターフェイスには関連付けていないものです。
  - 関連付けられた Amazon 所有の連続した EIP: Amazon 提供の連続したパブリック IPv4 IPAM プールから割り当てられ、リソースに関連付けられた Elastic IP アドレス。
  - 関連付けられていない Amazon 所有の連続した EIP: Amazon 提供の連続したパブリック IPv4 IPAM プールから割り当てられ、リソースに関連付けられていない Elastic IP アドレス。
- Amazon 所有の IPv4 連続した IP の使用状況: 時間の経過に伴う連続したパブリック IPv4 アドレスの使用状況と、関連する Amazon 所有の IPv4 IPAM プールを示すテーブル。
- パブリック IP アドレス: パブリック IPv4 アドレスとその属性の表です。
  - IP アドレス: パブリック IPv4 アドレスです。
  - 関連付けられた: そのアドレスが EC2 インスタンス、ネットワークインターフェイス、または AWS リソースに関連付けられているかどうかです。
    - 関連付けられた: そのパブリック IPv4 アドレスは EC2 インスタンス、ネットワークインターフェイス、または AWS リソースに関連付けられています。
    - 関連付けられていない: そのパブリック IPv4 アドレスは、AWS アカウントでどのリソースにも関連付けられておらず、アイドル状態です。
  - アドレスタイプ: IP アドレスのタイプです。
    - Amazon 所有 EIP: そのパブリック IPv4 アドレスは Elastic IP アドレスです。
    - BYOIP: そのパブリック IPv4 アドレスは BYOIP を使用して AWS に持ち込まれました。
    - EC2 パブリック IP: そのパブリック IPv4 アドレスは自動的に EC2 インスタンスに割り当てられました。
    - サービスマネージド BYOIP: パブリック IPv4 アドレスは AWS に Bring-Your-Own-IP (BYOIP) を導入しました。
    - サービスマネージド IP: このパブリック IPv4 アドレスは、AWS サービスによりプロビジョニングされて管理されています。
  - サービス: IP アドレスが関連付けられているサービスです。
    - AGA: AWS Global Accelerator。カスタムルーティングアクセラレーターを使用する場合、そのパブリック IP は表示されません。これらのパブリック IP を表示するには、「Viewing your custom routing accelerators」を参照してください。
    - Database Migration Service: AWS Database Migration Service (DMS) レプリケーションインスタンスです。
    - Redshift: Amazon Redshift クラスターです。

  - RDS: Amazon Relational Database Service (RDS) インスタンスです。
  - ロードバランサー (EC2): Application Load Balancer または Network Load Balancer です。
  - NAT ゲートウェイ (VPC): Amazon VPC のパブリック NAT ゲートウェイです。
  - Site-to-Site VPN: AWS Site-to-Site VPN 仮想プライベートゲートウェイです。
  - その他: 現在特定できないその他のサービスです。
- 名前 (EIP ID): このパブリック IPv4 アドレスが Elastic IP アドレス割り当ての場合、これが EIP 割り当ての名前と ID です。
- ネットワークインターフェイス ID: このパブリック IPv4 アドレスがネットワークインターフェイスに関連付けられている場合、これがネットワークインターフェイスの ID です。
- インスタンス ID: このパブリック IPv4 アドレスが EC2 インスタンスに関連付けられている場合、これがインスタンス ID です。
- セキュリティグループ: このパブリック IPv4 アドレスが EC2 インスタンスに関連付けられている場合、これがインスタンスに割り当てられたセキュリティグループの名前と ID です。
- パブリック IPv4 プール: これが Amazon が所有および管理する IP アドレスプールの Elastic IP アドレスである場合、値は「-」です。これがユーザーが所有し、(BYOIP を使用して) Amazon に持ち込んだ IP アドレス範囲の Elastic IP アドレスの場合、値はパブリック IPv4 プール ID です。
- ネットワークボーダーグループ: IP アドレスがアドバタイズされている場合、その IP アドレスはこの AWS リージョンからアドバタイズされています。
- オーナー ID: リソースオーナーの AWS アカウント数。
- サンプル時間: 最後に成功したリソース検出の時間。
- リソースディスカバリ ID: このパブリック IPv4 アドレスを検出したリソースディスカバリ ID。
- サービスリソース: リソース ARN または ID。

Elastic IP アドレスがアカウントに割り当てられているものの、ネットワークインターフェイスには関連付けられていない場合、アカウントに関連付けられていない EIP があるので解放するべきだと通知するバナーが表示されます。

> **Important**
>
> Public IP Insights は最近更新されました。GetIpamDiscoveredPublicAddresses を呼び出す権限がないというエラーが表示される場合は、共有されていたリソースディスカバリーにアタッチされている管理権限を更新する必要があります。リソースディスカバリの作成者に連絡して、管理権限 `AWSRAMPermissionIpamResourceDiscovery` をデフォルトバージョ

ンに更新するよう依頼してください。詳細については、AWS RAM ユーザーガイドの「リソース共有の更新」を参照してください。

AWS Management Console

パブリック IP アドレスのインサイトを表示するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[Public IP Insights] を選択します。
3. パブリック IP アドレスの詳細を表示するには、IP アドレスをクリックします。
4. IP アドレスに関する以下の情報が表示されます。

   - 詳細: アドレスタイプやサービスなど、メインの Public IP Insights ペインの列と同じ情報が表示されます。
   - インバウンドセキュリティグループのルール: この IP アドレスが EC2 インスタンスに関連付けられている場合、これらはインスタンスへのインバウンドトラフィックを制御するセキュリティグループルールです。
   - アウトバウンドセキュリティグループのルール: この IP アドレスが EC2 インスタンスに関連付けられている場合、これらはインスタンスからのアウトバウンドトラフィックを制御するセキュリティグループのルールです。
   - タグ: AWS リソースを整理するためのメタデータとして機能するキーと値のペアです。

Command line

IPAM によって検出されたパブリック IP アドレスを取得するには、get-ipam-discovered-public-addresses コマンドを使用します。

Amazon VPC IP Address Manager のチュートリアル

次のチュートリアルでは、AWS CLI を使用して一般的な IPAM タスクを実行する方法を示します。AWS CLI を取得する方法については、「IPAM へのアクセス」を参照してください。こちらのチュートリアルで説明している IPAM の概念の詳細については、「IPAM の仕組み」を参照してください。

内容

AWS CLI を使用した IPAM の開始方法

このチュートリアルでは、単一の AWS アカウントを使用して CLI で Amazon VPC IP Address Manager (IPAM) AWS をセットアップし使用するプロセスについて説明します。このチュートリアルを終えると、IPAM の作成、IP アドレスプール階層の作成、VPC への CIDR の割り当てが完了します。

前提条件

このチュートリアルを開始する前に、以下の要件を満たしていることを確認してください。

- IPAM リソースを作成および管理するためのアクセスが許可された AWS アカウントがある。
- AWS CLI がインストール済みで、適切な認証情報を使用して設定されている。AWS CLI のインストールについては、「AWS CLI の最新バージョンのインストールまたは更新」を参照してください。AWS CLI の設定については、「設定の基本」を参照してください。

- IP アドレス指定と CIDR 表記について基本的な理解がある。
- Amazon VPC の概念に関する基本的な知識がある。
- チュートリアルの所要時間は、約 30 分です。

IPAM を作成する

最初のステップでは、運用リージョンを使用して IPAM を作成します。IPAM を使用すると、AWS ワークロードの IP アドレスを計画、追跡、モニタリングできます。

us-east-1 と us-west-2 にオペレーションリージョンがある IPAM を作成します。

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

このコマンドを使用すると、IPAM を作成し、その IPAM で指定リージョンの IP アドレスを管理できるようになります。運用リージョンとは、IPAM によって IP アドレス CIDR を管理できる AWS リージョンを意味します。

IPAM が作成済みであることを確認します。

```
aws ec2 describe-ipams
```

出力された IPAM ID をメモします。この ID は、後続のステップで必要となります。

IPAM の作成が完了し、使用可能になるまで待ちます (約 20 秒)。

```
sleep 20
```

IPAM スコープ ID の取得

IPAM を作成すると、AWS によって、プライベートスコープとパブリックスコープが自動作成されます。このチュートリアルでは、プライベートスコープを使用します。

IPAM の詳細を取得して、プライベートスコープ ID を抽出します。

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

ipam-0abcd1234 を、実際の IPAM ID に置き換えます。

出力内にある PrivateDefaultScopeId フィールドのプライベートスコープ ID を特定し、メモします。ipam-scope-0abcd1234 のようになります。

トップレベル IPv4 プールを作成する

次に、プライベートスコープ内に最上位プールを作成します。このプールは、階層内にある他のすべてのプールの親として機能します。

トップレベル IPv4 プールを作成します。

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

ipam-scope-0abcd1234 を、実際のプライベートスコープ ID に置き換えます。

プールの作成が完了し、使用可能になるまで待ちます。

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

ipam-pool-0abcd1234 を、実際の最上位プール ID に置き換えます。状態が create-complete であることを確認し、次のステップに進みます。

プールが利用可能になったら、CIDR ブロックをプロビジョニングします。

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

CIDR のプロビジョニングが完了するまで待ちます。

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

状態が provisioned であることを確認し、次のステップに進みます。

リージョンの IPv4 プールを作成する

次に、最上位プール内にリージョンプールを作成します。このプールは、特定の AWS リージョンに固有のものです。

リージョンの IPv4 プールを作成します。

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

`ipam-scope-0abcd1234` を、実際のプライベートスコープ ID に、`ipam-pool-0abcd1234` を最上位プール ID に置き換えます。

リージョンプールの作成が完了し、使用可能になるまで待ちます。

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

`ipam-pool-1abcd1234` を実際のリージョンプール ID に置き換えます。状態が `create-complete` であることを確認し、次のステップに進みます。

プールが利用可能になったら、CIDR ブロックをプロビジョニングします。

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

CIDR のプロビジョニングが完了するまで待ちます。

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

状態が `provisioned` であることを確認し、次のステップに進みます。

開発 IPv4 プールを作成する

次に、リージョンプール内に開発プールを作成します。このプールは開発環境に使用します。

開発 IPv4 プールを作成します。

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

ipam-scope-0abcd1234 を実際のプライベートスコープ ID に置き換え、ipam-pool-1abcd1234 をリージョンプール ID に置き換えます。

注: 親プールのロケールと一致する --locale パラメータを指定することが重要です。

開発プールの作成が完了し、使用可能になるまで待ちます。

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

ipam-pool-2abcd1234 を実際の開発プール ID に置き換えます。状態が create-complete であることを確認し、次のステップに進みます。

プールが利用可能になったら、CIDR ブロックをプロビジョニングします。

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

CIDR のプロビジョニングが完了するまで待ちます。

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

状態が provisioned であることを確認し、次のステップに進みます。

IPAM プール CIDR が使用される VPC を作成する

最後に、IPAM プールの CIDR が使用される VPC を作成します。ここでは、IPAM を使用して IP アドレス空間を AWS リソースに割り当てる方法を示します。

IPAM プールの CIDR が使用される VPC を作成します。

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

`ipam-pool-2abcd1234` を実際の開発プール ID に置き換えます。

`--ipv4-netmask-length 26` パラメータを指定して、このプールから /26 CIDR ブロック (64 個の IP アドレス) を割り当てます。このネットマスク長を選択するのは、プールの CIDR ブロック (/24) よりも少ないアドレス個数を指定するためです。

VPC が作成済みであることを確認します。

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

IPAM プールの割り当てを確認する

CIDR が IPAM プールから割り当てられたことを確認します。

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

`ipam-pool-2abcd1234` を実際の開発プール ID に置き換えます。

このコマンドにより、指定した IPAM プールからのすべての割り当て情報が表示されます。これには、先ほど作成した VPC も含まれています。

トラブルシューティング

IPAM の使用中によく発生する問題を次に示します。

- アクセス許可エラー: IAM ユーザーまたはロールに、IPAM リソースの作成および管理に必要なアクセス許可があることを確認します。`ec2:CreateIpam`、`ec2:CreateIpamPool`、その他の関連するアクセス許可が必要になる場合があります。
- リソース制限の超過: デフォルトの場合、アカウントごとに作成できる IPAM は 1 つのみです。IPAM を新規作成するには、既存の IPAM を削除する必要があります。あるいは、既存の IPAM を使用します。
- CIDR 割り当ての失敗: CIDR をプールにプロビジョニングするときには、プロビジョニング対象の CIDR が他のプールに割り当て済みの CIDR と重複しないようにしてください。

- API リクエストのタイムアウト:「RequestExpired」エラーが発生した場合は、ネットワークレイテンシーまたは時刻同期の問題が原因である可能性があります。コマンドを再実行してみてください。
- 不正な状態エラー:「IncorrectState」エラーが発生した場合は、適切な状態ではないリソースにオペレーションを実行しようとしている可能性があります。リソースの作成またはプロビジョニングが完了するまで待ち、次のステップに進んでください。
- 割り当てサイズエラー: 割り当てサイズに関する「InvalidParameterValue」エラーが発生した場合は、プールサイズ上、適切なネットマスク長をリクエストしていることを確認してください。例えば、/24 プールから /25 CIDR を割り当てることはできません。
- 依存関係違反: リソースをクリーンアップする際に、「DependencyViolation」エラーが発生する可能性があります。これは、リソースが相互に依存していることで生じます。リソースは、作成時の逆の順序で削除するようにし、CIDR をプロビジョニング解除した後にプールを削除してください。

リソースをクリーンアップする

このチュートリアルを完了したら、不要な課金が発生しないよう、作成したリソースをクリーンアップする必要があります。

1. VPC の削除

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

2. 開発プールから CIDR のプロビジョニングを解除します。

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

3. 開発プールを削除します。

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

4. リージョンプールから CIDR をプロビジョニング解除します。

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

5. リージョンプールを削除します。

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

6. 最上位プールから CIDR をプロビジョニング解除します。

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

7. 最上位プールを削除します。

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

8. IPAM を削除します。

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

すべての ID を実際のリソース ID に置き換えます。

> **Note**
>
> これらのオペレーションの間、場合によっては、リソースの削除が完了するまで待機した後に、次のステップに進む必要があります。依存関係違反が発生した場合は、数秒待ってから再実行してみてください。

次のステップ

CLI で IPAM AWS を作成し使用する方法を習得できたので、その他の高度な機能についても知識を深めましょう。

- IP アドレスのプロビジョニング計画 – IP アドレス空間の効果的な計画について学ぶ
- リソースごとに CIDR の使用状況をモニタリングする – IP アドレスの使用状況をモニタリングする方法を理解する
- AWS RAM を使用して IPAM プールを共有する – AWS アカウント間で IPAM プールを共有する方法について学ぶ
- IPAM を AWS Organizations 内のアカウントと統合する – 組織全体で IPAM を活用する方法について知識を得る

チュートリアル: コンソールを使用して IPAM とプールを作成する

このチュートリアルでは、IPAM を作成し、AWS Organizations を統合し、IP アドレスプールを作成して、IPAM プールの CIDR を使って VPC を作成します。

このチュートリアルでは、IPAM を使用して、さまざまな開発ニーズに基づき IP アドレス空間を整理する方法について説明します。このチュートリアルを終了すると、本番稼働前のリソース用の IP アドレスプールが 1 つ完成します。その後、ルーティングとセキュリティのニーズに基づき、本番稼働用リソースのプールなど他のプールを作成することができます。

IPAM は単一のユーザーとしても使用できますが、AWS Organizations と統合すれば、組織内のアカウント全体の IP アドレスを管理できます。このチュートリアルでは、IPAM を組織内のアカウントと統合する方法も説明します。「IPAM を組織外のアカウントに統合する」方法については取り上げません。

> **Note**
>
> このチュートリアルでは、IPAM リソースに名前を付ける方法、特定のリージョンに IPAM リソースを作成する方法、プールに特定の IP アドレス CIDR 範囲を使用する方法を、説明します。これは、IPAM で利用できる選択肢を簡素化し、IPAM をすぐに開始できるようにすることを意図しています。このチュートリアルを終了すると、新しい IPAM を作成してその設定を変更できます。

内容

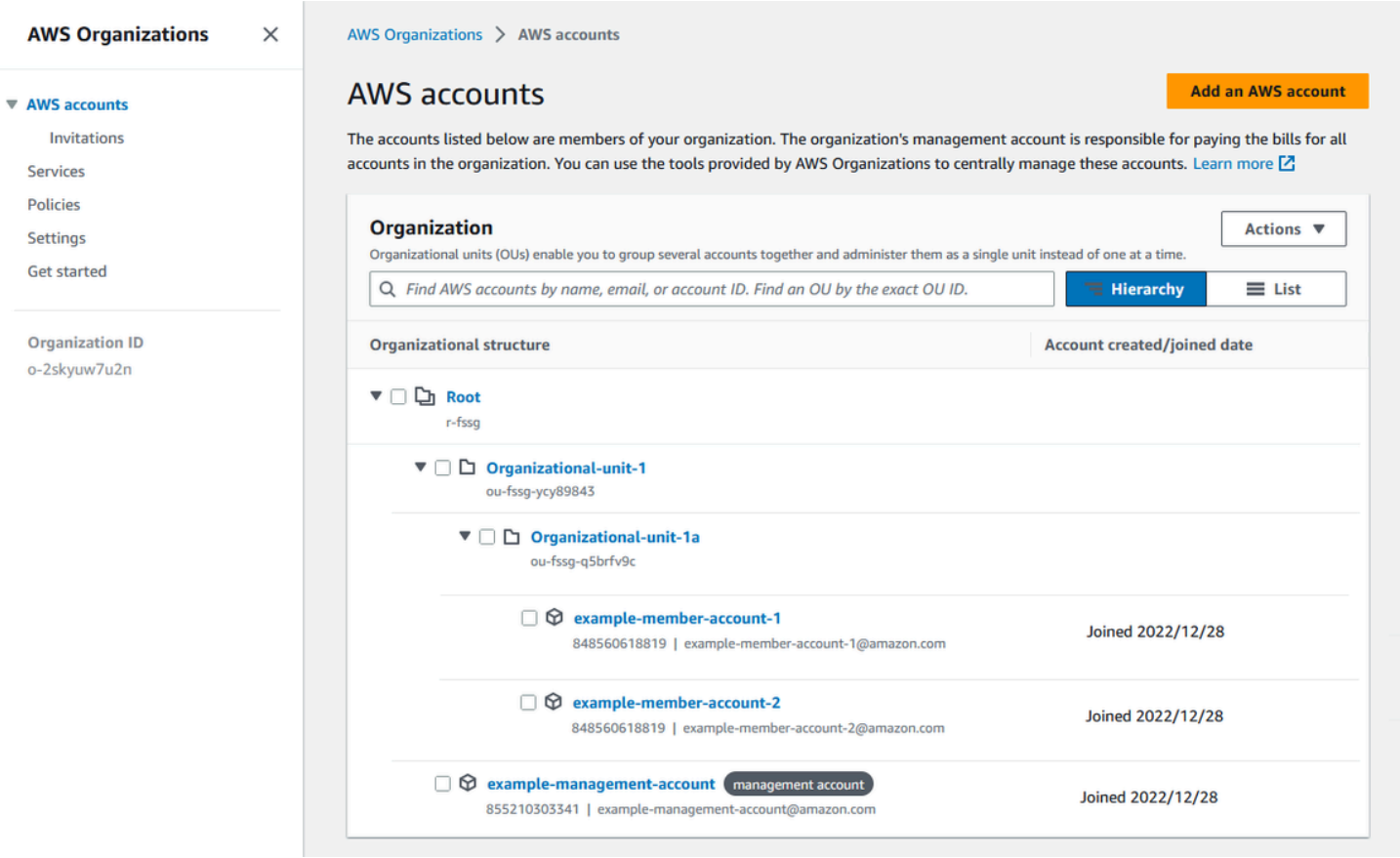
前提条件

開始する前に、1 つ以上のメンバーアカウントを持つ AWS Organizations アカウントを、セットアップする必要があります。手順については、「AWS Organizations ユーザーガイド」の「組織の作成と管理」を参照してください。

AWS Organizations を IPAM と統合する方法

このセクションでは、このチュートリアルで使用する AWS Organizations アカウントの例を紹介します。このチュートリアルで、IPAM と統合する際に使用する組織内のアカウントは、次の 3 つです。

- 管理アカウント (以下の図の example-management-account)。IPAM コンソールにログインして IPAM の管理者を委任するときに使用します。組織の管理アカウントを IPAM の管理者として使用することはできません。
- メンバーアカウント (以下の図の example-member-account-1)。IPAM の管理者アカウントとして使用します。IPAM の管理者アカウントは、IPAM の作成と、組織全体における IP アドレスの使用状況の、IPAM を使用した管理およびモニタリングを行います。組織内のメンバーアカウントは、いずれも IPAM の管理者として委任することが可能です。
- メンバーアカウント (以下の図の example-member-account-2)。デベロッパーアカウントとして使用します。このアカウントは、IPAM プールから割り当てられた CIDR を使って VPC を作成します。



これらのアカウントに加え、デベロッパーアカウントとして使用するメンバーアカウントが含まれる、組織単位の ID が必要になります (上の図の ou-fssg-q5brfv9c)。この ID は、後ほど、IPAM プールを共有するときに必要になります。こちらは OU と共有できます。

> **Note**
>
> 管理アカウントやメンバーアカウントなど、AWS Organizations アカウントの種類の詳細については、「AWS Organizations の用語と概念」を参照してください。

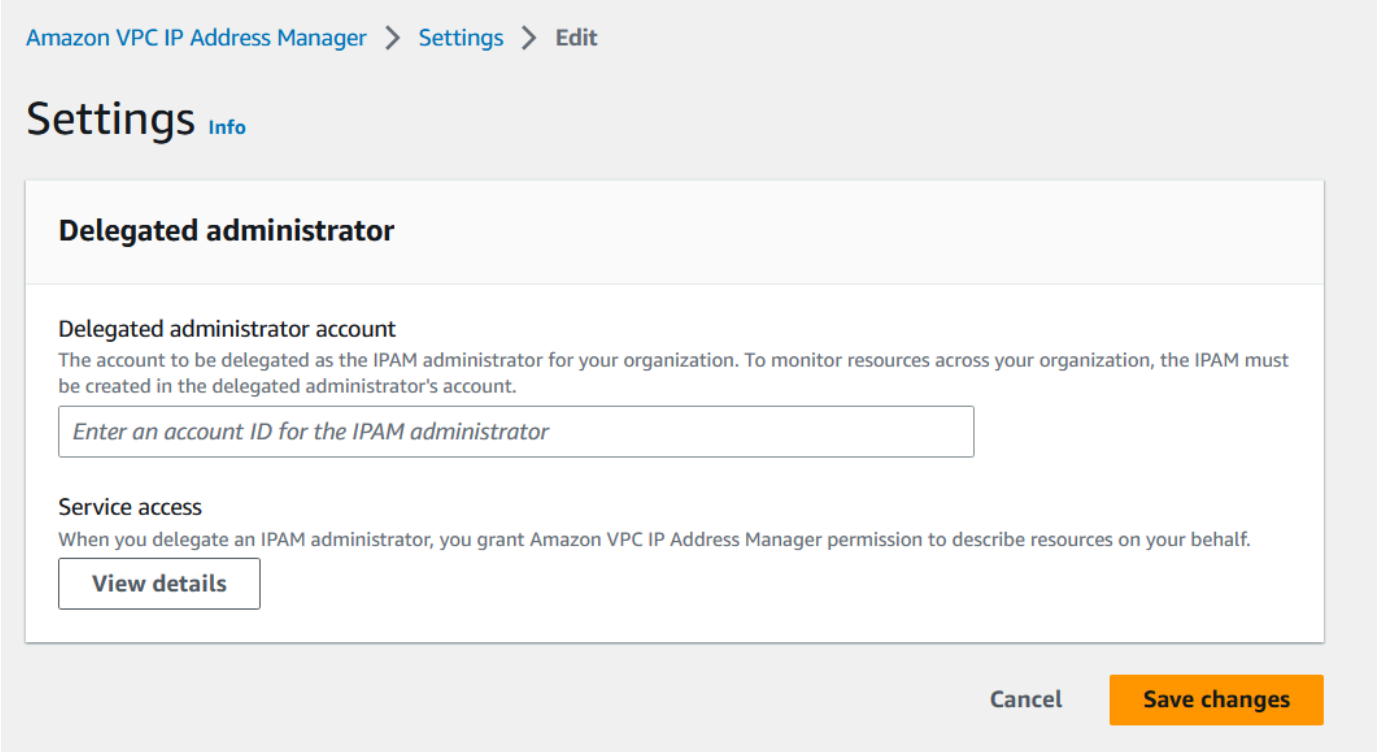
ステップ 1: IPAM の管理者を委任する

このステップでは、AWS Organizations メンバーアカウントを IPAM の管理者として委任します。IPAM の管理者として委任すると、サービスリンクロールが各 AWS Organizations メンバーアカウントに自動的に作成されます。IPAM は、各メンバーアカウントのサービスリンクロールを継承し、これらのアカウントにおける IP アドレスの使用状況をモニタリングします。それにより、組織単位に関係なく、リソースとその CIDR を検出することができます。

必要な AWS Identity and Access Management (IAM) アクセス許可がないと、このステップを完了できません。詳細については、「IPAM を AWS Organizations 内のアカウントと統合する」を参照してください。

IPAM の管理者アカウントとして委任するには

1. AWS Organizations 管理アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. AWS マネジメントコンソール で、IPAM を使用する AWS リージョンを選択します。
3. ナビゲーションペインで [組織の設定] を選択します。
4. [委任] を選択します。[委任] オプションは、コンソールに AWS Organizations 管理アカウントとしてログインしている場合のみ使用できます。
5. 組織のメンバーアカウントの AWS アカウント ID を入力します。IPAM の管理者は、AWS Organizations の管理アカウントではなく、メンバーアカウントでなければなりません。



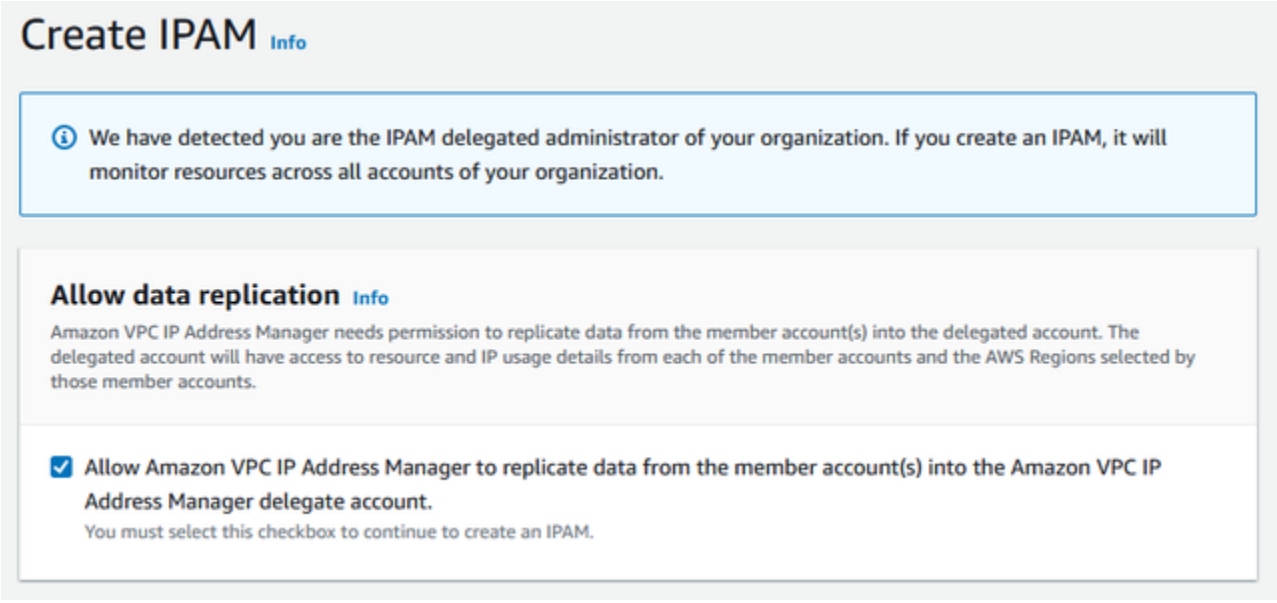
6. [Save changes] (変更の保存) をクリックします。[委任された管理者] の情報に、そのメンバーアカウントに関する詳細が入力されます。

ステップ 2: IPAM を作成する

このセクションでは、IPAM を作成します。IPAM を作成するときは、IPAM が、IPAM 用に 2 つのスコープを自動作成します。すべてのプライベートスペース用のプライベートスコープと、すべてのパブリックスペース用のパブリックスコープです。スコープは、プールおよび割り当てとともに、IPAM の主要なコンポーネントです。詳細については、「IPAM の仕組み」を参照してください。

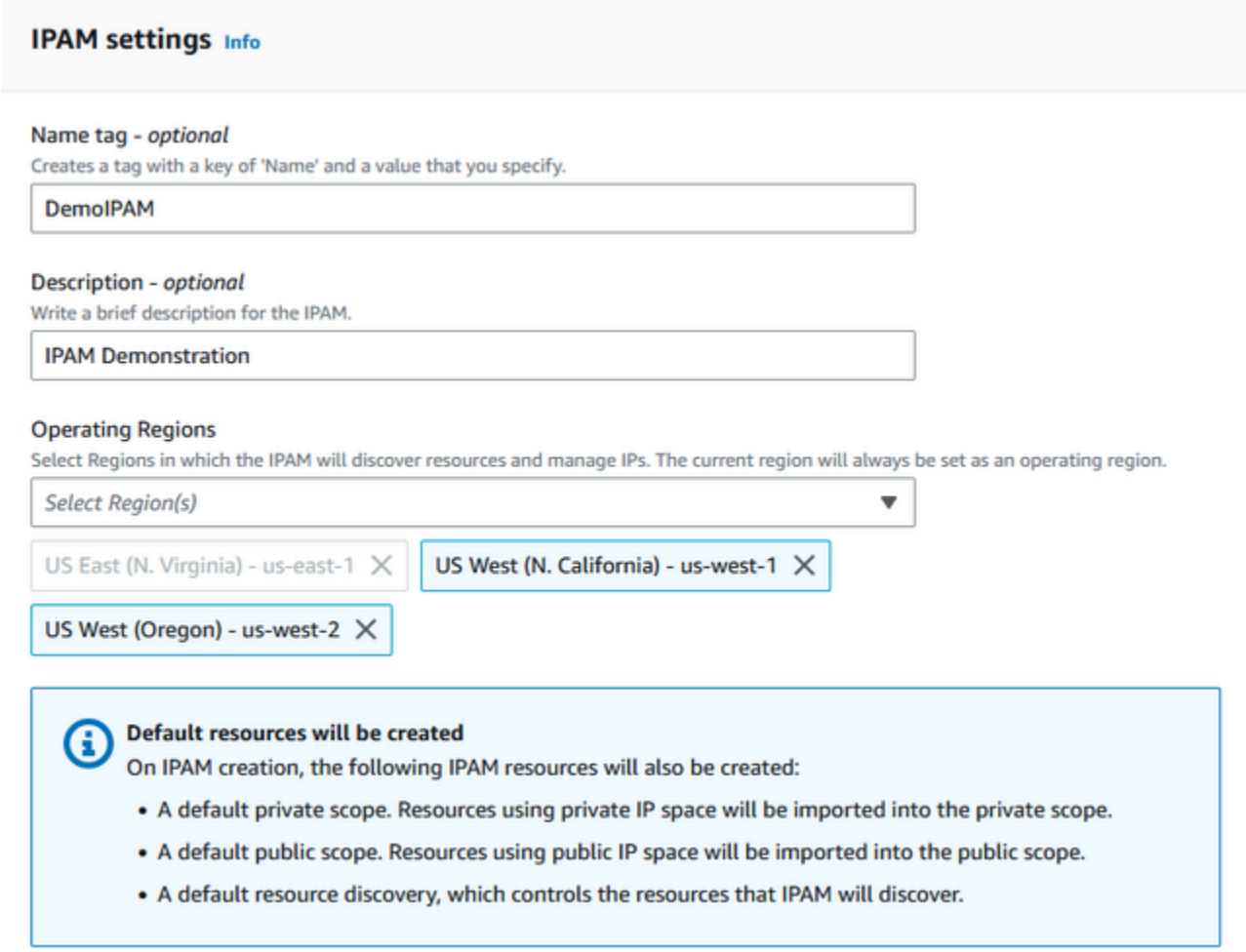
IPAM を作成するには

1. 前のステップで IPAM の管理者として委任した AWS Organizations メンバーアカウントを使用して、IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. AWS マネジメントコンソールで、IPAM を作成する AWS リージョンを選択します。オペレーションの主要リージョンに IPAM を作成します。
3. サービスホームページで [IPAM の作成] を選択します。
4. [Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account] (Amazon VPC IP Address Manager がソースアカウントから IPAM 委任アカウントにデータをレプリケートするのを許可する) を選択します。このオプションを選択しないと、IPAM を作成できません。

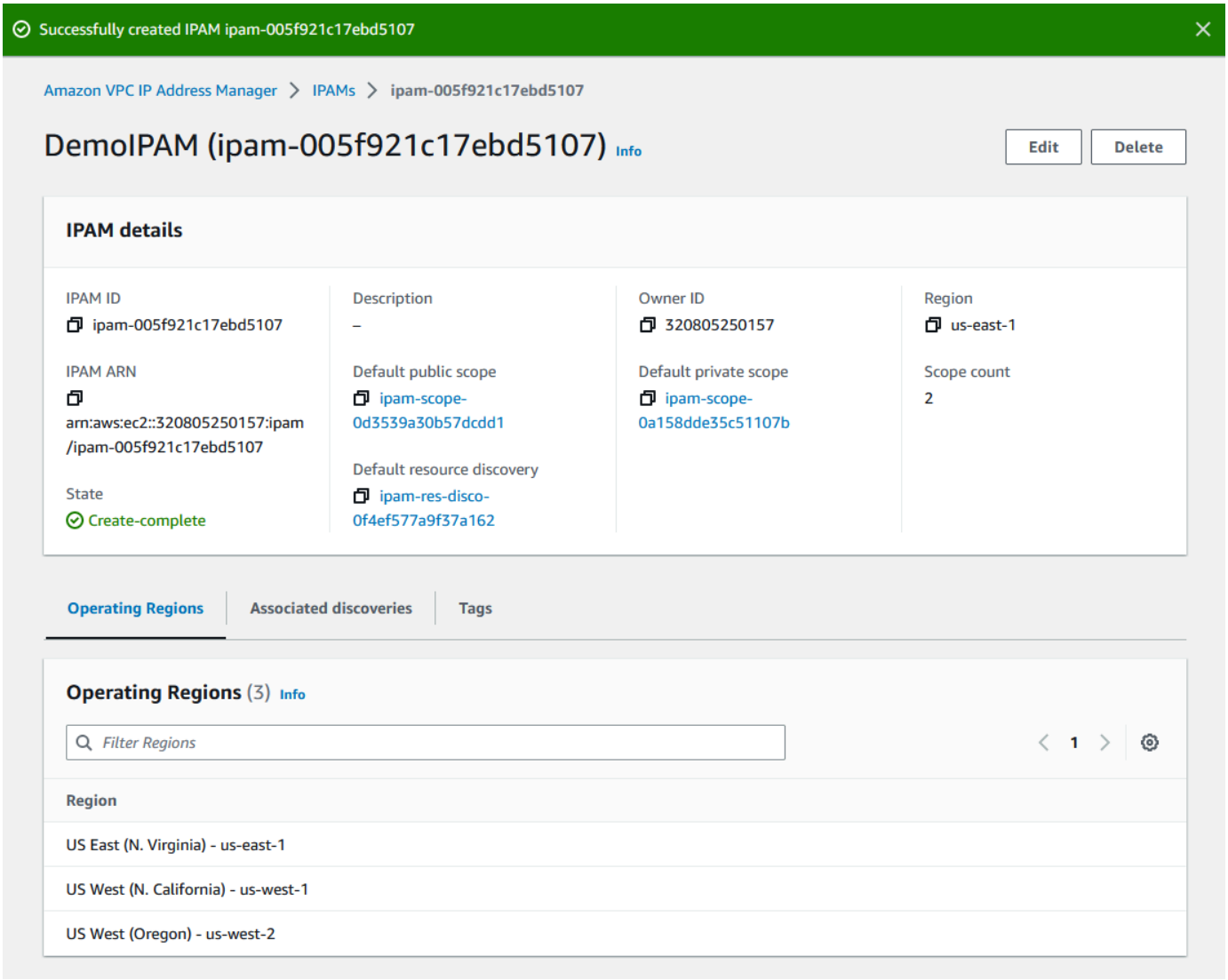


5. [運用リージョン] で、この IPAM がリソースを管理および検出できる AWS リージョンを選択します。IPAM を作成している AWS リージョンは、運用リージョンの 1 つとして自動的に選択されます。このチュートリアルでは、IPAM のホームリージョンは us-east-1 です。したがって、

追加の運用リージョンとして us-west-1 と us-west-2 を選択します。運用リージョンを忘れた場合は、後で IPAM の設定を編集し、リージョンを追加または削除することができます。



6. [Create IPAM] (IPAM を作成) を選択します。



ステップ 3: 最上位の IPAM プールの作成する

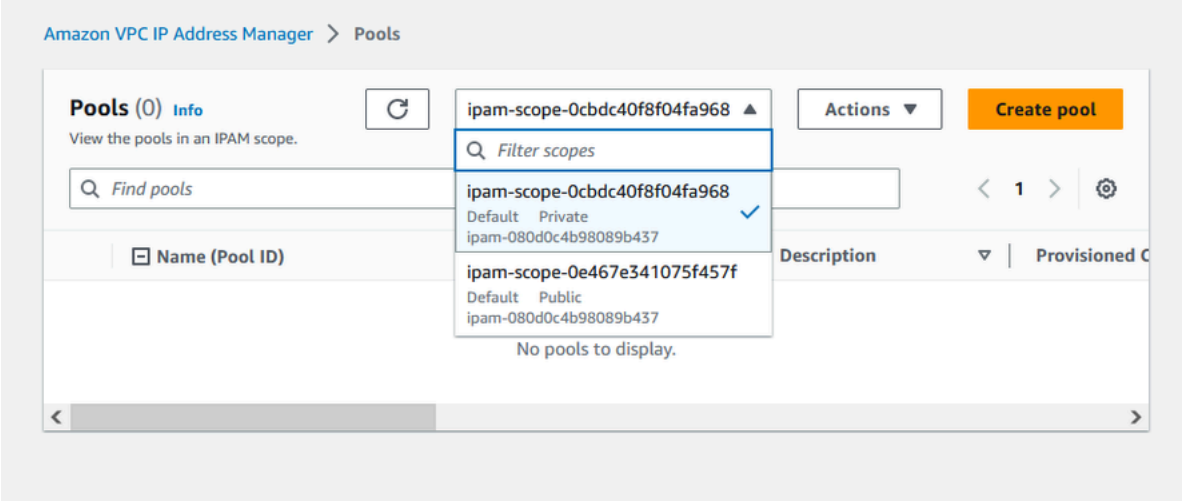
このチュートリアルでは、最上位の IPAM プールから始まるプールの階層を作成します。これ以降のステップでは、リージョンプールのペアと、そのうちの 1 つに含まれる本番稼働前開発プールを作成します。

IPAM を使って構築するプール階層の詳細については、「IPAM プール計画の例」を参照してください。

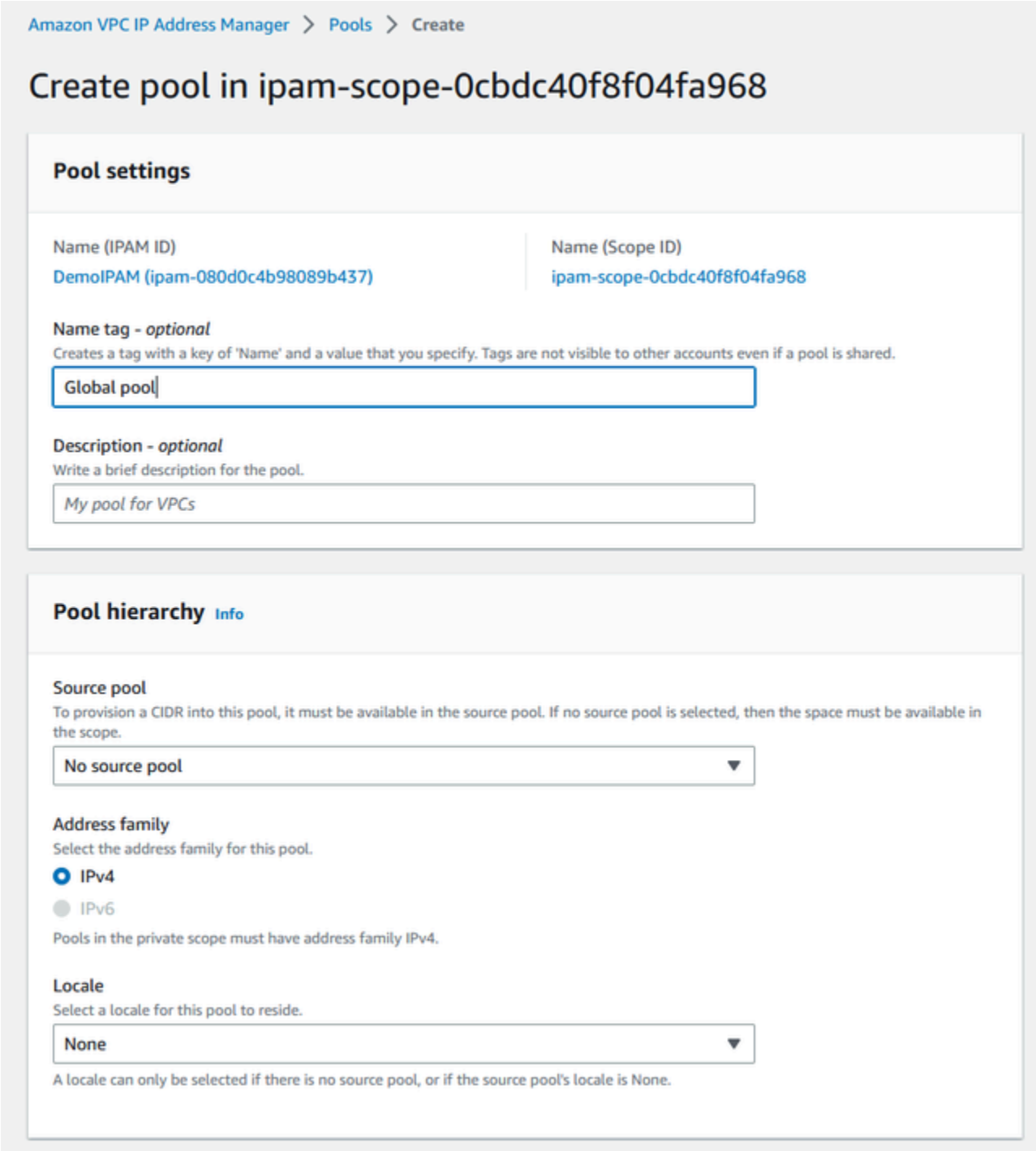
最上位のプールを作成するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。

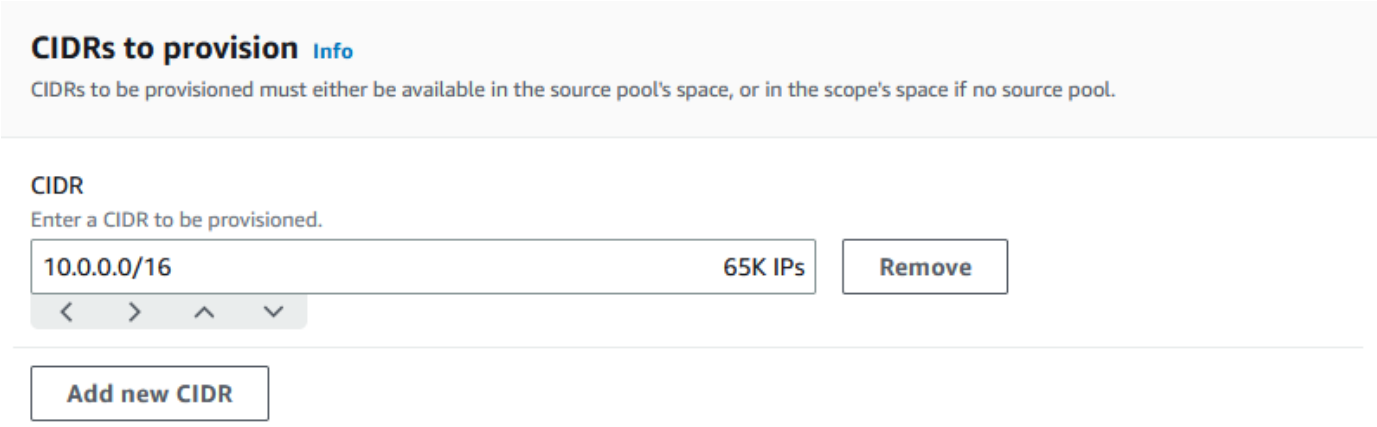
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択します。



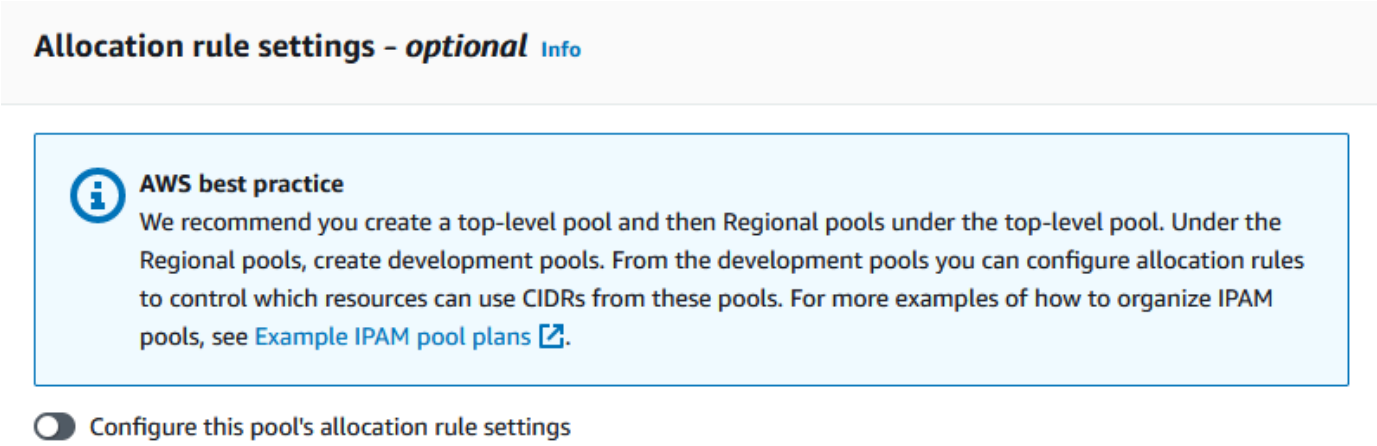
4. [プールを作成] を選択します。
5. [IPAM スコープ] では、プライベートスコープを選択したままにします。
6. (オプション) プールの [名前タグ] とプールの説明 (「グローバルプール」など) を追加します。
7. [ソース]で [IPAM 範囲] を選択します。こちらは最上位のプールであるためソースプールはありません。
8. [アドレスファミリー] には [IPv4] を選択します。
9. [リソース計画] で、[範囲内のIP 空間計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
10. [Locale] (ロケール) で、[None] (なし) を選択します。ロケールは、この IPAM プールを割り当て可能にしようとしている AWS リージョンです。作成するリージョンプールのロケールは、本チュートリアルの次のセクションで設定します。



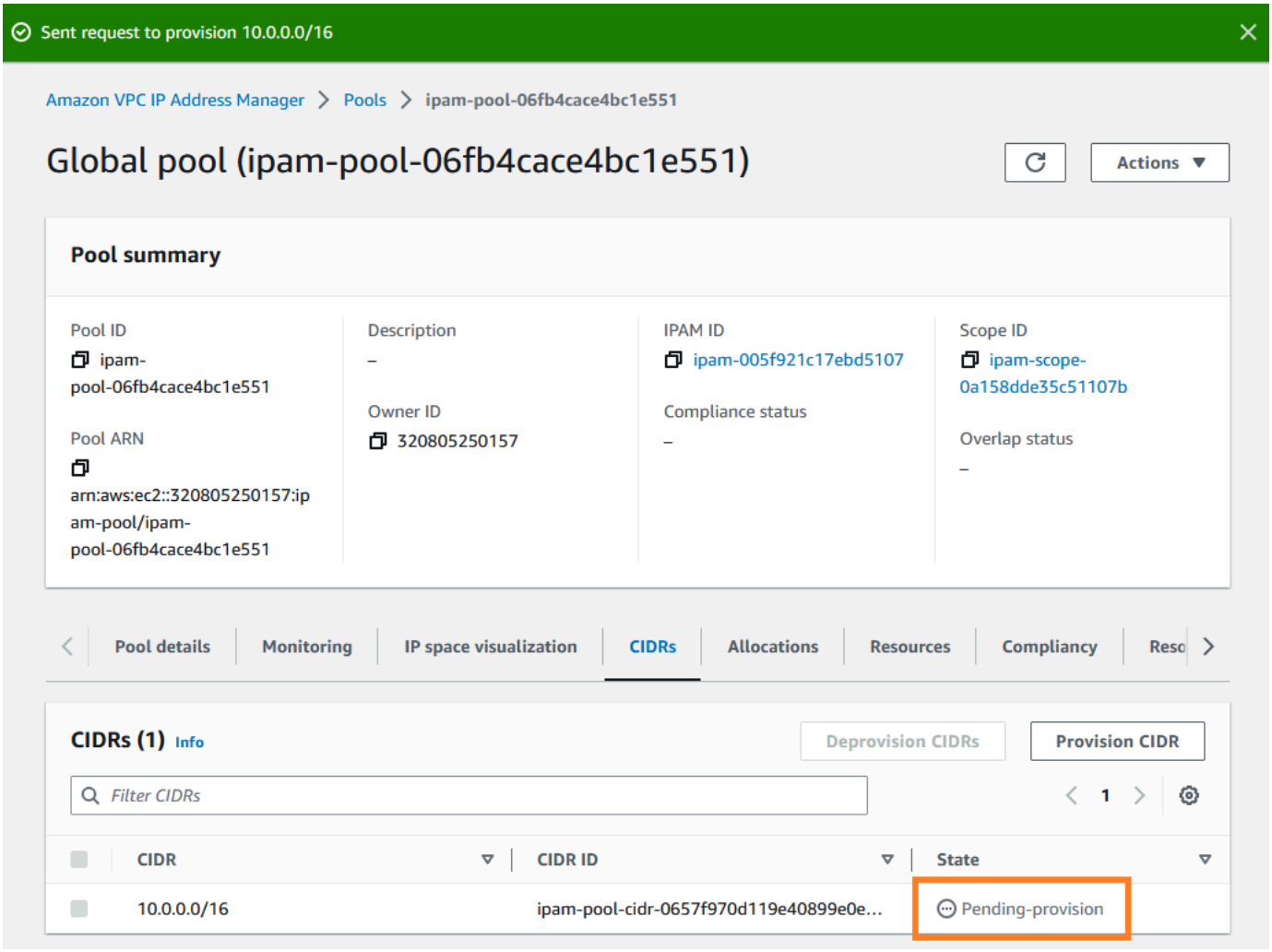
11. (オプション) プール用にプロビジョニングする CIDR を選択します。こちらの例では、10.0.0.0/16 をプロビジョニングします。



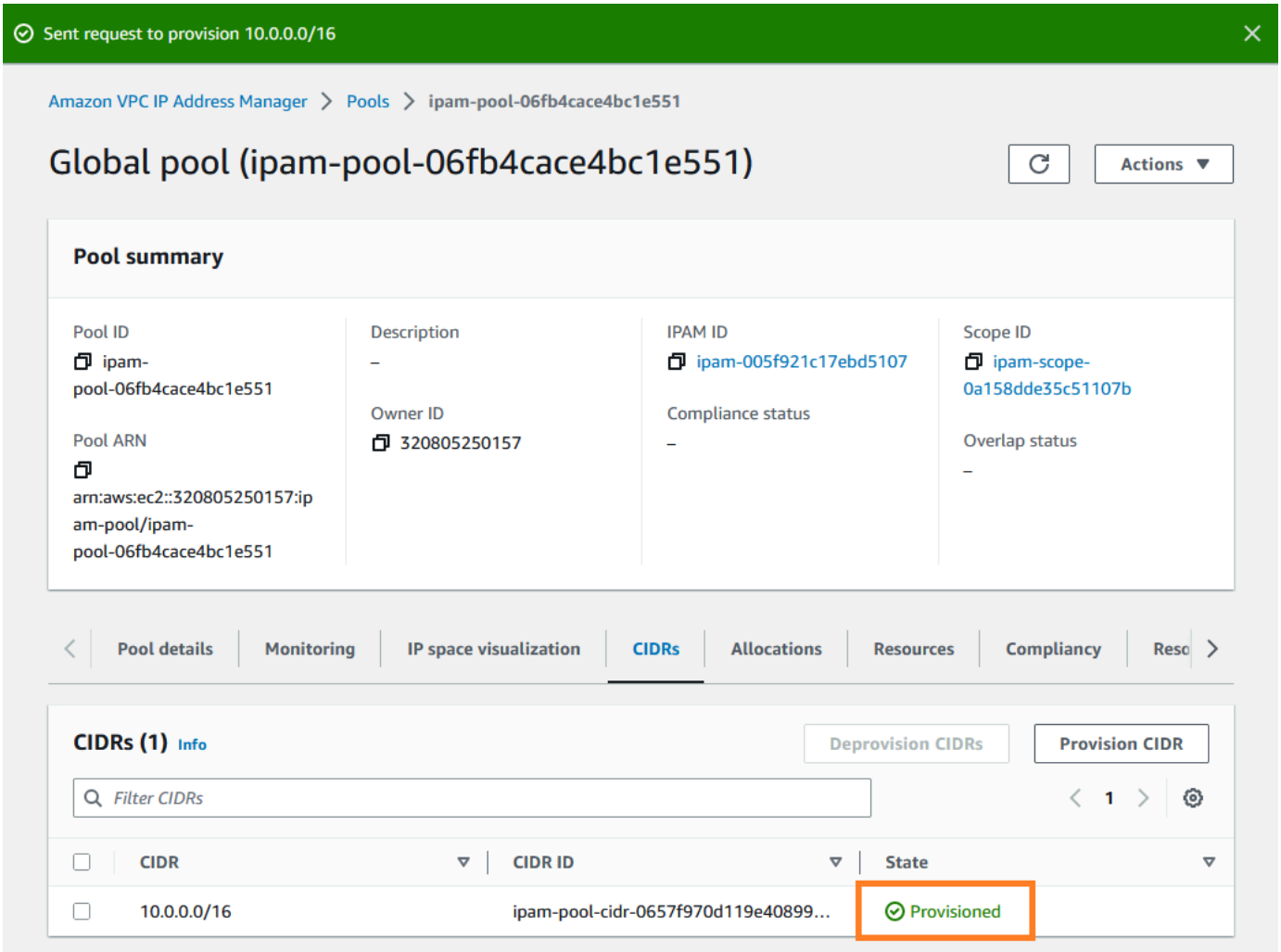
12. [このプールの割り当てルールを設定する] は無効のままにします。こちらは最上位のプールであり、このプールから VPC へ CIDR を直接割り当てることはできません。代わりに、このプールから作成したサブプールから、割り当てを行います。



13. [プールを作成] を選択します。プールが作成され、CIDR が [保留中のプロビジョン] 状態になります。



14. 状態が [プロビジョニング済み] に変わったら、次のステップに進みます。



最上位のプールが作成されたので、次に、us-west-1 と us-west-2 にリージョンプールを作成します。

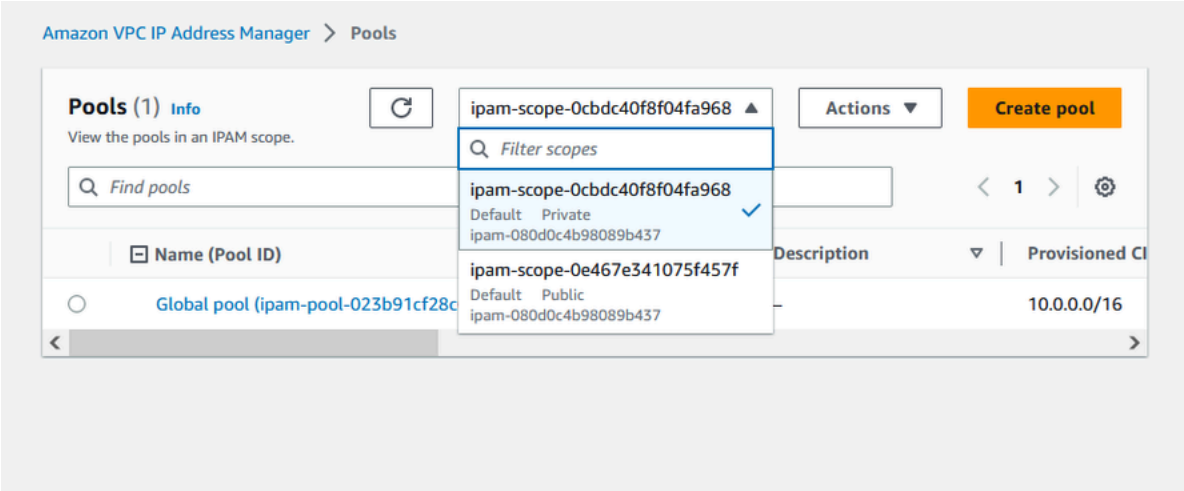
ステップ 4: リージョンの IPAM プールを作成する

このセクションでは、2 つのリージョンプールを使用して IP アドレスを整理する方法について説明します。このチュートリアルでは、IPAM プールプラン例の 1 つに従い、組織内のメンバーアカウントが VPC に CIDR を割り当てるときに使用できる、2 つのリージョンプールを作成します。

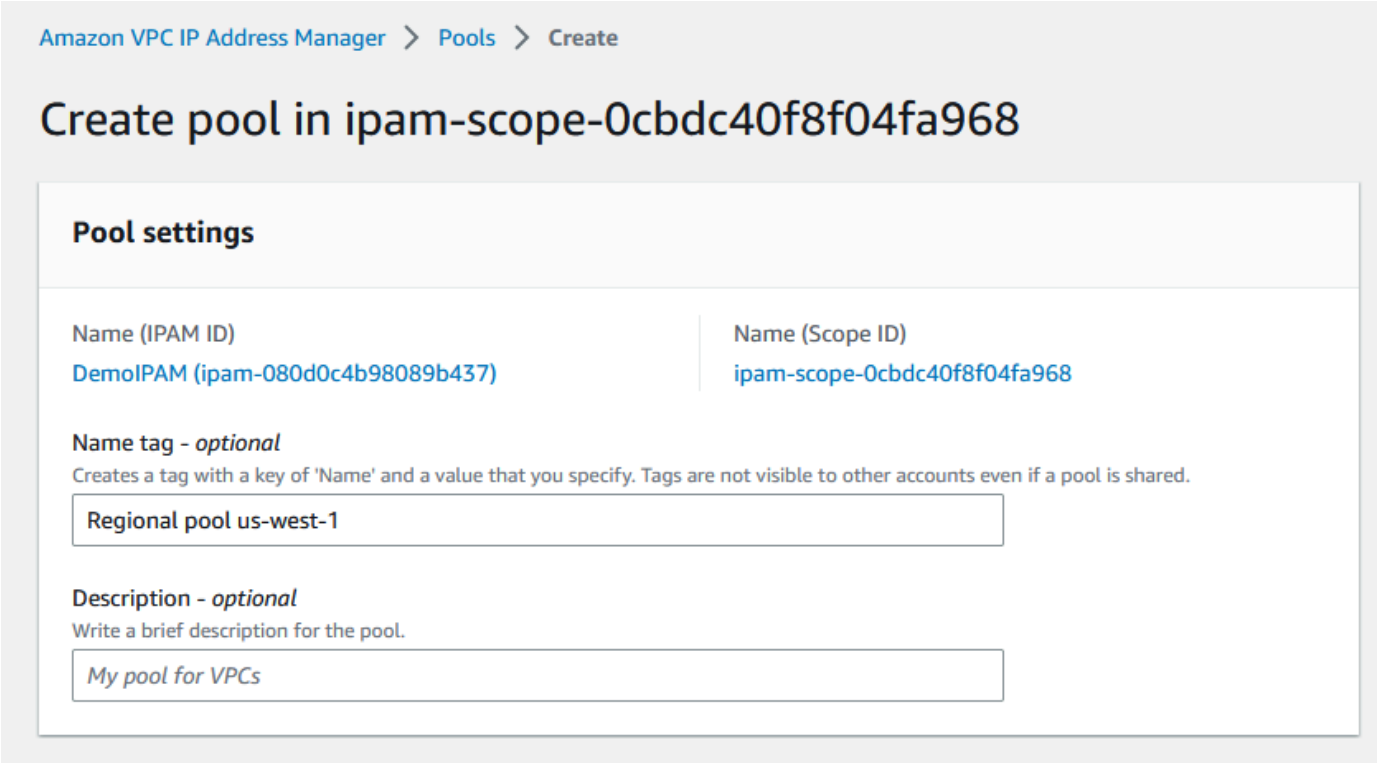
リージョンプールを作成するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。

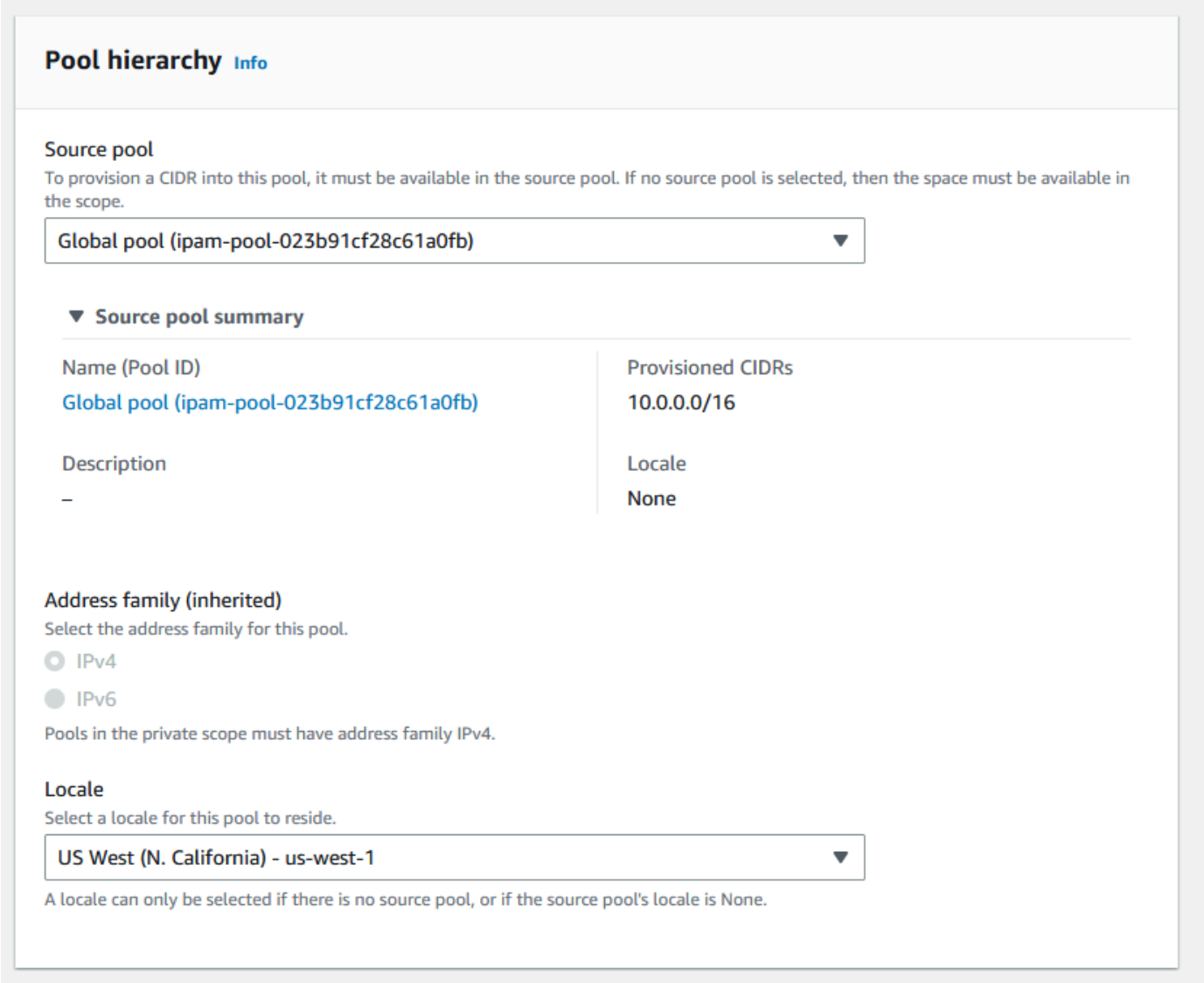
3. プライベートスコープを選択します。



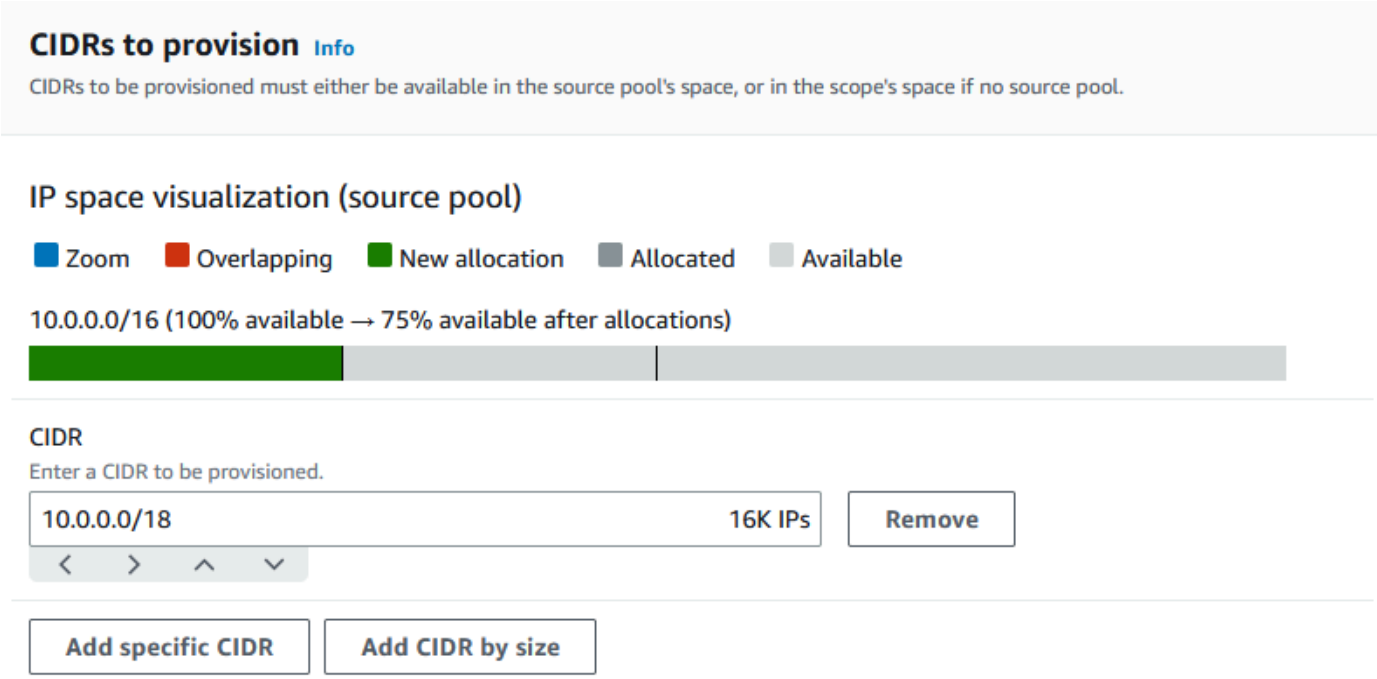
4. [プールを作成] を選択します。
5. [IPAM スコープ] では、プライベートスコープを選択したままにします。
6. (オプション) プールの [名前タグ] と、プールの説明 (Regional pool us-west-1 など) を追加します。



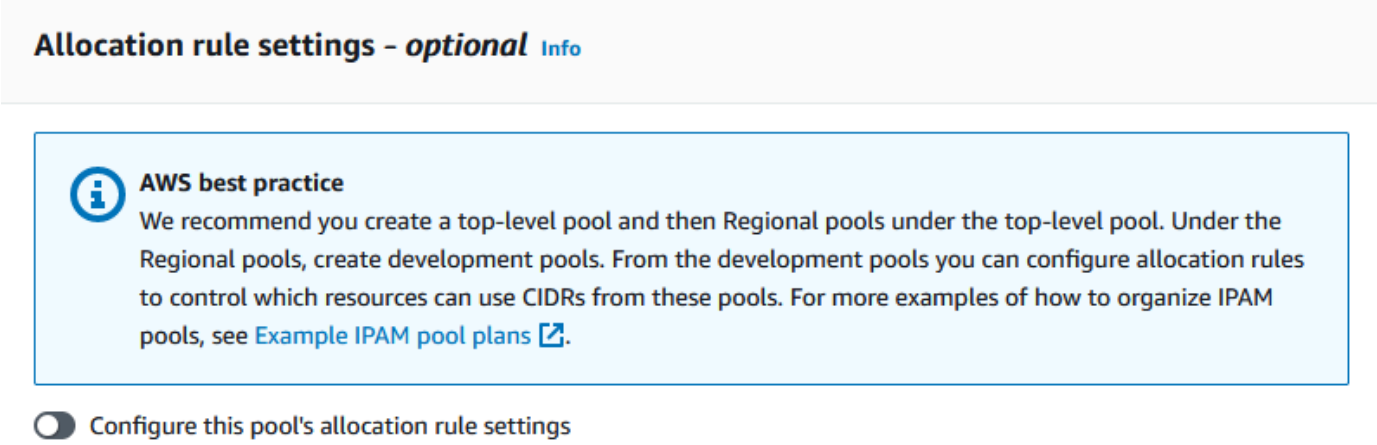
7. [ソース] で、[IPAM プール] を選択し、「ステップ 3: 最上位の IPAM プールの作成する」で作成した最上位のプール (「グローバルプール」) を選択します。次に、[ロケール] で us-west-1 を選択します。



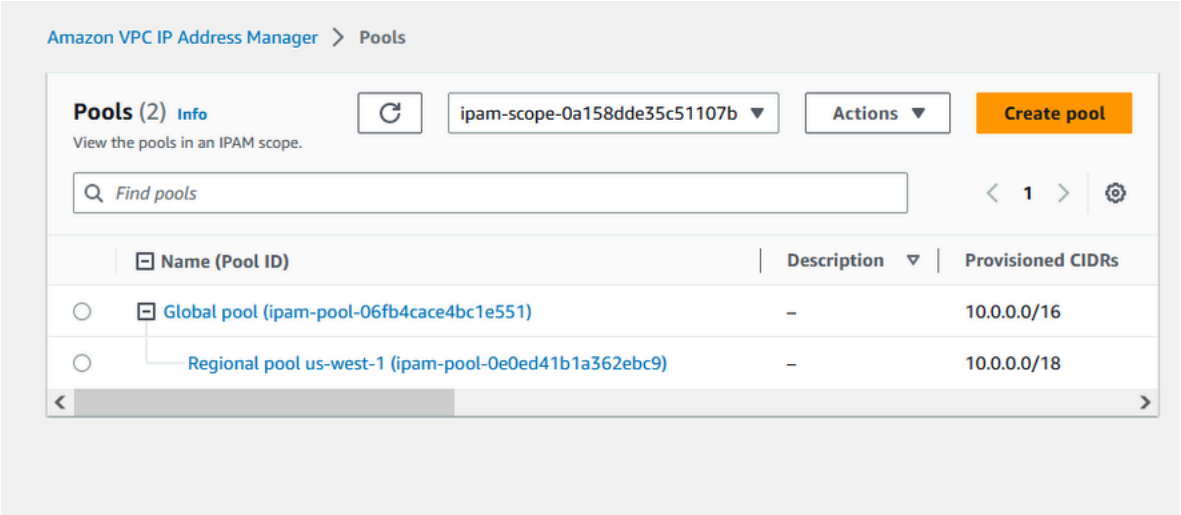
8. [リソース計画] で、[範囲内の IP スペースを計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
9. [プロビジョニングする CIDR] に 10.0.0.0/18 と入力します。これにより、このプールで約 16,000 の IP アドレスが利用できるようになります。



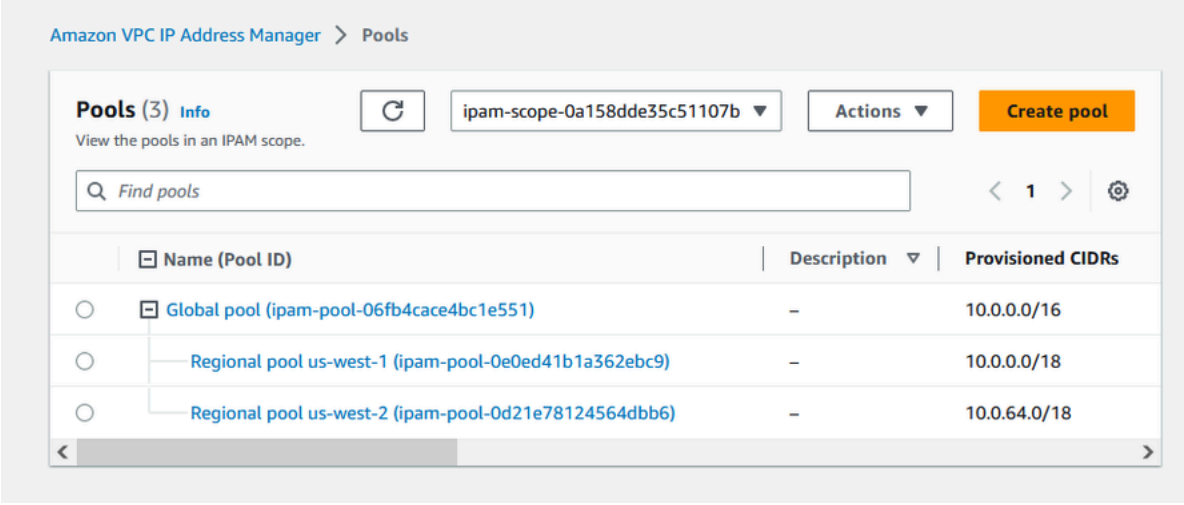
10. [このプールの割り当てルールを設定する] は無効のままにします。このプールから VPC へ CIDR を直接割り当てることはできません。代わりに、このプールから作成したサブプールから、割り当てを行います。



11. [プールを作成] を選択します。
12. [プール] 画面に戻ると、作成した IPAM プールの階層を確認できます。



13. このセクションのステップを繰り返し、us-west-2 ロケールに、それのためにプロビジョニングされた CIDR 10.0.64.0/18 を使って、2 つ目のリージョンプールを作成します。このプロセスを完了すると、次のように、階層に 3 つのプールが完成しています。

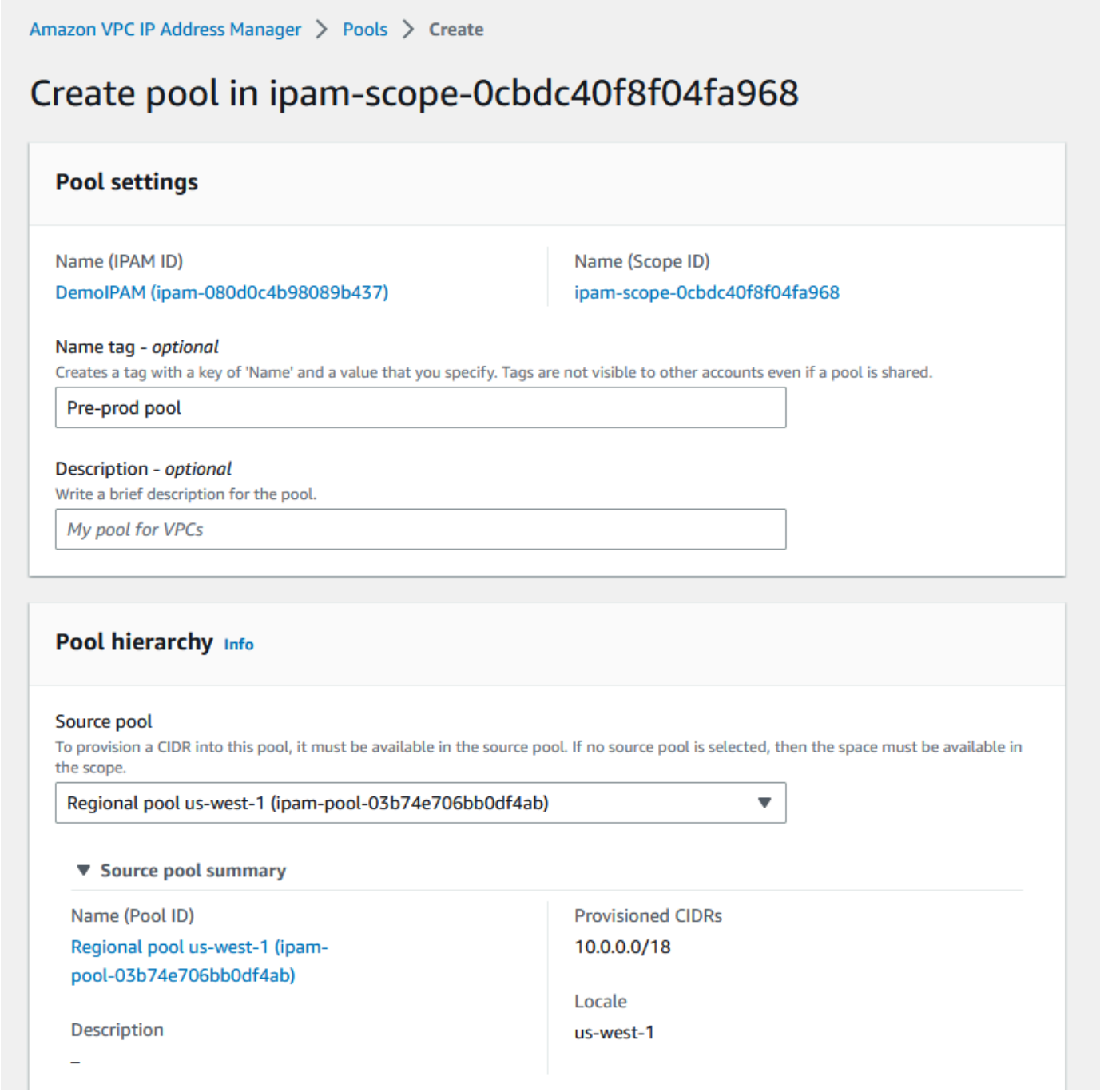


ステップ 5: 本番稼働前の開発プールを作成する

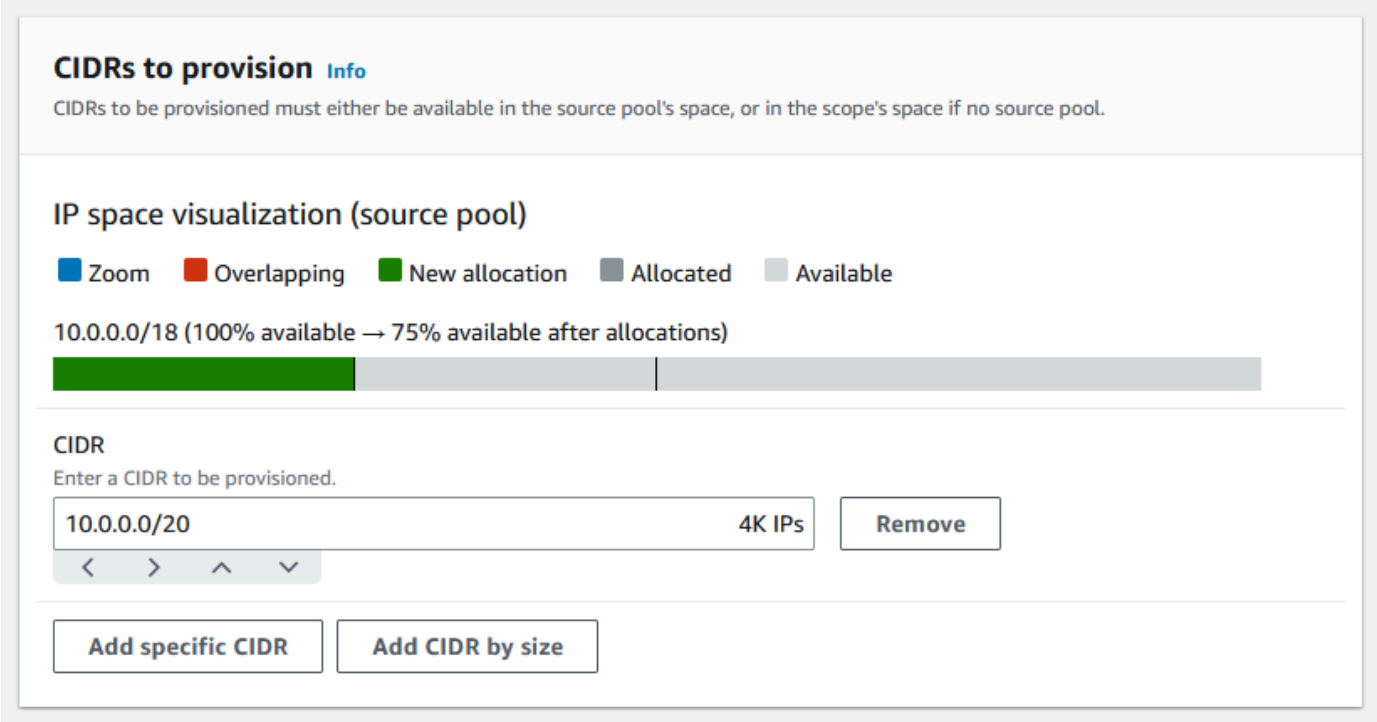
このセクションのステップに従って、いずれかのリージョンプールに、本番稼働前のリソース用の開発プールを作成します。

本番稼働前の開発プールを作成するには

1. 前のセクションで行った方法と同じ方法で、IPAM の管理者アカウントを使用して Pre-prod pool という名前のプールを作成します。ただし、ここではソースプールに Regional pool us-west-1 を使用します。

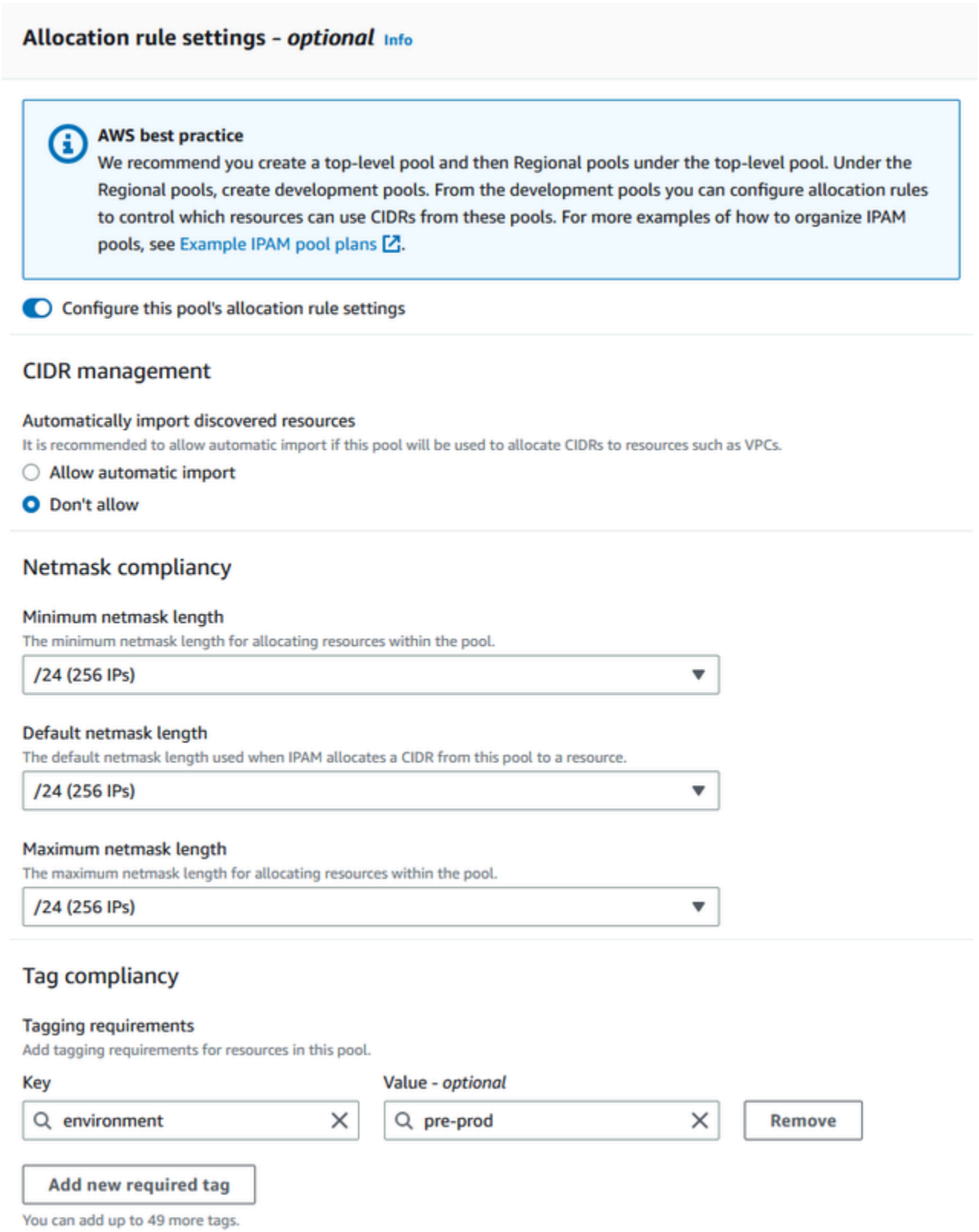


2. プロビジョニングする CIDR を 10.0.0.0/20 に指定します。これで、このプールに約 4,000 の IP アドレスが付与されます。



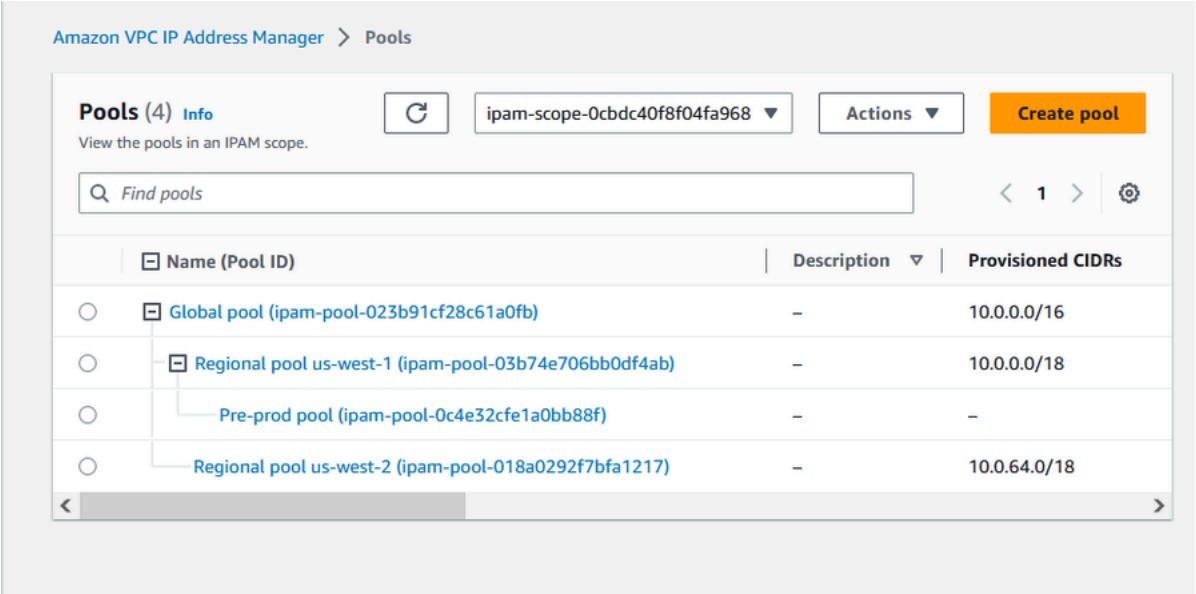
3. [このプールの割り当てルールを設定する] のオプションを切り替えます。以下の操作を実行します。

   1. [CIDR 管理] の [検出されたリソースを自動的にインポート] は、デフォルトの [許可しない] を選択したままにします。これを選択しておくことで、IPAM は、プールの口ケールで検出したリソース CIDR を、自動的にインポートすることができます。このオプションの詳しい説明は本チュートリアルの対象外ですが、詳細は「トップレベル IPv4 プールを作成する」でご覧いただけます。
   2. [ネットマスクのコンプライアンス] で、最小、デフォルト、最大のネットマスクの長さとして、[/24] を選択します。このオプションの詳しい説明は本チュートリアルの対象外ですが、詳細は「トップレベル IPv4 プールを作成する」でご覧いただけます。注意すべき点は、後ほどこのプールの CIDR を使用して作成する VPC は、ここでの設定に基づき、/24 に制限されるということです。
   3. [タグコンプライアンス] に environment/pre-prod と入力します。このタグは、VPC がプールからスペースを割り当てるときに必要になります。この仕組みについては、後ほど説明します。



4. [プールを作成] を選択します。

5. プール階層の Regional pool us-west-1 の下に、新たにサブプールが追加されました。



これで、組織内の別のメンバーアカウントと IPAM プールを共有し、そのアカウントでプールから CIDR を割り当て、VPC を作成する準備が整いました。

ステップ 6: IPAM プールを共有する

このセクションのステップに従って、AWS Resource Access Manager (RAM) を使用して本番稼働前の IPAM プールを共有します。

このセクションは 2 つのサブセクションから構成されています。

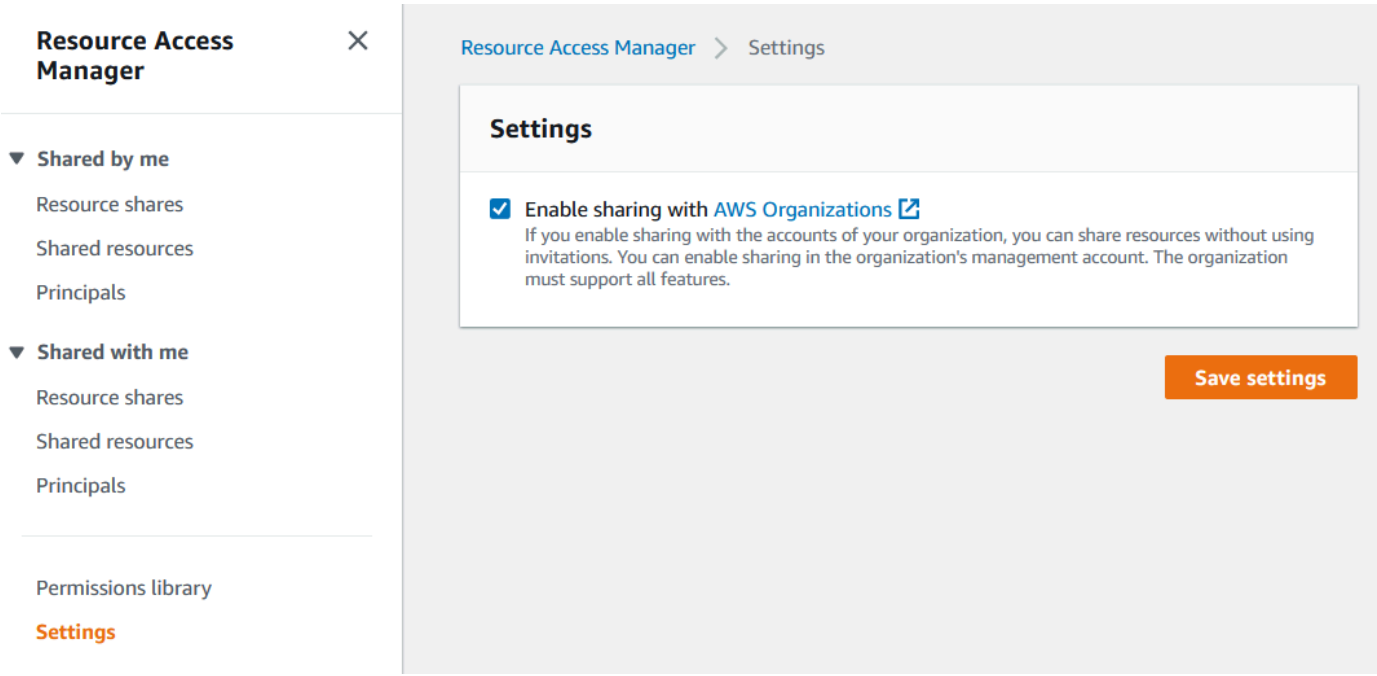
- ステップ 6.1. AWS RAM 内でリソース共有を有効にする: このステップは AWS Organizations 管理アカウントが実行します。
- ステップ 6.2. AWS RAM を使用して IPAM プールを共有する: このステップは、IPAM の管理者が実行します。

ステップ 6.1. AWS RAM 内でリソース共有を有効にする

IPAM を作成したら、IP アドレスプールを組織内の他のアカウントと共有する必要があります。IPAM プールを共有する前に、このセクションのステップを完了し、AWS RAM とのリソース共有を有効にします。

リソース共有を有効にするには

1. AWS Organizations 管理アカウントを使って AWS RAM コンソール (https://console.aws.amazon.com/ram/) を開きます。
2. ナビゲーションペインで [設定] を選択し、[AWS Organizations との共有を有効にする] を選択し、[設定の保存] を選択します。



これで、IPAM プールを組織の他のメンバーと共有できるようになりました。

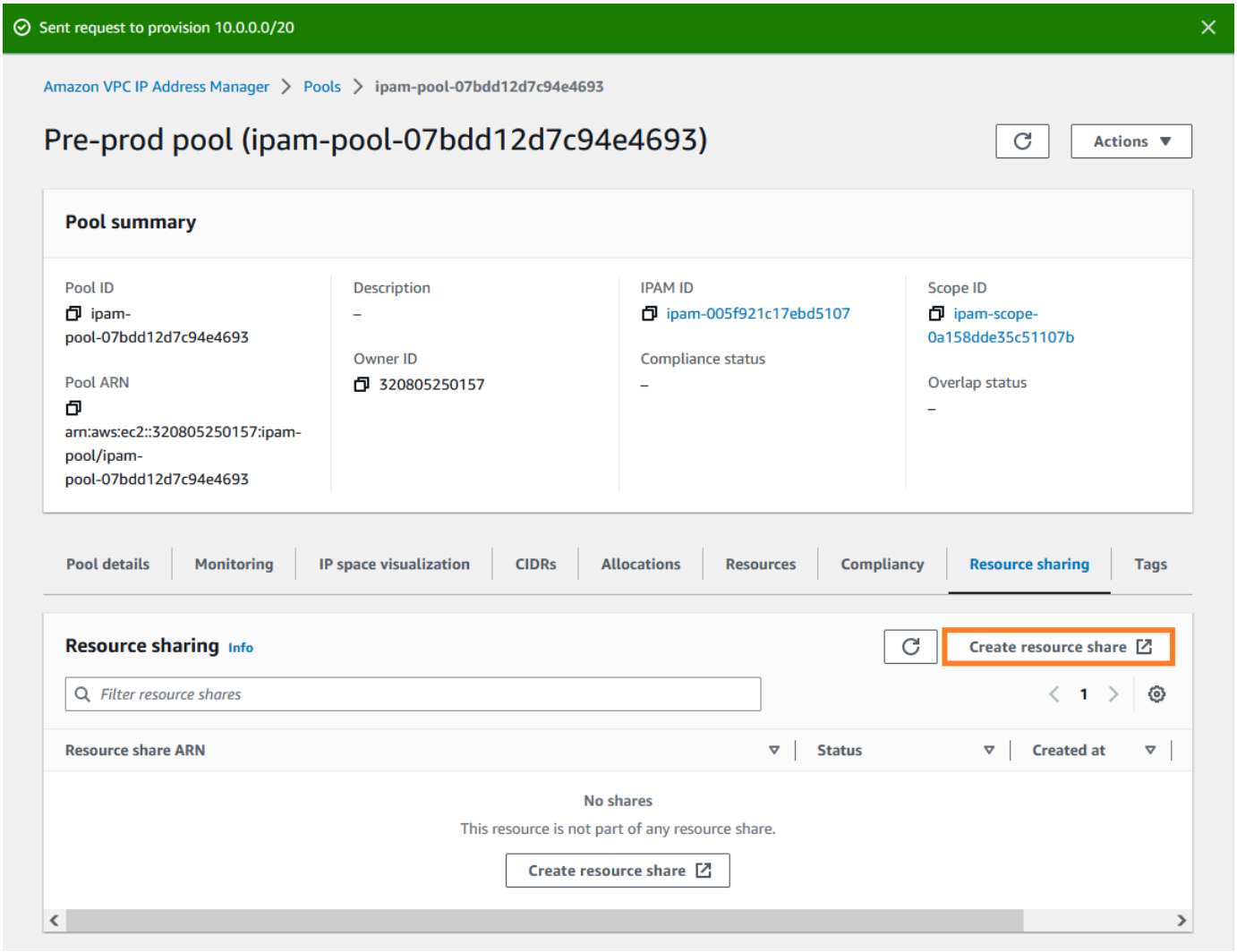
ステップ 6.2. AWS RAM を使用して IPAM プールを共有する

このセクションでは、本番稼働前開発プールを他の AWS Organizations メンバーアカウントと共有します。必要な IAM アクセス許可に関する情報を含め、IPAM プールの共有に関する詳細な手順については、「AWS RAM を使用して IPAM プールを共有する」を参照してください。

AWS RAM を使用して IPAM プールを共有するには

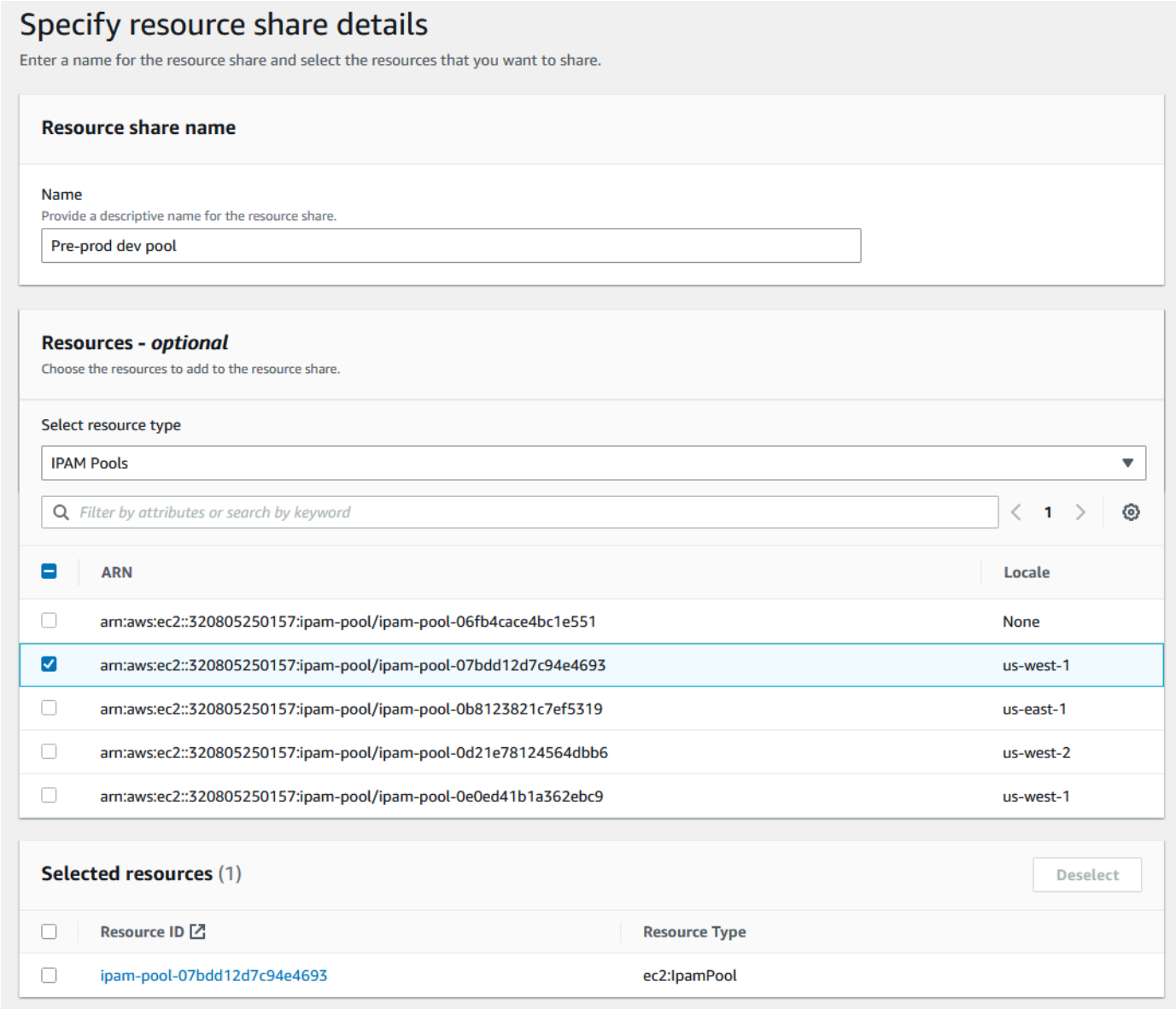
1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択し、本番稼働前の IPAM プールを選択して、[アクション] > [詳細を表示] の順に選択します。

4. [Resource sharing] (リソース共有) で [Create resource share] (リソース共有の作成) を選択します。AWS RAM コンソールが開きます。AWS RAM を使用してプールを共有します。
5. [リソースの共有の作成] を選択します。

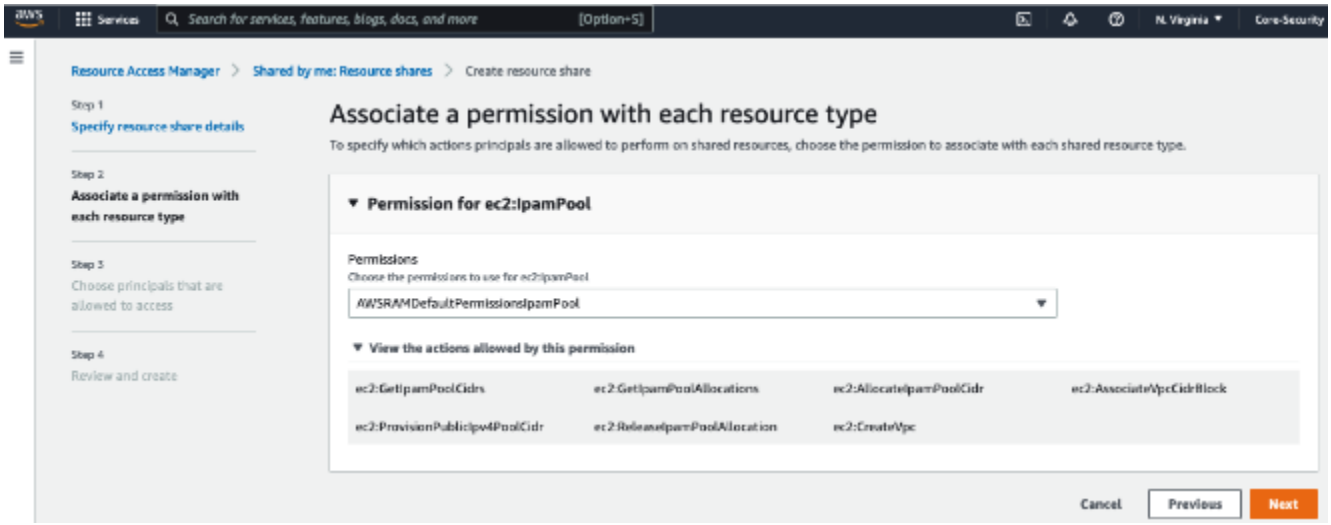


AWS RAM コンソールが開きます。

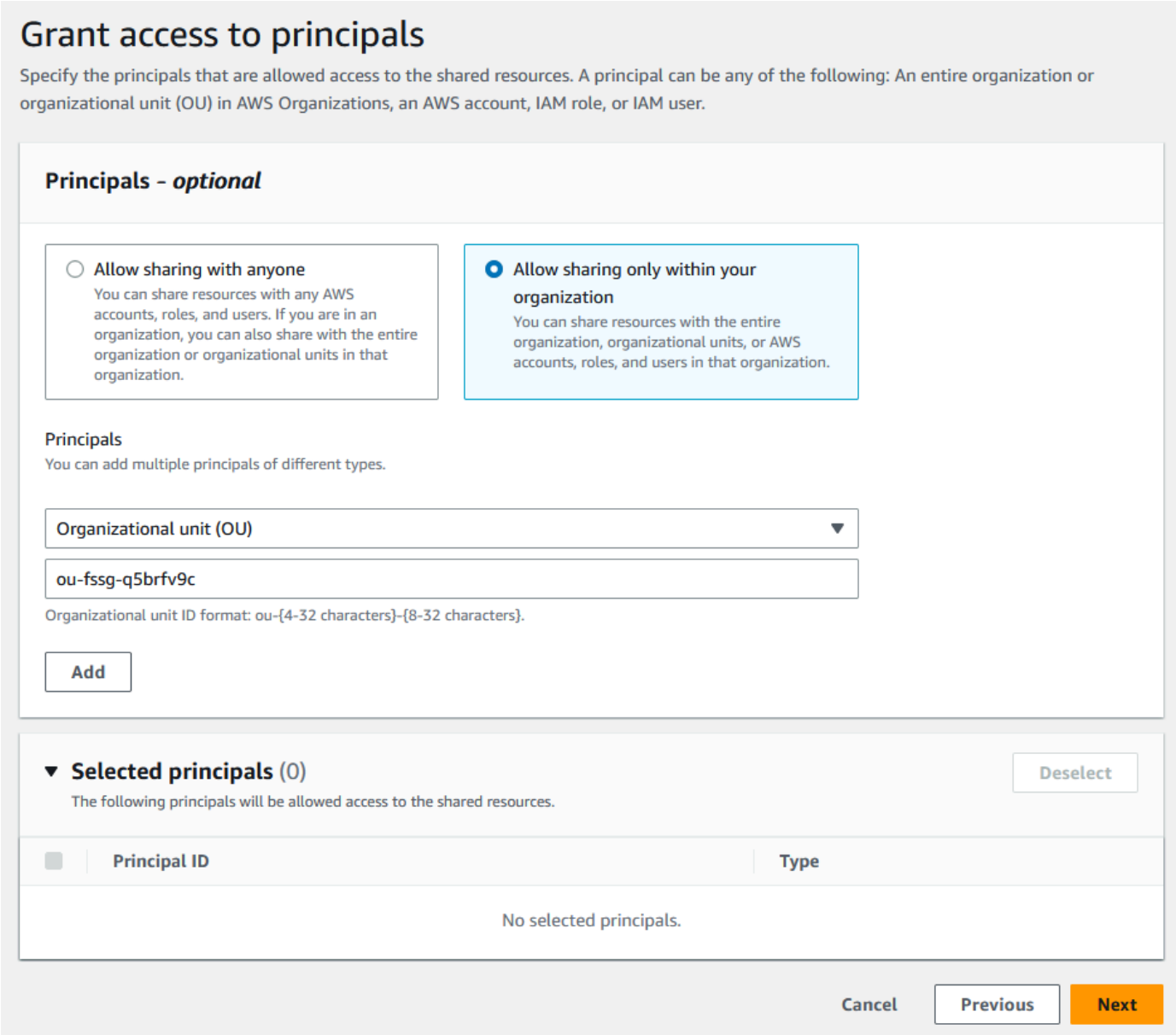
6. AWS RAM コンソールで、[リソースの共有を作成] を再度選択します。
7. 共有リソースの [名前] を追加します。
8. [リソースタイプを選択] で [IPAM プール] を選択し、次に、本番稼働前開発プールの ARN を選択します。



9. [次へ] を選択します。
10. デフォルトの AWSRAMDefaultPermissionsIpamPool アクセス許可を選択したままにしておきます。アクセス許可オプションの詳細は本チュートリアルの対象外ですが、このオプションの詳細は「AWS RAM を使用して IPAM プールを共有する」にてご覧いただけます。



11. [次へ] を選択します。
12. [プリンシパル] で [自分の組織内でのみ共有を許可] を選択します。AWS Organizations 組織単位 ID を入力し (「AWS Organizations を IPAM と統合する方法」の説明のとおり)、[追加] を選択します。



13. [次へ] を選択します。
14. リソース共有オプションと共有先のプリンシパルを確認し、[作成] を選択します。

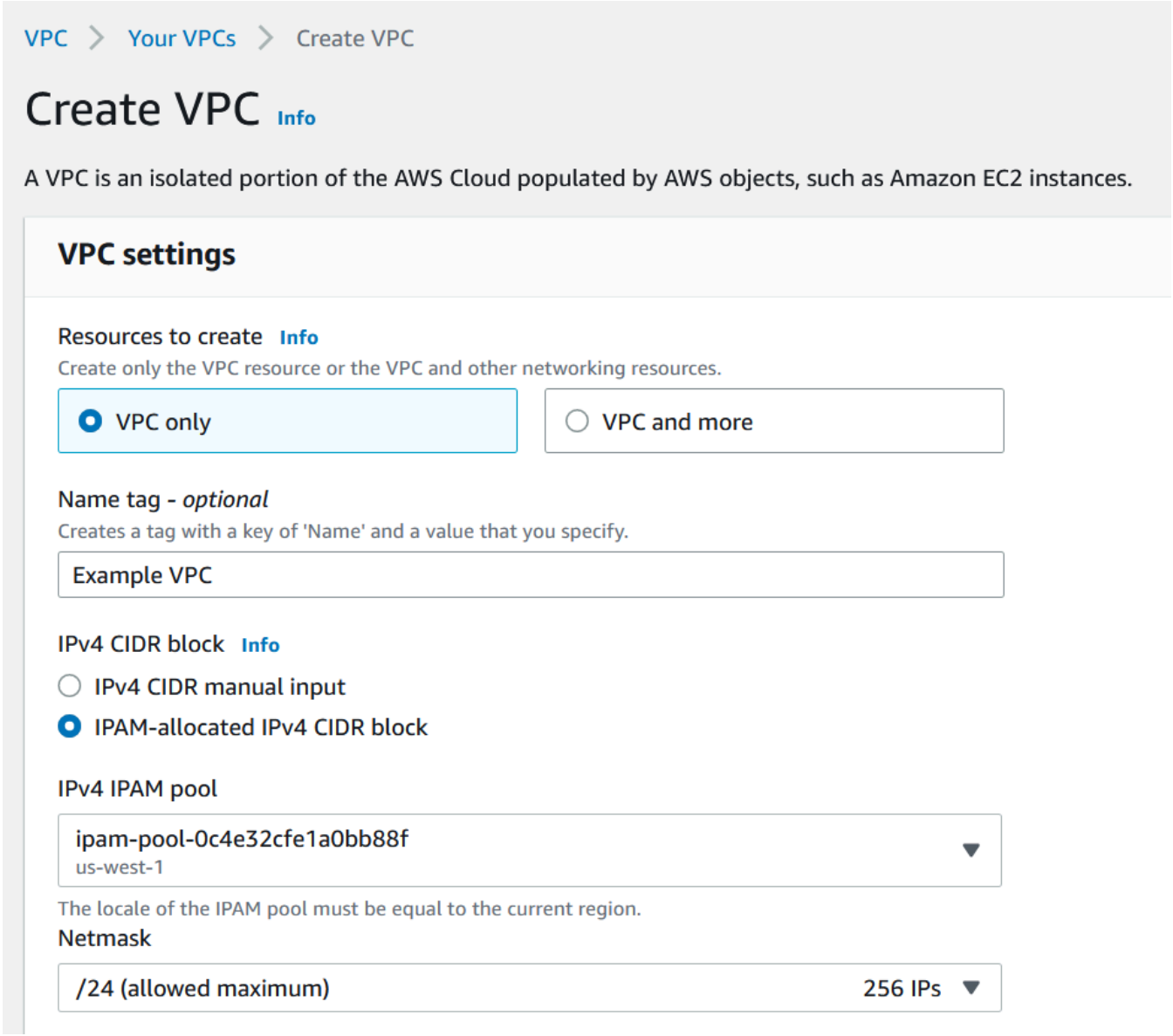
プールが共有されたので、次のステップで、IPAM プールから割り当てられた CIDR を使って VPC を作成します。

ステップ 7: IPAM プールから割り当てられた CIDR を使用して VPC を作成する

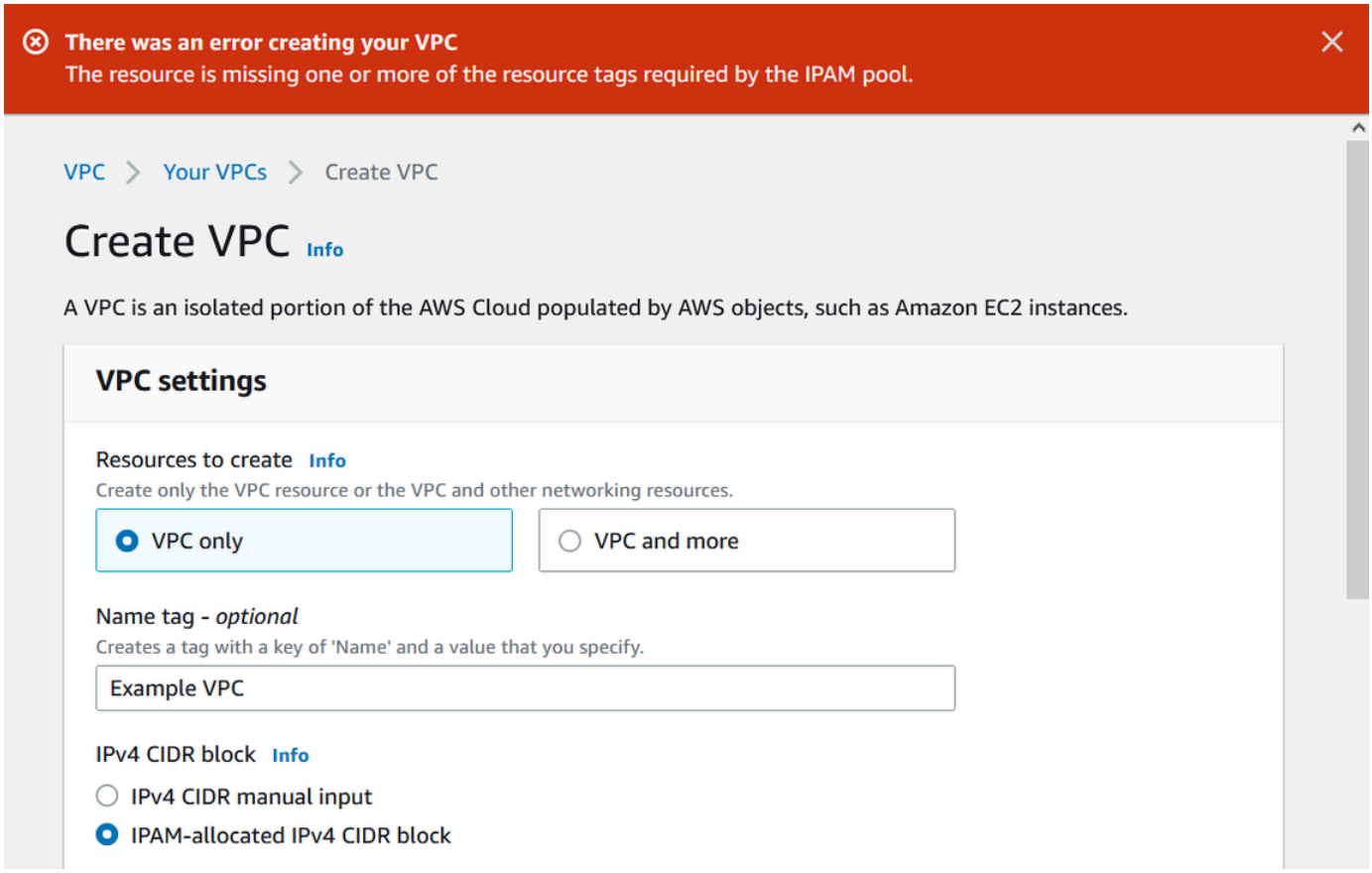
このセクションのステップに従って、本番稼働前のプールから割り当てられた CIDR を使って VPC を作成します。このステップは、前のセクションで IPAM プールが共有された、OU のメンバーアカウント (「AWS Organizations を IPAM と統合する方法」の example-member-account-2) が実行する必要があります。VPC の作成に必要な IAM アクセス許可の詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC ポリシーの例」を参照してください。

IPAM プールから割り当てられた CIDR を使って VPC を作成するには

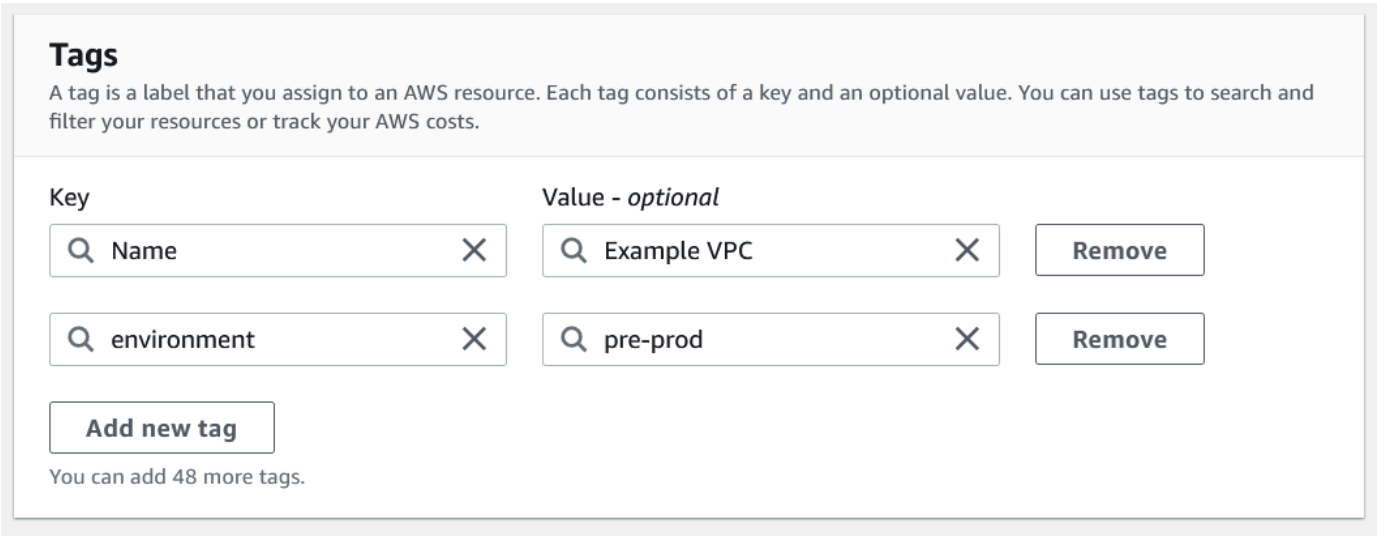
1. メンバーアカウントを使用して、デベロッパーアカウントとして使用するメンバーアカウントとして VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. [Create VPC (VPC の作成)] を選択します。
3. 以下の操作を実行します。
    1. 名前 (Example VPC など) を入力します。
    2. [IPAM が割り当てられた IPv4 CIDR ブロック] を選択します。
    3. [IPv4 IPAM プール] で本番稼働前プールの ID を選択します。
    4. [ネットマスク] の長さを選択します。このプールで使用できるネットマスクの長さは (「ステップ 5: 本番稼働前の開発プールを作成する」で) /24 に制限されているため、選択可能なオプションは /24 のみです。



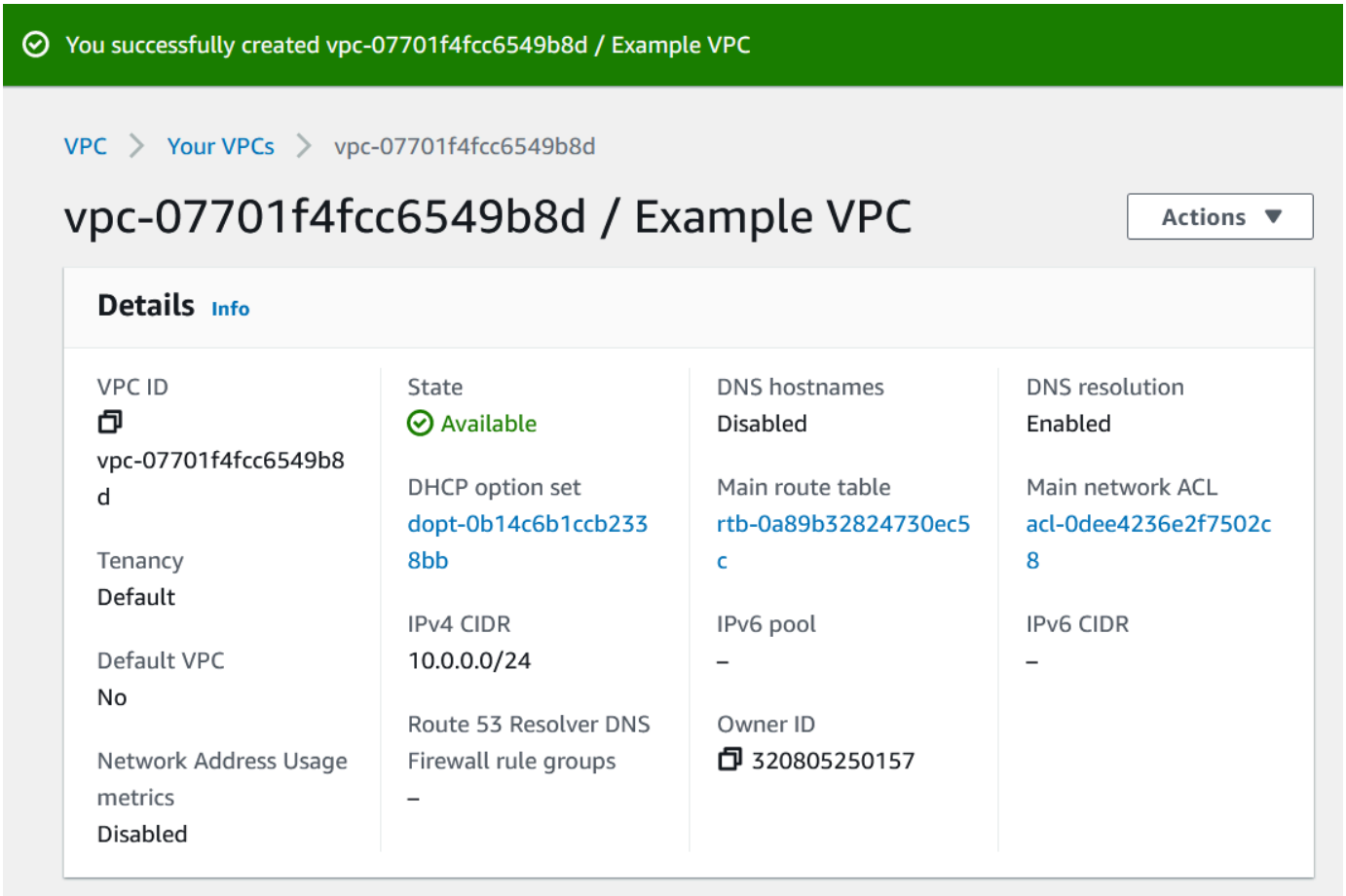
4. 例として示すため、この時点では、[タグ] 下にいずれのタグも追加しません。(「ステップ 5: 本番稼働前の開発プールを作成する」で) 本番稼働前のプールを作成した際に、このプールの CIDR を使って作成した VPC には environment/pre-prod タグを付けなければならない、という割り当てルールを追加しました。ここでは、必要なタグが付いていないことを示すエラーを確認できるようにするため、environment/pre-prod タグは付けずに次へ進みます。
5. [Create VPC (VPC の作成)] を選択します。
6. 必要なタグが追加されていないことを示すエラーが表示されます。このエラーは、本番稼働前プールを作成したとき (「ステップ 5: 本番稼働前の開発プールを作成する」) に割り当てルールを設定したため、表示されています。この割り当てルールは、このプールの CIDR を使って作成されるすべての VPC に、environment/pre-prod タグを付けることを要求していました。



7. 次に、[タグ] で、タグ environment/pre-prod を追加し、[VPC を作成] を再度選択します。



8. VPC が正常に作成されました。この VPC は、本番稼働前プールのタグルールに準拠しています。



IPAM コンソールの [リソース] ペインでは、IPAM の管理者は、VPC とそこに割り当てられた CIDR を閲覧し、管理することができます。VPC が [リソース] ペインに表示されるまで、しばらく時間がかかる場合があります。

ステップ 8: クリーンアップ

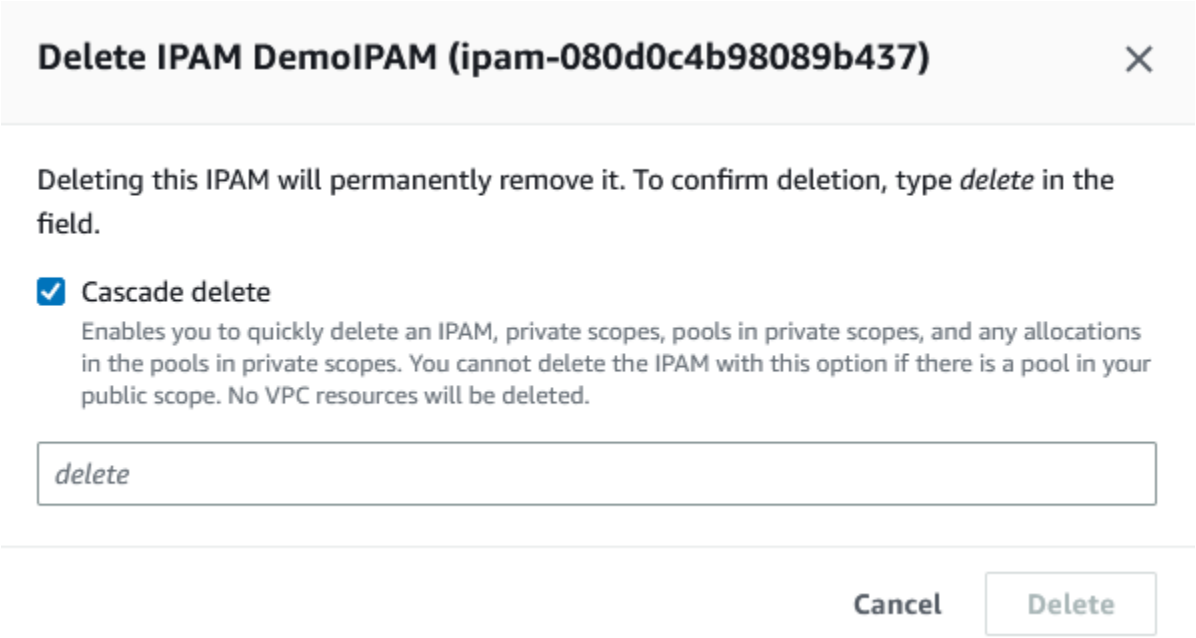
このチュートリアルでは、委任された管理者を含む IPAM を作成し、複数のプールを作成して、プールから VPC CIDR を割り当てることを組織のメンバーアカウントに許可しました。

このセクションのステップに従って、このチュートリアルで作成したリソースをクリーンアップします。

このチュートリアルで作成したリソースをクリーンアップするには

1. サンプルの VPC を作成したメンバーアカウントを使用して、VPC を削除します。詳細な手順については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPC の削除」を参照してください。

2. IPAM の管理者アカウントを使用して、AWS RAM コンソールのサンプルのリソース共有を削除します。詳細な手順については、「AWS Resource Access Manager ユーザーガイド」にアクセスし、「AWSAWS RAM のリソース共有の削除」を参照してください。
3. IPAM の管理者アカウントを使用して RAM コンソールにログインし、「ステップ 6.1. AWS RAM 内でリソース共有を有効にする」で有効にした AWS Organizations との共有を、無効にします。
4. IPAM の管理者アカウントを使用して、IPAM コンソールで IPAM を選択し、[アクション] > [削除] の順に選択してサンプルの IPAM を削除します。詳細な手順については、「IPAM を削除する」を参照してください。
5. IPAM の削除を求めるメッセージが表示されたら、[カスケード削除] を選択します。これで、IPAM を削除する前に、IPAM 内のすべてのスコープとプールが削除されます。



6. delete と入力し、[削除] を選択します。
7. AWS Organizations 管理アカウントを使用して IPAM コンソールにログインし、[設定] を選択して、委任された管理者アカウントを削除します。
8. (オプション) IPAM を AWS Organizations と統合すると、IPAM は、サービスリンクロールを各メンバーアカウントに自動的に作成します。各 AWS Organizations メンバーアカウントを使用して IAM にログインし、各メンバーアカウントの AWSServiceRoleForIPAM サービスにリンクされたロールを削除します。
9. これで、クリーンアップは完了です。

チュートリアル: AWS CLI を使用して IPAM とプールを作成する

このチュートリアルのステップに従って、AWS CLI を使用して IPAM を作成し、IP アドレスプールを作成して、IPAM プールの CIDR を使って VPC を割り当てます。

次に、このセクションのステップに従って作成するプール構造の階層の例を示します。

- AWS リージョン 1、AWS リージョン 2 で運用されているIPAM
  - プライベートスコープ
    - 最上位プール
      - AWS リージョン 2 のリージョンプール
        - 開発プール
          - VPC の割り当て

> **Note**
>
> このセクションでは、IPAM を作成します。デフォルトでは、作成できる IPAM は 1 つだけです。詳細については、「IPAM のクォータ」を参照してください。既に IPAM アカウントを委任し、IPAM を作成済みの場合は、ステップ 1 と 2 をスキップできます。

内容

ステップ 1: 組織で IPAM を有効にする

この手順は省略可能です。このステップを実行して、AWS CLI を使用して組織で IPAM を有効にし、委任された IPAM を構成します。IPAM アカウントのロールの詳細については、IPAM を AWS Organizations 内のアカウントと統合する を参照してください。

このリクエストは、AWS Organizations 管理アカウントから行われる必要があります。次のコマンドを実行するときは、以下のアクションを許可する IAM ポリシーを持つロールを使用していることを確認します。

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

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

有効化に成功したことを示す次の出力が表示されます。

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

ステップ 2: IPAM を作成する

このセクションのステップに従って IPAM を作成し、作成されたスコープに関する追加情報を表示します。この IPAM は、後のステップでプールを作成し、それらのプールの IP アドレス範囲をプロビジョニングするときに使用します。

> **Note**
>
> 運用リージョンオプションによって、IPAM プールを使用できる AWS リージョンが決まります。運用リージョンの詳細については、IPAM を作成する を参照してください。

AWS CLI を使用して IPAM を作成するには

1. 次のコマンドを実行して IPAM インスタンスを作成します。

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

IPAM を作成すると、AWS は以下を自動的に実行します。

- IPAM のグローバルに一意のリソース ID (IpamId) を返します。
- デフォルトのパブリックスコープ (PublicDefaultScopeId) とデフォルトのプライベートスコープ (PrivateDefaultScopeId) を作成します。

```
{

    "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. 以下のコマンドを実行して、スコープに関連する追加情報を表示します。パブリックスコープは、パブリックインターネット経由でアクセスされる IP アドレスを対象としています。プライベートスコープは、パブリックインターネット経由でアクセスされない IP アドレスを対象としています。

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

出力には、使用可能なスコープが表示されます。次のステップでは、プライベートスコープ ID を使用します。

```
{
    "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
        }
    ]
}
```

ステップ 3: IPv4 アドレスプールを作成する

このセクションのステップに従って IPv4 アドレスプールを作成します。

> **Important**
>
> この最上位プールでは `--locale` オプションを使用しません。後ほどリージョンプールでロケールオプションを設定します。ロケールは、CIDR 割り振りのためにプールを利用可能とする AWS リージョンです。最上位レベルプールにロケールを設定しない結果、ロケール

はデフォルトで None になります。プールの口ケールが None の場合、プールはどの AWS リージョンの VPC リソースでも使用できません。スペースを予約するためにできるのは、プール内の IP アドレス空間を手動で割り振ることだけです。

AWS CLI を使用してすべての AWS リソースの IPv4 アドレスプールを作成するには

1. 以下のコマンドを実行して IPv4 アドレスプールを作成します。前のステップで作成した IPAM のプライベートスコープの ID を使用します。

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

出力には、プールの create-in-progress という状態が表示されます。

```
{
    "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. 出力に create-complete という状態が表示されるまで、次のコマンドを実行します。

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

以下の出力の例は、正しい状態を示しています。

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

ステップ 4: CIDR を最上位プールにプロビジョニングする

このセクションのステップに従って CIDR を最上位プールにプロビジョニングし、CIDR がプロビジョニングされていることを確認します。詳細については、「CIDR をプールにプロビジョニングする」を参照してください。

AWS CLI を使用して CIDR ブロックをプールにプロビジョニングするには

1. 以下のコマンドを実行して CIDR をプロビジョニングします。

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

出力では、プロビジョニングの状態を確認できます。

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

```
    }
}
```

2. 出力に provisioned という状態が表示されるまで、次のコマンドを実行します。

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

以下の出力の例は、正しい状態を示しています。

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

ステップ 5. 最上位プールから取得された CIDR を使用してリージョンプールを作成する

IPAM プールを作成すると、プールはデフォルトで IPAM の AWS リージョンに属します。VPC を作成するとき、VPC による取得元のプールは、VPC と同じリージョンに存在する必要があります。プールを作成するとき、--locale オプションを使用して、IPAM のリージョン以外のリージョンのサービスでプールを使用できるようにすることが可能です。このセクションのステップに従って、別の口ケールでリージョンプールを作成します。

AWS CLI を使用して、前のプールから取得された CIDR を使用してプールを作成するには

1. 次のコマンドを実行して、プールを作成し、前のプールから取得された既知の使用可能な CIDR を持つスペースを挿入します。

```
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
```

出力には、作成したプールの ID が表示されます。この ID は次のステップで必要になります。

```
{
    "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. 出力に create-complete という状態が表示されるまで、次のコマンドを実行します。

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

出力には、IPAM にあるプールが表示されます。このチュートリアルでは、最上位プールとリージョンプールを作成したので、両方が表示されます。

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


ステップ 6: リージョンプールに CIDR をプロビジョニングする

このセクションの手順に従って、CIDR ブロックをプールに割り当てて、正常にプロビジョニングされたことを検証します。

AWS CLI を使用して CIDR ブロックをリージョンプールに割り当てるには

1. 以下のコマンドを実行して CIDR をプロビジョニングします。

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

出力には、プールの状態が表示されます。


```
{
    "IpamPoolCidr": {
```

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

2. 出力に provisioned という状態が表示されるまで、次のコマンドを実行します。

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

以下の出力の例は、正しい状態を示しています。

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

3. 以下のコマンドを実行して、最上位プールをクエリして割り当てを表示します。リージョンプールは、最上位プール内の割り当てと見なされます。

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

出力では、最上位プール内の割り当てとしてリージョンプールが表示されます。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "10.0.0.0/16",
            "IpamPoolAllocationId": "ipam-pool-alloc-
fbd525f6c2bf4e77a75690fc2d93479a",
            "ResourceId": "ipam-pool-0da89c821626f1e4b",
            "ResourceType": "ipam-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

ステップ 7. アカウント間の IP 割り当てを有効にするために RAM 共有を作成する

この手順は省略可能です。このステップは、IPAM を AWS Organizations 内のアカウントと統合するを完了した場合にのみ完了できます。

IPAM プールの AWS RAM 共有を作成すると、アカウント間の IP 割り当てが有効になります。RAM 共有は、ホーム AWS リージョンでのみ使用できます。この共有は、プールのローカルリージョンではなく、IPAM と同じリージョンに作成することに注意してください。IPAM リソースに対するすべての管理操作は、IPAM のホームリージョンを通じて行われます。このチュートリアルの例では 1 つのプールに対して 1 つの共有を作成しますが、1 つの共有に複数のプールを追加できます。入力する必要があるオプションの説明など、詳細については、AWS RAM を使用して IPAM プールを共有するを参照してください。

リソース共有を作成するには、以下のコマンドを実行します。

```
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
```

出力は、プールが作成されたことを示しています。

```
{
    "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
    }
}
```

ステップ 8. 「VPC を作成する」

次のコマンドを実行して VPC を作成し、新しく作成した IPAM 内のプールから VPC に CIDR ブロックを割り当てます。

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

出力は、VPC が作成されたことを示しています。

```
{
    "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
    }
}
```

ステップ 9. クリーンアップ

このセクションのステップに従って、このチュートリアルで作成した IPAM リソースを削除します。

1. VPC を削除します。

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

2. IPAM プールの RAM 共有を削除します。

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

3. リージョンプールからプール CIDR をプロビジョニング解除します。

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

4. 最上位プールからプール CIDR をプロビジョニング解除します。

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

5. IPAM を削除します。

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

チュートリアル: AWS CLI を使用して IP アドレス履歴を表示する

このセクションのシナリオでは、AWS CLI を使用して IP アドレス使用率を分析し監査する方法を説明します。AWS CLI の使用に関する一般的な情報については、AWS コマンドラインインターフェイスユーザーガイドにある「AWS CLI の使用」を参照してください。

内容

概要:

IPAM は、IP アドレス監視データを最大 3 年間自動的に保持します。履歴データを使用して、ネットワークセキュリティおよびルーティングポリシーを分析および監査できます。以下のタイプのリソースについて、履歴インサイトを検索できます。

- VPC
- VPC サブネット
- Elastic IP アドレス
- 実行中の EC2 インスタンス
- インスタンスにアタッチされた EC2 ネットワークインターフェイス

> **Important**
>
> IPAM はインスタンスにアタッチされた Amazon EC2 インスタンスおよび EC2 ネットワークインターフェイスを監視しませんが、IP 履歴検索機能を使用して EC2 インスタンスおよびネットワークインターフェイス CIDR 上の履歴データを検索できます。

> **Note**
>
> - このチュートリアルにあるコマンドは、IPAM を所有するアカウントと IPAM をホストする AWS リージョンを使用して実行する必要があります。
> - CIDR に対する変更のレコードは、定期的なスナップショットで取得されます。これは、レコードが表示または更新されるまでに時間がかかることを指し、SampledStartTime および SampledEndTime の値が、実際の発生時刻と異なる場合があります。

シナリオ

このセクションのシナリオでは、AWS CLI を使用して IP アドレス使用率を分析し監査する方法を説明します。サンプリングされた終了時間や開始時間など、このチュートリアルで説明する値の詳細については、IP アドレス履歴の表示 を参照してください。

シナリオ 1: 2021 年 12 月 27 日 (UTC) の午前 1 時から午後 9 時の間に、**10.2.1.155/32** に関連付けられたリソースはどれか？

1. 次のコマンドを実行します。

```
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. 分析の結果を表示します。以下の例では、CIDR はネットワークインターフェイスと EC2 インスタンスに一定期間にわたって割り当てられています。SampledEndTime 値がないことは、レコードがアクティブ状態のままであることを意味します。次の出力に表示される値の詳細については、IP アドレス履歴の表示を参照してください。

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

ネットワークインターフェイスがアタッチされているインスタンスの所有者 ID が、ネットワークインターフェイスの所有者 ID と異なる場合 (NAT ゲートウェイ、VPC 内の Lambda ネットワークインターフェイス、およびその他の AWS サービス場合と同様に)、ResourceOwnerId はネットワークインターフェイスの所有者のアカウント ID ではなく amazon-aws になります。次の例は、NAT ゲートウェイに関連付けられている CIDR のレコードを示しています。

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

シナリオ 2: 2021 年 12 月 1 日 ~ 2021 年 12 月 27 日 (UTC) の間に、**10.2.1.0/24** に関連付けられるリソースはどれか？

1. 次のコマンドを実行します。

```
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. 分析の結果を表示します。以下の例では、CIDR はサブネットと VPC に一定期間にわたって割り当てられています。SampledEndTime 値がないことは、レコードがアクティブ状態のままであることを意味します。次の出力に表示される値の詳細については、IP アドレス履歴の表示を参照してください。

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

シナリオ 3: 2021 年 12 月 1 日 ~ 2021 年 12 月 27 日 (UTC) の間に、**2605:9cc0:409::/56** に関連付けられるリソースはどれか？

1. 次のコマンドを実行します。--region は IPAM ホームリージョンとなります:

```
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. 分析の結果を表示します。次の例では、CIDR は、IPAM ホームリージョン外のリージョンで、一定の期間にわたって 2 つの異なる VPC に割り当てられています。SampledEndTime 値がないことは、レコードがアクティブ状態のままであることを意味します。次の出力に表示される値の詳細については、IP アドレス履歴の表示を参照してください。

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

シナリオ 4: 過去 24 時間に、**10.0.0.0/24** に関連付けられたリソースはどれか (現時刻は 2021 年 12 月 27 日 (UTC) の午前 0 時であると仮定)?

1. 次のコマンドを実行します。

```
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. 分析の結果を表示します。以下の例では、CIDR が多くのサブネットと VPC に一定期間にわたって割り当てられています。SampledEndTime 値がないことは、レコードがアクティブ状態のままであることを意味します。次の出力に表示される値の詳細については、IP アドレス履歴の表示を参照してください。

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


シナリオ 5: 現在 **10.2.1.155/32** に関連付けられているリソースはどれか?

1. 次のコマンドを実行します。

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

2. 分析の結果を表示します。以下の例では、CIDR がネットワークインターフェイスと EC2 インスタンスに一定期間にわたって割り当てられています。SampledEndTime 値がないことは、レコードがアクティブ状態のままであることを意味します。次の出力に表示される値の詳細については、IP アドレス履歴の表示を参照してください。

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

シナリオ 6: 現在 **10.2.1.0/24** に関連付けられているリソースはどれか?

1. 次のコマンドを実行します。

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

2. 分析の結果を表示します。以下の例では、CIDR が VPC とサブネットに一定期間にわたって割り当てられています。この /24 CIDR に完全に一致する結果のみが返されます。/24 CIDR のすべての /32 ではありません。SampledEndTime 値がないことは、レコードがアクティブ状態のままであることを意味します。次の出力に表示される値の詳細については、IP アドレス履歴の表示を参照してください。

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

シナリオ 7: 現在 **54.0.0.9/32** に関連付けられているリソースはどれか?

この例では、54.0.0.9/32 が IPAM と統合されている AWS Organizations の一部ではない Elastic IP アドレスに割り当てられています。

1. 次のコマンドを実行します。

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

2. この例では、54.0.0.9/32 が IPAM と統合されている AWS Organizations の一部ではない Elastic IP アドレスに割り当てられているため、レコードは返されません。

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

チュートリアル: ASN を IPAM に取り込む

パートナーやお客様がネットワークで許可リストに登録している信頼できる IP アドレスと AS 番号 (ASN) を AWS のアプリケーションで使用している場合、パートナーやお客様が許可リストを変更しなくてもこれらのアプリケーションを実行できます。

AS 番号 (ASN) は、インターネット上でネットワークのグループを識別し、ボーダーゲートウェイプロトコルを使用して他のネットワークと動的にルーティングデータを交換できるようにする、世界的に一意な番号です。例えば、インターネットサービスプロバイダー (ISP) は ASN を使用してネットワークトラフィックソースを識別します。すべての組織が独自の ASN を購入するわけではありませんが、購入する組織は ASN を AWS に持ち込むことができます。

独自の自律システム番号の持ち込み (BYOASN) を利用すると、AWS に持ち込んだ IPv4 または IPv6 アドレスを AWS ASN ではなく独自のパブリック ASN でアドバタイズできます。BYOASN を使用すると、IP アドレスから発信されるトラフィックには AWS ASN ではなく ASN が伝送され、IP アドレスと ASN に基づいてリストされたトラフィックを許可しているお客様やパートナーがワークロードにアクセスできるようになります。

Important

- IPAM のホームリージョンの IPAM アカウントを使用して、このチュートリアルを完了します。
- このチュートリアルでは、IPAM に持ち込みたいパブリック ASN を所有していて、すでに AWS に BYOIP CIDR をパブリックスコープのプールに持ち込み、プロビジョニングしていることを前提としています。ASN は IPAM にいつでも持ち込むことができますが、使用するには AWS アカウントに持ち込んだ CIDR に関連付ける必要があります。このチュートリアルでは、これを実行済みであることを前提としています。詳細については、「チュートリアル: IP アドレスを IPAM に移行する」を参照してください。
- 独自の ASN と AWS ASN の広告を遅滞なく切り替えることができますが、AWS ASN から独自の ASN への変更は 1 時間に 1 回に制限されます。
- BYOIP CIDR が現在広告されている場合は、ASN に関連付けるために広告から撤回する必要はありません。

ASN のオンボーディングの前提条件

このチュートリアルを完了するに必要なものは以下のとおりです。

- 2 バイトまたは 4 バイトのパブリック ASN。
- AWS の チュートリアル: IP アドレスを IPAM に移行する で IP アドレス範囲を既に持ち込んでいる場合は、IP アドレス CIDR 範囲が必要となります。さらに、プライベートキーも必要です。IP アドレス CIDR 範囲を AWS に持ち込んだときに作成したプライベートキーを使用するか、Amazon EC2 ユーザーガイドの「Create a private key and generate an X.509 certificate」で説明されているように新しいプライベートキーを作成できます。
- チュートリアル: IP アドレスを IPAM に移行する で AWS に IPv4 または IPv6 アドレス範囲を持ち込む際に、X.509 証明書を作成し、その X.509 証明書を RIR の RDAP レコードにアップロードします。ASN には、 RIR の RDAP レコードに作成したものと同じ証明書をアップロードする必要があります。エンコードされた部分の前後の `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` 文字列を、必ず含めます。このコンテンツはすべて、長い 1 行にする必要があります。RDAP を更新する手順はご使用の RIR によって異なります。
  - ARIN の場合は、Account Manager ポータルで [ASN の変更] オプションを使用して、ASN を表す「ネットワーク情報」オブジェクトの [パブリックコメント] オプションに証明書を追加します。組織の [comments] セクションには追加しないでください。
  - RIPE の場合は、ASN を表す aut-num オブジェクトに、新しい [descr] フィールドとして証明書を追加します。これらは通常、

    RIPE データベースポータルの [マイリソース] セクションにあります。組織の [コメント] セクションや、aut-num オブジェクトの [備考] フィールドには追加しないでください。
  - APNIC の場合は、証明書をメールで helpdesk@apnic.net に送信し、ASN の [備考] フィールドに手動で追加します。ASN の APNIC 正規連絡先を使用してメールを送信します。
- IPAM に IP アドレス範囲を持ち込む場合は、ROA を作成して、IPAM に持ち込む IP アドレス空間を制御していることを検証します。その ROA に加えて、IPAM に持ち込む ASN を持つ RIR に 2 つ目の ROA が必要です。RIR の ASN のためにこの 2 つ目の ROA がない場合は、「3. RIR に ROA オブジェクトを作成する」を完了します。他のステップは無視します。

チュートリアルのステップ

AWS コンソールまたは AWS CLI を使用して、以下の手順を実行します。

AWS Management Console

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. 左側のナビゲーションペインで、[IPAM] を選択します。
3. IPAM を選択します。

4. [BYOASN] タブを選択し、[BYOASN のプロビジョニング] を選択します。
5. ASN を入力します。その結果、[メッセージ] フィールドには、次のステップでサインインする必要があるメッセージが自動的に入力されます。

   - メッセージの形式は次のとおりです。ACCOUNT は AWS アカウント番号、ASN は IPAM に持ち込む ASN、YYYMMDD はメッセージの有効期限 (デフォルトでは翌月の最終日) です。例:

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

6. メッセージをコピーし、必要に応じて有効期限を独自の値に置き換えます。
7. プライベートキーを使用してメッセージに署名します。例:

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

8. [署名] に、署名を入力します。
9. (オプション) 別の ASN をプロビジョニングするには、[別の ASN をプロビジョニング] を選択します。最大 5 つの ASN をプロビジョニングできます。このクォータを引き上げるには、IPAM のクォータ を参照してください。
10. [プロビジョニング] を選択します。
11. [BYOASN] タブにプロビジョニングプロセスを表示します。状態が 「プロビジョニング待ち」から「プロビジョニング済み」に変わるのを待ちます。プロビジョニングに失敗した状態の BYOASN は 7 日後に自動的に削除されます。ASN が正常にプロビジョニングされたら、それを BYOIP CIDR に関連付けることができます。
12. 左のナビゲーションペインで、[プール] を選択します。
13. 公開範囲を選択します。スコープの詳細については、IPAM の仕組みを参照してください。
14. BYOIP CIDR がプロビジョニングされているリージョナルプールを選択します。プールにはサービス が EC2 に設定され、ロケールが選択されている必要があります。
15. [CIDR] タブを選択し、BYOIP CIDR を選択します。
16. [アクション] で [BYOSAN 関連付けの管理] を選択します。
17. [関連する BYOSAN] で、AWS に取り込む ASN を選択します。ASN が複数ある場合は、複数の ASN を BYOIP CIDR に関連付けることができます。IPAM には、いくつでも ASN を関連付けることができます。デフォルトでは、最大 5 つの ASN を IPAM に追加できることに注意してください。詳細については、「IPAM のクォータ」を参照してください。

18. [関連付ける] を選択してください。
19. ASN の関連付けが完了するのを待機します。ASN が BYOIP CIDR に正常に関連付けられたら、BYOIP CIDR を再度広告できます。
20. [CIDR] タブを選択します。
21. BYOIP CIDR を選び、[Actions] (アクション) > [Advertise] (アドバタイズ) を選択します。その結果、Amazon ASN と IPAM に持ち込んだすべての ASN の ASN オプションが表示されます。
22. IPAM に持ち込んだ ASN を選択し、[CIDR を広告する] を選択します。その結果、BYOIP CIDR が広告され、[広告] 列の値が 「取り消し」から「広告済み」に変わります。「AS 番号」列には、CIDR に関連付けられた ASN が表示されます。
23. (オプション) ASN 関連付けを Amazon ASN に戻す場合は、BYOIP CIDR を選択し、[アクション] で [アドバタイズ] をもう一度選択します。今回は Amazon ASN を選択します。Amazon ASN にはいつでもスワップバックできますが、カスタム ASN に変更できるのは 1 時間に 1 回だけです。

チュートリアルは完了です。

クリーンアップ

1. ASN と BYOIP CIDR との関連付けを解除します。
   - BYOIP CIDR を広告から除外するには、[公開範囲] のプールで [BYOIP CIDR] を選択し、[アクション]、[広告から除外] の順に選択します。
   - ASN と CIDR の関連付けを解除するには、[アクション]、[BYOSAN 関連付けの管理] の順に選択します。
2. ASN のプロビジョニング解除
   - ASN をプロビジョニング解除するには、[ByOSNS] タブで [ASN] を選択し、[ASN のプロビジョニング解除] を選択します。その結果、ASN はプロビジョニング解除されます。プロビジョニング解除状態の BYOASN は 7 日後に自動的に削除されます。

これで、クリーンアップは完了です。

Command line

1. ASN と認可メッセージを含めて ASN をプロビジョニングします。署名とは、プライベートキーで署名されたメッセージです。

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

2. プロビジョニングプロセスを追跡できるように ASN を記述します。リクエストが成功すると、数分後に プロビジョニング状態が「プロビジョニング済み」に設定されているはずです。

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

3. ASN を BYOIP CIDR に関連付けます。広告元となるカスタム ASN は、まず CIDR に関連付ける必要があります。

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

4. 関連付けプロセスを追跡できるように CIDR を記述します。

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

5. CIDR を ASN とともにこうこくします。CIDR がすでに広告されている場合は、オリジン ASN が Amazon のオリジン ASN からお客様の ASN に切り替わります。

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

6. CIDR を記述して、ASN の状態が「関連付け済み」から「広告済み」に変化することを確認します。

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

チュートリアルは完了です。

クリーンアップ

1. 次のいずれかを行います。

   - ASN の広告だけを取り消して、CIDR を広告したまま Amazon ASN の使用に戻すには、ASN パラメータに特別な AWS 値を指定して advertise-byoip-cidr を呼び出す必要があります。Amazon ASN への切り替えはいつでも可能ですが、カスタム ASN に変更できるのは 1 時間に 1 回だけです。

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

- CIDR と ASN の広告を同時に取り消すには、withdraw-byoip-cidr を呼び出します。

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

2. ASN をクリーンアップするには、まず ASN と BYOIP CIDR との関連付けを解除する必要があります。

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

3. ASN と ASN を関連付けていたすべての BYOIP CIDR との関連付けが解除されたら、プロビジョニングを解除できます。

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

4. すべての ASN 関連付けが削除されたら、BYOIP CIDR のプロビジョニングを解除することもできます。

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

5. プロビジョニング解除を確認します。

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

これで、クリーンアップは完了です。

チュートリアル: IP アドレスを IPAM に移行する

このセクションのチュートリアルでは、パブリック IP アドレス空間を AWS に取り込み、IPAM でその空間を管理するプロセスを説明します。

IPAM でパブリック IP アドレス空間を管理することには、次の利点があります。

- 組織全体でのパブリック IP アドレスの利用率を向上: IPAM を使用して、AWS アカウント間で IP アドレス空間を共有することができます。IPAM を使用しないと、パブリック IP スペースを AWS Organizations アカウントで共有することはできません。

- パブリック IP スペースを AWS に取り込むプロセスを簡素化: IPAM を使ってパブリック IP アドレス空間を一度オンボーディングし、その後 IPAM を使ってリージョン間でパブリック IP を EC2 インスタンスやApplication Load Balancer などのリソースに配布できます。IPAM がないと、AWS リージョンごとにパブリック IP をオンボーディングする必要があります。

内容

ドメインコントロールの検証

IP アドレス範囲を AWS に持ち込む前に、このセクションで説明したオプションのいずれかを使用して、IP アドレススペースがユーザーによって制御されていることを確認する必要があります。後に、IP アドレス範囲を AWS に持ち込むと、AWS で IP アドレス範囲がユーザーによって制御されていることが検証されます。この検証により、お客様は他のユーザーに属する IP 範囲を使用できなくなり、ルーティングやセキュリティの問題を防ぐことができます。

範囲がユーザーによって制御されていることを確認するのに使用できる方法は 2 つあります。

- X.509 証明書: IP アドレス範囲が RDAP をサポートするインターネットレジストリ (ARIN、RIPE、APNIC など) に登録されている場合、X.509 証明書を使用してドメインの所有権を検証できます。
- DNS TXT レコード: インターネットレジストリが RDAP をサポートしているかどうかにかかわらず、検証トークンと DNS TXT レコードを使用してドメインの所有権を検証できます。

内容

X.509 証明書を使用してドメインを検証する

このセクションでは、IP アドレス範囲を IPAM に持ち込む前に、X.509 証明書を使用してドメインを検証する方法について説明します。

X.509 証明書を使用してドメインを検証するには

1. 「Amazon EC2 ユーザーガイド」の「Prerequisites for BYOIP in Amazon EC2」の 3 つのステップを完了します。

   > **Note**
   >
   > ROA を作成する際、IPv4 の CIDR では、IP アドレスのプレフィックスの最大長を /24 に設定する必要があります。IPv6 CIDR については、アドバタイズ可能なプールに追加する場合、IP アドレスのプレフィックスの最大長は /48 である必要があります。これにより、パブリック IP アドレスを AWS リージョンごとに分割して利用する柔軟性がもたらされます。IPAM では、設定した最大長が適用されます。最大長は、このルートで許可する最小のプレフィックス長アナウンスです。例えば、/20 の CIDR ブロックを AWS に取り込んだ場合、最大長を /24 に設定することで、大きなブロックを任意に分割 (/21、/22、/24 など) して、それらの小さな CIDR ブロックを任意のリージョンに配布することができます。最大長を /23 に設定した場合、大きなブロックから /24 を分割して広告することはできません。なお、/24 は最小の IPv4 ブロック、/48 はリージョンからインターネットにアドバタイズできる最小の IPv6 ブロックです。

2. 「Amazon EC2 ユーザーガイド」の「AWS でパブリックにアドバタイズ可能なアドレス範囲をプロビジョニングする」のステップ 1 と 2 のみを完了し、アドレス範囲のプロビジョニング (ステップ 3) はまだしないでください。`text_message` と `signed_message` を保存します。これらは後にこのプロセスで必要になります。

これらのステップが完了したら、「AWS マネジメントコンソールと AWS CLI の両方を使用して、独自の IP を IPAM に持ち込む」または「AWS CLI のみを使用した IPAM への独自の IP CIDR の持ち込み」に進みます。

DNS TXT レコードを使用してドメインを検証する

IP アドレス範囲を IPAM に持ち込む前に、このセクションのステップを完了して、DNS TXT レコードによりドメインを検証します。

DNS TXT レコードを使用して、パブリック IP アドレス範囲がユーザーによって制御されていることを検証できます。DNS TXT レコードは、ドメイン名に関する情報が入った DNS レコードの一種です。この機能を使用すると、RDAP (Registration Data Access Protocol) レコードベースの検証をサポートするインターネットレジストリ (ARIN、RIPE、APNIC など) だけでなく、任意のインター

ネットレジストリ (JPNIC、LACNIC、AFRINIC など) に登録された IP アドレスを使用できるようになります。

> **Important**
>
> 続行するには、無料利用枠またはアドバンスト枠で IPAM を作成しておく必要があります。IPAM がない場合は、まず IPAM を作成する を完了してください。

内容

ステップ 1: ROA がない場合は ROA を作成する

アドバタイズする IP アドレス範囲のために、地域インターネットレジストリ (RIR) に Route Origin Authorization (ROA) が必要です。RIR に ROA がない場合は、「Amazon EC2 ユーザーガイド」の「3. 「Amazon EC2 ユーザーガイド」の「RIR に ROA オブジェクトを作成する」を完了してください。他のステップは無視します。

取得できる最も具体的な IPv4 アドレス範囲は /24 です。提供できる最も具体的な IPv6 アドレス範囲はパブリックにアドバタイズ可能な CIDR の場合は /48、パブリックにアドバタイズ可能でない CIDR の場合は /60 です。

ステップ 2. 検証トークンを作成する

検証トークンは、外部リソースの制御を証明するのに使用できる AWS 生成のランダム値です。例えば、検証トークンを使用して、IP アドレス範囲を AWS に持ち込む (BYOIP) ときに、パブリック IP アドレス範囲がユーザーによって制御されていることを検証できます。

このセクションのステップを完了して検証トークンを作成します。検証トークンは、このチュートリアルの以降のステップで IP アドレス範囲を IPAM に持ち込むのに必要になります。AWS コンソールまたは AWS CLI について、以下の手順に従ってください。

AWS Management Console

検証トークンを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. AWS マネジメントコンソールで、IPAM を作成した AWS リージョンを選択します。
3. 左側のナビゲーションペインで、[IPAM] を選択します。
4. IPAM を選択し、[検証トークン] タブを選択します。
5. [検証トークンを作成] を選択します。
6. トークンを作成した後は、このブラウザタブを開いたままにします。次のステップで [トークン値]、[トークン名]、その後のステップで [トークン ID] が必要になります。

次の点に注意してください。

- 検証トークンを作成すると、72 時間以内に IPAM からプロビジョニングした複数の BYOIP CIDR に対してそのトークンを再利用できます。72 時間経過後にさらに CIDR をプロビジョニングする場合は、新しいトークンが必要です。
- 最大 100 個のトークンを作成できます。この制限に達した場合は、期限切れのトークンを削除してください。

Command line

- IPAM が create-ipam-external-resource-verification-token で DNS 設定に使用する検証トークンを作成するリクエスト:

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

これにより、IpamExternalResourceVerificationTokenId、TokenName と TokenValue を含むトークン、およびトークンの有効期限 (NotAfter) が返されます。

```
{
    "IpamExternalResourceVerificationToken": {
        "IpamExternalResourceVerificationTokenId": "ipam-ext-res-ver-
token-0309ce7f67a768cf0",
        "IpamId": "ipam-0f9e8725ac3ae5754",
        "TokenValue": "a34597c3-5317-4238-9ce7-50da5b6e6dc8",
        "TokenName": "86950620",
```

```
        "NotAfter": "2024-05-19T14:28:15.927000+00:00",
        "Status": "valid",
        "Tags": [],
        "State": "create-in-progress" }
}
```

次の点に注意してください。

- 検証トークンを作成すると、72 時間以内に IPAM からプロビジョニングした複数の BYOIP CIDR に対してそのトークンを再利用できます。72 時間経過後にさらに CIDR をプロビジョニングする場合は、新しいトークンが必要です。
- describe-ipam-external-resource-verification-tokens を使用してトークンを表示できます。
- 最大 100 個のトークンを作成できます。この制限に達した場合は、delete-ipam-external-resource-verification-token を使用して期限切れのトークンを削除できます。

ステップ 3. DNS ゾーンと TXT レコードを設定する

このセクションのステップを完了して、DNS ゾーンと TXT レコードを設定します。Route53 を DNS として使用していない場合は、DNS プロバイダーが提供するドキュメントに従って DNS ゾーンを設定し、TXT レコードを追加します。

Route53 を使用している場合は、次に注意してください。

- AWS コンソールでリバースルックアップゾーンを作成するには、「Amazon Route 53 デベロッパーガイド」の「パブリックホストゾーンの作成」を参照するか、AWS CLI コマンド create-hosted-zone を使用してください。
- AWS コンソールでリバースルックアップゾーンにレコードを作成するには、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 コンソールを使用したレコードの作成」を参照するか、AWS CLI コマンド change-resource-record-sets を使用してください。
- ホストゾーンの作成が完了したら、RIR から Route53 が提供するネームサーバー (LACNIC や APNIC などのもの) にホストゾーンを委任します。

別の DNS プロバイダーと Route53 のどちらを使用している場合でも、TXT レコードを設定する際には、次の点に注意してください。

- レコード名はトークン名である必要があります。
- レコードタイプは TXT である必要があります。

- ResourceRecord 値はトークン値である必要があります。

例:

- 名前: 86950620.113.0.203.in-addr.arpa
- タイプ: TXT
- ResourceRecords 値: a34597c3-5317-4238-9ce7-50da5b6e6dc8

コードの説明は以下のとおりです。

- 86950620 は検証トークン名です。
- 113.0.203.in-addr.arpa はリバースルックアップゾーン名です。
- TXT はレコードタイプです。
- a34597c3-5317-4238-9ce7-50da5b6e6dc8 は検証トークン値です。

> **Note**
>
> BYOIP を使用して IPAM に持ち込むプレフィックスのサイズに応じて、DNS に 1 つ以上の認証レコードを作成する必要があります。この認証レコードはレコードタイプ TXT であり、プレフィックス自体またはその親プレフィックスのリバースゾーンに配置する必要があります。
>
> - IPv4 では、認証レコードは、プレフィックスを構成するオクテット境界の範囲にアライメントする必要があります。
>   - 例
>   - オクテット境界で既にアライメントされている 198.18.123.0/24 の場合、次のように認証レコードを 1 つ作成する必要があります。
>   - *token-name*.123.18.198.in-addr.arpa. IN TXT “*token-value*”
>   - それ自体がオクテット境界にアライメントされていない 198.18.12.0/22 の場合、認証レコードを 4 つ作成する必要があります。これらのレコードは、オクテット境界でアライメントされているサブネット 198.18.12.0/24、198.18.13.0/24、198.18.14.0/24、および 198.18.15.0/24 をカバーする必要があります。対応する DNS エントリは次のようにする必要があります。
>   - *token-name*.12.18.198.in-addr.arpa. IN TXT “*token-value*”

        - *token-name*.13.18.198.in-addr.arpa. IN TXT "*token-value*"
        - *token-name*.14.18.198.in-addr.arpa. IN TXT "*token-value*"
        - *token-name*.15.18.198.in-addr.arpa. IN TXT "*token-value*"
    - オクテット境界で既にアライメントされている 198.18.0.0/16 の場合、認証レコードを 1 つ作成する必要があります。
        - *token-name*.18.198.in-addr.arpa. IN TXT "*token-value*"
- IPv6 では、認証レコードは、プレフィックスを構成するニブル境界の範囲にアライメントする必要があります。有効なニブル値は、32、36、40、44、48、52、56、60 などです。
    - 例
        - ニブル境界で既にアライメントされている 2001:0db8::/40 の場合、認証レコードを 1 つ作成する必要があります。
            - *token-name*.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
        - それ自体がニブル境界でアライメントされていない 2001:0db8:80::/42 の場合、認証レコードを 4 つ作成する必要があります。これらのレコードは、ニブル境界でアライメントされているサブネット 2001:db8:80::/44、2001:db8:90::/44、2001:db8:a0::/44、および 2001:db8:b0::/44 をカバーする必要があります。対応する DNS エントリは次のようにする必要があります。
            - *token-name*.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
            - *token-name*.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
            - *token-name*.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
            - *token-name*.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
        - それ自体がニブル境界でアライメントされていない、アドバタイズされていない範囲 2001:db8:0:1000::/54 の場合、認証レコードを 4 つ作成する必要があります。これらのレコードは、ニブル境界でアライメントされているサブネット 2001:db8:0:1000::/56、2001:db8:0:1100::/56、2001:db8:0:1200::/56、および 2001:db8:0:1300:::/56 をカバーする必要があります。対応する DNS エントリは次のようにする必要があります。
            - *token-name*.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
            - *token-name*.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"

- *token-name*.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”
- *token-name*.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”

- token-name と文字列「ip6.arpa」の間の正しい 16 進数の数値を確認するには、その数値に 4 を掛けます。この結果はプレフィックスの長さと一致する必要があります。例えば、プレフィックス /56 の場合、16 進数での桁数を 14 にする必要があります。

これらのステップが完了したら、「AWS マネジメントコンソールと AWS CLI の両方を使用して、独自の IP を IPAM に持ち込む」または「AWS CLI のみを使用した IPAM への独自の IP CIDR の持ち込み」に進みます。

AWS マネジメントコンソールと AWS CLI の両方を使用して、独自の IP を IPAM に持ち込む

IPAM に自分の IP を導入 (BYOIP) すると、AWS で組織の既存の IPv4 および IPv6 アドレス範囲を使用できます。これにより、独自の IP アドレス空間でオンプレミス環境とクラウド環境を統一することで、一貫したブランドを維持し、ネットワークパフォーマンスを改善するとともに、セキュリティを強化して、管理を簡素化できます。

AWS マネジメントコンソールと AWS CLI の両方を使用して、IPv4 または IPv6 CIDR を IPAM に取り込むには、次のステップを実行してください。

> **Note**
>
> 開始する前に、まずドメインコントロールを検証する必要があります。

IPv4 アドレス範囲を AWS に設定すると、最初のアドレス (ネットワークアドレス) と最後のアドレス (ブロードキャストアドレス) を含む、その範囲内のすべての IP アドレスを使用できます。

内容

- AWS マネジメントコンソールと AWS CLI の両方を使用して、独自の IPv4 CIDR を IPAM に取り込む
- AWS マネジメントコンソールを使用して、独自のパブリック IPv6 CIDR を IPAM に取り込む

AWS マネジメントコンソールと AWS CLI の両方を使用して、独自の IPv4 CIDR を IPAM に取り込む

AWS マネジメントコンソールと AWS CLI の両方を使用して、IPAM に IPv4 CIDR を取り込み、Elastic IP アドレス (EIP) を CIDR に割り当てる手順は次のとおりです。

Important

- このチュートリアルでは、次のセクションのステップがすでに完了していることを前提としています。
  - IPAM を AWS Organizations 内のアカウントと統合する.
  - IPAM を作成する.
- このチュートリアルの各ステップを、3 つの AWS Organizations アカウントのいずれかで実行する必要があります。
  - 管理アカウント。
  - IPAM を AWS Organizations 内のアカウントと統合する で IPAM 管理者として設定されるメンバーアカウント。このチュートリアルでは、このアカウントを IPAM アカウントと呼びます。
  - IPAM プールから CIDR を割り当てる組織内のメンバーアカウント。このチュートリアルでは、このアカウントをメンバーアカウントと呼びます。

内容

ステップ 1: AWS CLI の名前付きプロファイルと IAM ロールを作成する

このチュートリアルをシングル AWS ユーザーとして完了するには、AWS CLI の名前付きプロファイルを使用して、1 つの IAM ロールから別のアカウントへと切り替えることができます。名前付きプロファイルは、AWS CLI を使用して `--profile` オプションを使用するときに参照する設定と認証情報の集まりです。AWS アカウントの IAM ロールと指定したプロファイルを作成する方法の詳細については、の「AWS CLI での IAM ロールの使用」を参照してください。

このチュートリアルで使用する 3 つの AWS アカウントごとに、1 つのロールと 1 つの名前付きプロファイルを作成します。

- AWS Organizations 管理アカウント向けの `management-account` と呼ばれるプロファイル。
- IPAM 管理者として設定された AWS Organizations メンバーアカウント向けの、`ipam-account` と呼ばれるプロファイル。
- IPAM プールから CIDR を割り当てる自分の組織の AWS Organizations メンバーアカウント向けの、`member-account` と呼ばれるプロファイル。

IAM ロールと名前付きプロファイルを作成した後、このページに戻り次のステップに進みます。なお、このチュートリアルの残りの部分では、サンプルの AWS CLI コマンドで `--profile` オプションを名前付きプロファイルのうちの 1 つとともに使用することにより、どのアカウントでコマンドを実行する必要があるのかを示しています。

ステップ 2: 最上位の IPAM プールを作成する

このセクションのステップに従って、最上位の IPAM プールを作成します。

このステップは、IPAM アカウントで実行する必要があります。

プールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。パブリックスコープを選択します。スコープの詳細については、「IPAM の仕組み」を参照してください。
4. [プールを作成] を選択します。
5. (オプション) プールの [名前タグ] とプールの [説明] を追加します。
6. [ソース] で [IPAM 範囲] を選択します。

7. [アドレスファミリー] には [IPv4] を選択します。
8. [リソース計画] で、[範囲内のIP 空間計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
9. [ロケール] には [なし] を選択します。

   IPAM を BYOIP と統合するには、BYOIP CIDR に使用されるプールにロケールを設定する必要があります。内部に 1 つのリージョンプールが含まれる最上位の IPAM プールを作成し、リージョンプールから Elastic IP アドレスにスペースを割り当てるため、最上位プールではなくリージョンプールにロケールを設定します。後のステップでリージョンプールを作成するときに、リージョンプールにロケールを追加します。

   > **Note**
   >
   > 内部にリージョンプールを含むトップレベルプールを作成するのではなく、プールを 1 つだけ作成する場合は、このプールにロケールを選択して、プールを割り当てることができるようにします。

10. [パブリック IP ソース] で、[BYOIP] を選択します。
11. [プロビジョニングする CIDR] で次のいずれかを実行します。

    - X.509 証明書でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR と BYOIP メッセージおよびそのステップで作成した証明書署名を含める必要があります。
    - DNS TXT レコード でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR およびそのステップで作成した IPAM 検証トークンを含める必要があります。

    IPv4 CIDR を最上位のプール内のプールにプロビジョニングするとき、プロビジョンできる最小の IPv4 CIDR は /24 です。より具体的な CIDR (/25 など) は許可されません。

    > **Important**
    >
    > ほとんどのプロビジョニングは 2 時間以内に完了しますが、パブリックにアドバタイズ可能な範囲のプロビジョニングプロセスが完了するまでに最大 1 週間かかる場合があります。

12. [このプールの割り当てルールを設定する] は選択しません。
13. (オプション) プールのタグを選択します。
14. [プールを作成] を選択します。

続行する前に、この CIDR のプロビジョンが完了したことを確認してください。プロビジョニングの状態は、プールの詳細ページの CIDR タブで確認できます。

ステップ 3. 最上位プール内にリージョンプールを作成する

最上位プール内にリージョンプールを作成する IPAM を BYOIP と統合するには、BYOIP CIDR に使用されるプールにロケールを設定する必要があります。このセクションでリージョンプールを作成するときに、リージョンプールにロケールを追加します。`Locale` は、IPAM の作成時に設定した運用リージョンのいずれかに属している必要があります。例えば、us-east-1 のロケールは、us-east-1 が IPAM の運用リージョンである必要があることを意味します。us-east-1-scl-1 (ローカルゾーンに使用されるネットワーク境界グループ) のロケールは、IPAM に us-east-1 の運用リージョンが必要であることを意味します。

このステップは、IPAM アカウントで実行する必要があります。

トップレベルプール内にリージョンプールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。デフォルトのプライベートスコープを使用しない場合は、コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、「IPAM の仕組み」を参照してください。
4. [プールを作成] を選択します。
5. (オプション) プールの [名前タグ] とプールの [説明] を追加します。
6. [ソース] で、前のセクションで作成した最上位レベルのプールを選択します。
7. [リソース計画] で、[範囲内のIP スペースの計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
8. [Locale] (ロケール) で、プールのロケールを選択します。このチュートリアルでは、`us-east-2` をリージョンプールのロケールとして使用します。使用可能なオプションは、IPAM を作成したときに選択した運用リージョンによって提供されます。

プールのロケールは、以下のいずれかにする必要があります。

- この IPAM プールを割り当て可能にする AWS リージョン。
- この IPAM プールを割り当て可能にする AWS Local Zone のネットワーク境界グループ (サポートされるローカルゾーン)。このオプションを利用できるのは、パブリックスコープ内の IPAM IPv4 プールのみです。
- AWS Dedicated Local Zone。AWS Dedicated Local Zone 内にプールを作成するには、セレクタ入力に AWS Dedicated Local Zone を入力します。
- `Global` CloudFront ロケーションなど、すべての AWS リージョンで IP アドレスをグローバルに使用する場合。`Global` ロケールはパブリック IPv4 プールでのみ使用できます。

例えば、VPC の CIDR は、VPC のリージョンとロケールを共有する IPAM プールからしか割り当てることができません。プールのロケールを選択したら、変更はできないことに注意してください。停止が原因で IPAM のホームリージョンが使用できなくなり、プールのロケールが IPAM のホームリージョンと異なる場合でも、プールを使用して IP アドレスを割り当てることができます。

ロケールを選択すると、プールとそのプールから割り当てられるリソースの間にクロスリージョン依存関係がないことが保証されます。

9. [Service] (サービス) で、[EC2 (EIP/VPC)] を選択します。選択したサービスによって、CIDR がアドバタイズ可能になる AWS サービスが決定します。現在、唯一の選択肢は EC2 (EIP/VPC) であり、このプールから割り当てられた CIDR は、Amazon EC2 サービス (Elastic IP アドレスの場合) と Amazon VPC サービス (VPC に関連付けられている CIDR の場合) に対してアドバタイズできるようになります。
10. [CIDRs to provision] (プロビジョニングする CIDR) で、プールにプロビジョニングする CIDR を選択します。

> **Note**
>
> CIDR を最上位プール内のリージョンプールにプロビジョニングする場合、プロビジョニングできる最も具体的な IPv4 CIDR は /24 です。より具体的な CIDR (/25 など) は許可されません。リージョンプールを作成すると、リージョンプール内に小さなプール (/25 など) を作成できます。リージョンプールまたはリージョンプール内のプールを共有する場合、これらのプールは同じリージョンプールで設定されたロケールでのみ使用できることに注意してください。

11. [このプールの割り当てルールを設定する] を有効にします。ここでは、トップレベルプールを作成したときと同じ割り当てルールオプションがあります。プールの作成時に使用できるオプションの説明については、トップレベル IPv4 プールを作成する を参照してください。リージョンプールの割り当てルールは、トップレベルプールから継承されません。ここでルールを適用しない場合、プールに割り当てルールは設定されません。
12. (オプション) プールのタグを選択します。
13. プールの設定が完了したら、[Create pool] (プールの作成) を選択します。

続行する前に、この CIDR のプロビジョンが完了したことを確認してください。プロビジョニングの状態は、プールの詳細ページの CIDR タブで確認できます。

ステップ 4: CIDR のアドバタイズ

このセクションのステップは、IPAM アカウントで実行する必要があります。Elastic IP アドレス (EIP) をインスタンスまたは Elastic Load Balancing に関連付けると、Service EC2 (EIP/VPC) が定義されているプール内にある、AWS に取り込んだ CIDR のアドバタイズを開始できます。このチュートリアルでは、これはリージョンプールです。デフォルトでは、CIDR はアドバタイズされません。つまり、インターネット経由でパブリックにアクセスできません。

このステップは、IPAM アカウントで実行する必要があります。

> **Note**
>
> アドバタイズメントステータスによって Elastic IP アドレスを割り当てる機能が制限されることはありません。BYOIPv4 CIDR がアドバタイズされていなくても、IPAM プールから EIP を作成できます。

CIDR をアドバタイズするには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。パブリックスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
4. このチュートリアルで作成したリージョンプールを選択します。
5. [CIDRs] (CIDR) タブを選択します。

6. BYOIP CIDR を選び、[Actions] (アクション) > [Advertise] (アドバタイズ) を選択します。
7. [Advertise CIDR] (CIDR のアドバタイズ) を選択します。

その結果、BYOIP CIDR がアドバタイズされ、[Advertising] (アドバタイズ) 列の値が [Withdrawn] (取り消し) から [Advertised] (アドバタイズ済み) に変わります。

ステップ 5. リージョンプールを共有する

このセクションのステップに従い、AWS Resource Access Manager (RAM) を使用して IPAM プールを共有します。

AWS RAM 内でリソース共有を有効にする

IPAM を作成したら、リージョンプールを組織内の他のアカウントと共有する必要があります。IPAM プールを共有する前に、このセクションのステップを完了し、AWS RAM とのリソース共有を有効にします。AWS CLI を使用してリソース共有を有効にする場合は、`--profile` **`management-account`** オプションを使用します。

リソース共有を有効にするには

1. AWS Organizations 管理アカウントを使って AWS RAM コンソール (https://console.aws.amazon.com/ram/) を開きます。
2. ナビゲーションペインで [設定] を選択し、[AWS Organizations との共有を有効にする] を選択し、[設定の保存] を選択します。

これで、IPAM プールを組織の他のメンバーと共有できるようになりました。

AWS RAM を使用して IPAM プールを共有する

このセクションでは、リージョンプールを他の AWS Organizations メンバーアカウントと共有します。必要な IAM アクセス許可に関する情報を含め、IPAM プールの共有に関する詳細な手順については、「AWS RAM を使用して IPAM プールを共有する」を参照してください。AWS CLI を使用してリソース共有を有効にする場合は、`--profile` **`ipam-account`** オプションを使用します。

AWS RAM を使用して IPAM プールを共有するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。

3. プライベートスコープを選択し、IPAM プールを選択して、[アクション] > [詳細を表示] の順に選択します。
4. [Resource sharing] (リソース共有) で [Create resource share] (リソース共有の作成) を選択します。AWS RAM コンソールが開きます。AWS RAM を使用してプールを共有します。
5. [リソースの共有の作成] を選択します。
6. AWS RAM コンソールで、[リソースの共有を作成] を再度選択します。
7. 共有リソースの [名前] を追加します。
8. [リソースタイプを選択] で [IPAM プール] を選択し、次に共有したいプールの ARN を選択します。
9. [次へ] を選択します。
10. AWSRAMPermissionIpamPoolByoipCidrImport 許可を選択します。アクセス許可オプションの詳細は本チュートリアルの対象外ですが、このオプションの詳細は「AWS RAM を使用して IPAM プールを共有する」にてご覧いただけます。
11. [次へ] を選択します。
12. [プリンシパル] > [プリンシパルタイプを選択] で、[AWS アカウント] を選択し、IPAM に IP アドレス範囲を取り込むアカウントのアカウント ID を入力して、[追加] を選択します。
13. [次へ] を選択します。
14. リソース共有オプションと共有先のプリンシパルを確認し、[作成] を選択します。
15. IPAM プールからの IP アドレス CIDR の割り当てを **member-account** アカウントに許可するには、`AWSRAMDefaultPermissionsIpamPool` を使用して 2 つ目のリソース共有を作成します。`--resource-arns` の値は、前のセクションで作成した IPAM プールの ARN です。`--principals` の値は、**member-account** のアカウント ID です。`--permission-arns` の値は、`AWSRAMDefaultPermissionsIpamPool` アクセス許可の ARN です。

ステップ 6: プールから Elastic IP アドレスを割り当てる

プールから Elastic IP アドレスを割り当てるには、このセクションのステップを実行します。パブリック IPv4 プールを使用して Elastic IP アドレスを割り当てる場合は、このセクションのステップではなく、ステップ 6 の代替方法 の代替ステップを使用できます。

> **Important**
>
> ec2:AllocateAddress を呼び出す許可がないことに関するエラーが表示される場合は、共有された IPAM プールに現在割り当てられているマネージド許可を更新する必要があります。リソース共有の作成者に連絡して、マネージド許可

AWSRAMPermissionIpamResourceDiscovery をデフォルトバージョンに更新するよう依頼してください。詳細については、AWS RAM ユーザーガイドの「リソース共有の更新」を参照してください。

AWS Management Console

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを割り当てる」のステップに従ってアドレスを割り当てます。ただし、次の点に注意してください。

- このステップは、メンバーアカウントで実行する必要があります。
- EC2 コンソールで使用している AWS リージョンが、リージョンレベルのプールの作成時に選択したロケールオプションと一致しているようにします。
- アドレスプールを選択する際には、[IPv4 IPAM プールを使用して割り当てる] オプションを選択し、作成したリージョンレベルのプールを選択します。

Command line

allocate-address コマンドを使用して、プールからアドレスを割り当てます。使用する --region は、ステップ 2 でプールを作成した際に選択した -locale オプションと一致する必要があります。--ipam-pool-id のステップ 2 で作成した IPAM プールの ID を含めます。オプションで、--address オプションを使用して IPAM プール内の特定の /32 を選択することもできます。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

レスポンスの例:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを割り当てる」を参照してください。

ステップ 7: Elastic IP アドレスと EC2 インスタンスの関連付け

Elastic IP アドレスを EC2 インスタンスに関連付けるには、このセクションのステップを実行します。

AWS Management Console

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを関連付ける」のステップに従って、IPAM プールから Elastic IP アドレスを割り当てます。ただし、次に注意してください: AWS マネジメントコンソールオプションを使用する場合、Elastic IP アドレスを関連付ける AWS リージョンは、リージョンレベルのプールの作成時に選択したロケールオプションと一致する必要があります。

このステップは、メンバーアカウントで実行する必要があります。

Command line

このステップは、メンバーアカウントで実行する必要があります。`--profile` **`member-account`** オプションを使用する

associate-address コマンドを使用して、Elastic IP アドレスをインスタンスに関連付けます。Elastic IP アドレスを関連付ける `--region` は、リージョンレベルのプールを作成した際に選択した `--locale` オプションと一致する必要があります。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

レスポンスの例:

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスをインスタンスまたはネットワークインターフェイスに関連付ける」を参照してください。

ステップ 8: クリーンアップ

このセクションのステップに従って、このチュートリアルでプロビジョンし、作成したリソースをクリーンアップします。

ステップ 1: CIDR のアドバタイズを取り消す

このステップは、IPAM アカウントで実行する必要があります。

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。パブリックスコープを選択します。
4. このチュートリアルで作成したリージョンプールを選択します。
5. [CIDRs] (CIDR) タブを選択します。
6. BYOIP CIDR を選び、[Actions] (アクション) > [Withdraw from advertising] (アドバタイズの取り消し) を選択します。
7. [Withdraw CIDR] (CIDR の取り消し) を選択します。

その結果、BYOIP CIDR のアドバタイズが取り消され、[Advertising] (アドバタイズ) 列の値が [Advertised] (アドバタイズ済み) から [Withdrawn] (取り消し) に変わります。

ステップ 2: Elastic IP アドレスの関連付けを解除する

このステップは、メンバーアカウントで実行する必要があります。AWS CLI を使用する場合は、`--profile` **`member-account`** オプションを使用します。

- 「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスの関連付けを解除する」にあるステップを実行して、EIP の関連付けを解除します。AWS マネジメントコンソールで EC2 を開くときには、EC2 との関連付けを解除した AWS リージョンが、BYOIP CIDR に使用するプールを作成したときに選択した `Locale` オプションと一致している必要があります。このチュートリアルでは、このプールはリージョンプールになります。

ステップ 3: Elastic IP アドレスを解放する

このステップは、メンバーアカウントで実行する必要があります。AWS CLI を使用する場合は、`--profile` **`member-account`** オプションを使用します。

- 「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを解放する」にあるステップを実行して、パブリック IPv4 プールから Elastic IP アドレス (EIP) を解放します。AWS マネジメントコンソールで EC2 を開くときには、EC2 を割り当てた AWS リージョンが、BYOIP CIDR に使用するプールを作成したときに選択した `Locale` オプションと一致している必要があります。

ステップ 4: RAM 共有をすべて削除して、RAM の AWS Organizations との統合を無効にする

このステップは、IPAM アカウントと管理アカウントのそれぞれで実行する必要があります。AWS CLI を使用して RAM 共有を削除し、RAM 統合を無効にする場合は、 `--profile` **`ipam-account`** および `--profile` **`management-account`** オプションを使用します。

- 「AWS RAM ユーザーガイド」内にある「AWS RAM のリソース共有を削除」と「AWS Organizations とのリソース共有を無効化」に記載されているステップをこの順序で行い、RAM 共有を削除して、AWS Organizations との RAM 統合を無効にします。

ステップ 5: リージョンレベルのプールと最上位プールから CIDR のプロビジョニングを解除する

このステップは、IPAM アカウントで実行する必要があります。AWS CLI を使用してプールを共有する場合は、`--profile` **`ipam-account`** オプションを使用します。

- プールから CIDR のプロビジョニングを解除するには のステップを実行して、リージョンプール、次に最上位プールの順序で、CIDR のプロビジョニングを解除します。

ステップ 6: リージョンレベルのプールと最上位プールを削除する

このステップは、IPAM アカウントで実行する必要があります。AWS CLI を使用してプールを共有する場合は、`--profile` **`ipam-account`** オプションを使用します。

- プールを削除する のステップを実行して、リージョンプール、次に最上位プールの順序で、リージョンプールを削除します。

ステップ 6 の代替方法

パブリック IPv4 プールを使用して Elastic IP アドレスを割り当てる場合は、ステップ 6: プールから Elastic IP アドレスを割り当てる のステップではなく、このセクションのステップを使用できます。

内容

ステップ 1: パブリック IPv4 プールの作成

このステップは、Elastic IP アドレスをプロビジョニングするメンバーアカウントが実行する必要があります。

> **Note**
>
> - このステップは、AWS CLI を使用してメンバーアカウントが実行する必要があります。
> - パブリック IPv4 プールと IPAM プールは、別個の AWS リソースによって管理されます。パブリック IPv4 プールは、パブリック所有の CIDR を Elastic IP アドレスに変換できるようにする単一のアカウントリソースです。IPAM プールは、パブリック空間をパブリック IPv4 プールに割り当てるために使用できます。

AWS CLI を使用してパブリック IPv4 プールを作成するには

- 以下のコマンドを実行して CIDR をプロビジョニングします。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールを作成したときに選択した `Locale` オプションと `--region` の値が一致する必要があります。

```
aws ec2 create-public-ipv4-pool --region us-east-2 --profile member-account
```

出力に、パブリック IPv4 プール ID が示されます。この ID は次のステップで必要になります。

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

ステップ 2: パブリック IPv4 CIDR のパブリック IPv4 プールへのプロビジョン

パブリック IPv4 CIDR をパブリック IPv4 プールにプロビジョンします。BYOIP CIDR に使用されるプールを選択したときに入力した `Locale` 値と `--region` の値が一致する必要があります。`--netmask-length` は、IPAM プールのスペースのうち、パブリックプールに取り込むスペースの量です。値は IPAM プールのネットマスクの長さより大きくすることはできません。定義できる最も具体的でない `--netmask-length` は 24 です。

> **Note**
>
> - /24 CIDR 範囲を IPAM に持ち込んで AWS Organization 全体で共有している場合は、このチュートリアルで示されているように /24 CIDR 全体をプロビジョニングするのではなく (`-- netmask-length 24` を使用)、/27 など、より小さいプレフィックスを複数の IPAM プールにプロビジョニングできます (`-- netmask-length 27` を使用)。
> - このステップは、AWS CLI を使用してメンバーアカウントが実行する必要があります。

AWS CLI を使用してパブリック IPv4 プールを作成するには

1. 以下のコマンドを実行して CIDR をプロビジョニングします。

```
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
```

   出力に、プロビジョンされた CIDR が示されます。

```
{
    "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. 次のコマンドを実行して、パブリック IPv4 プールにプロビジョンされた CIDR を表示します。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --max-results 10 --
profile member-account
```

   出力に、プロビジョンされた CIDR が示されます。デフォルトでは、CIDR はアドバタイズされません。つまり、インターネット経由でパブリックにアクセスできません。このチュートリアルの最後のステップで、この CIDR をアドバタイズするように設定できます。

```
{
```

```
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 255
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 255,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

パブリック IPv4 プールを作成した後に、IPAM リージョンプールに割り当てられているパブリック IPv4 プールを表示するには、IPAM コンソールを開き、[Allocations] (割り当て) または [Resources] (リソース) にあるリージョンプールの割り当てを確認します。

ステップ 3: パブリック IPv4 プールからの Elastic IP アドレスの割り当て

「Amazon EC2 ユーザーガイド」の 「Elastic IP アドレスを割り当てる」にあるステップを実行して、パブリック IPv4 プールから EIP を割り当てます。AWS マネジメントコンソールで EC2 を開くときには、EC2 を割り当てた AWS リージョンが、BYOIP CIDR に使用するプールを作成したときに選択した `Locale` オプションと一致している必要があります。

このステップは、メンバーアカウントで実行する必要があります。AWS CLI を使用する場合は、`--profile` **`member-account`** オプションを使用します。

これらの 3 つのステップを完了したら、ステップ 7: Elastic IP アドレスと EC2 インスタンスの関連付け に戻り、チュートリアルを完了するまで続行します。

ステップ 6 の代替方法 クリーンアップ

ステップ 9 の代替方法を使用して作成されたパブリック IPv4 プールをクリーンアップするには、次のステップを実行します。これらのステップは、ステップ 8: クリーンアップ の標準クリーンアッププロセス中に Elastic IP アドレスを解放した後に実行する必要があります。

ステップ 1: パブリック IPv4 CIDR のパブリック IPv4 プールへのプロビジョンを解除する

> **Important**
>
> このステップは、AWS CLI を使用してメンバーアカウントが実行する必要があります。

1. BYOIP CIDR を表示します。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

出力に、BYOIP CIDR の IP アドレスが示されます。

```
{
    "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. 次のコマンドを実行して、CIDR をパブリック IPv4 プールから解放します。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-2 --pool-id ipv4pool-
ec2-09037ce61cf068f9a --cidr 130.137.245.0/24 --profile member-account
```

3. BYOIP CIDR を再度表示して、プロビジョンされたアドレスがないことを確認します。このセクションのコマンドを実行するときは、--region の値が IPAM のリージョンと一致する必要があります。

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

出力に、パブリック IPv4 プール内の IP アドレス数が示されます。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

> **Note**
>
> IPAM では、パブリック IPv4 プールの割り当てが削除されたことが検出されるまでに時間がかかることがあります。割り当てが IPAM から削除されたことが表示されるまでは、IPAM プール CIDR のクリーンアップとプロビジョン解除を続行できません。

ステップ 2: パブリック IPv4 プールを削除する

このステップは、メンバーアカウントで実行する必要があります。

- 次のコマンドを実行して、パブリック IPv4 プールの CIDR を削除します。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールを作成したときに選択した Locale オプションと --region の値が一致する必要があります。このチュートリアルでは、このプールはリージョンプールになります。このステップは、AWS CLI を使用して実行する必要があります。

```
aws ec2 delete-public-ipv4-pool --region us-east-2 --pool-id ipv4pool-
ec2-09037ce61cf068f9a --profile member-account
```

出力には、戻り値 true が表示されます。

```
{
"ReturnValue": true
}
```

プールを削除した後に、IPAM によって管理されていない割り当てを表示するには、IPAM コンソールを開いて [Allocations] (割り当て) 内にあるリージョンプールの詳細を確認します。

AWS マネジメントコンソールを使用して、独自のパブリック IPv6 CIDR を IPAM に取り込む

このチュートリアルのステップに従って IPv6 CIDR を IPAM に取り込み、AWS マネジメントコンソールと AWS CLI の両方を使用して VPC を CIDR に割り振ります。

インターネット経由で IPv6 アドレスをアドバタイズする必要がない場合は、プライベート GUA IPv6 アドレスを IPAM にプロビジョニングできます。詳細については、「プライベート IPv6 GUA CIDR のプロビジョニングを有効にする」を参照してください。

Important

- このチュートリアルでは、次のセクションのステップがすでに完了していることを前提としています。
  - IPAM を AWS Organizations 内のアカウントと統合する.
  - IPAM を作成する.
- このチュートリアルの各ステップを、3 つの AWS Organizations アカウントのいずれかで実行する必要があります。
  - 管理アカウント。
  - IPAM を AWS Organizations 内のアカウントと統合する で IPAM 管理者として設定されるメンバーアカウント。このチュートリアルでは、このアカウントを IPAM アカウントと呼びます。

- IPAM プールから CIDR を割り当てる組織内のメンバーアカウント。このチュートリアルでは、このアカウントをメンバーアカウントと呼びます。

内容

ステップ 1: 最上位の IPAM プールを作成する

内部に 1 つのリージョンプールが含まれる最上位の IPAM プールを作成し、リージョンプールからリソースにスペースを割り当てるため、最上位のプールではなくリージョンプールにロケールを設定します。後のステップでリージョンプールを作成するときに、リージョンプールにロケールを追加します。IPAM を BYOIP と統合するには、BYOIP CIDR に使用されるプールにロケールを設定する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

プールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。パブリックスコープを選択します。スコープの詳細については、「IPAM の仕組み」を参照してください。
4. [プールを作成] を選択します。
5. (オプション) プールの [名前タグ] とプールの [説明] を追加します。
6. [ソース] で [IPAM 範囲] を選択します。
7. [アドレスファミリー] で、[IPv6] を選択します。

8. [リソース計画] で、[範囲内のIP スペースの計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
9. [Locale] (ロケール) で、[None] (なし) を選択します。リージョンプールにロケールを設定します。

   ロケールは、この IPAM プールを割り当てることができるようにする AWS リージョンです。例えば、VPC の CIDR は、VPC のリージョンとロケールを共有する IPAM プールからしか割り当てることができません。プールのロケールを選択したら、変更はできないことに注意してください。停止が原因で IPAM のホームリージョンが使用できなくなり、プールのロケールが IPAM のホームリージョンと異なる場合でも、プールを使用して IP アドレスを割り当てることができます。

   > **Note**
   >
   > 内部にリージョンプールを含むトップレベルプールを作成するのではなく、プールを 1 つだけ作成する場合は、このプールにロケールを選択して、プールを割り当てることができるようにします。

10. [パブリック IP ソース] には、[BYOIP] がデフォルトで選択されています。
11. [プロビジョニングする CIDR] で次のいずれかを実行します。

    - X.509 証明書でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR と BYOIP メッセージおよびそのステップで作成した証明書署名を含める必要があります。
    - DNS TXT レコード でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR およびそのステップで作成した IPAM 検証トークンを含める必要があります。

    IPv6 CIDR をトップレベルのプール内にあるプールにプロビジョニングする際、持ち込みできる最も具体的な IPv6 アドレス範囲は、パブリックにアドバタイズ可能な CIDR の場合は /48 であり、パブリックにアドバタイズ可能でない CIDR の場合は /60 であることに注意してください。

> **Important**
>
> ほとんどのプロビジョニングは 2 時間以内に完了しますが、パブリックにアドバタイズ可能な範囲のプロビジョニングプロセスが完了するまでに最大 1 週間かかる場合があります。

12. [このプールの割り当てルールを設定する] は選択しません。
13. (オプション) プールのタグを選択します。
14. [プールを作成] を選択します。

続行する前に、この CIDR のプロビジョンが完了したことを確認してください。プロビジョニングの状態は、プールの詳細ページの CIDR タブで確認できます。

ステップ 2. 最上位プール内にリージョンプールを作成する

最上位プール内にリージョンプールを作成する プールにはロケールが必須であり、IPAM を作成したときに構成したオペレーションリージョンのいずれかを指定する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

トップレベルプール内にリージョンプールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。デフォルトのプライベートスコープを使用しない場合は、コンテンツペインの上部にあるドロップダウンメニューから、使用するスコープを選択します。スコープの詳細については、「IPAM の仕組み」を参照してください。
4. [プールを作成] を選択します。
5. (オプション) プールの[名前タグ]とプールの説明を入力します。
6. [ソース] で、前のセクションで作成した最上位レベルのプールを選択します。
7. [リソース計画] で、[範囲内のIP スペースの計画] は選択したままにしておきます。このオプションを使用して VPC 内のサブネット IP スペースを計画する方法の詳細については、「チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する」を参照してください。
8. プールのロケールを選択します。ロケールを選択すると、プールとそのプールから割り当てられるリソースの間にクロスリージョン依存関係がないことが保証されます。使用可能なオプション

は、IPAM を作成したときに選択した運用リージョンによって提供されます。このチュートリアルでは、us-east-2 をリージョンプールのロケールとして使用します。

ロケールは、この IPAM プールを割り当てることができるようにする AWS リージョンです。例えば、VPC の CIDR は、VPC のリージョンとロケールを共有する IPAM プールからしか割り当てることができません。プールのロケールを選択したら、変更はできないことに注意してください。停止が原因で IPAM のホームリージョンが使用できなくなり、プールのロケールが IPAM のホームリージョンと異なる場合でも、プールを使用して IP アドレスを割り当てることができます。

9. [Service] (サービス) で、[EC2 (EIP/VPC)] を選択します。選択したサービスによって、CIDR がアドバタイズ可能になる AWS サービスが決定します。現在、唯一の選択肢は EC2 (EIP/VPC) であり、このプールから割り当てられた CIDR は、Amazon EC2 サービスと Amazon VPC サービス (VPC に関連付けられている CIDR の場合) に対してアドバタイズできるようになります。
10. [CIDRs to provision] (プロビジョニングする CIDR) で、プールにプロビジョニングする CIDR を選択します。IPv6 CIDR をトップレベルのプール内にあるプールにプロビジョニングする際、持ち込みできる最も具体的な IPv6 アドレス範囲は、パブリックにアドバタイズ可能な CIDR の場合は /48 であり、パブリックにアドバタイズ可能でない CIDR の場合は /60 であることに注意してください。
11. [このプールの割り当てルールを設定する] を有効にし、このプールのオプションルールを選択します。

    - [Automatically import discovered resources] (検出されたリソースを自動的にインポートする): このオプションは、[Locale] (ロケール) が [None] (なし) に設定されている場合は選択できません。選択すると、IPAM はこのプールの CIDR 範囲内のリソースを継続的に検索し、自動的に割り当てとして IPAM にインポートします。次の点に注意してください。
      - インポートを成功させるためには、これらのリソースに割り当てられる CIDR がすでに他のリソースに割り当られていてはなりません。
      - IPAM は、プールの割り当てルールに準拠しているかどうかに関係なく CIDR をインポートするため、リソースがインポートされ、その後、非準拠としてマークされる可能性があります。
      - 重複する複数の CIDR を IPAM が検出した場合、IPAM は最大 CIDR のみをインポートします。
      - IPAM が一致する CIDR を持つ複数の CIDR を検出した場合、IPAM はそれらのうちの 1 つだけをランダムにインポートします。
    - [Minimum netmask length] (ネットマスクの最小長): この IPAM プール内の CIDR 割り当てが準拠するために必要なネットマスクの最小長と、プールから割り当てられる最大サイズの

CIDR ブロック。ネットマスクの最小長は、ネットマスクの最大長より小さくなければなりません。IPv4 アドレスに使用できるネットマスクの長さは `0 ~ 32` です。IPv6 アドレスに使用できるネットマスクの長さは `0 ~ 128` です。

- [Default netmask length] (デフォルトのネットマスク長): このプールに追加される割り当てのデフォルトのネットマスク長。
- [Maximum netmask length] (ネットマスクの最大長): このプールの CIDR 割り当てに必要なネットマスクの最大長。この値は、プールから割り当てられる最小サイズの CIDR ブロックを示します。この値が最小でも **/48** であることを確認します。
- [タグ付け要件]: プールからスペースを割り当てるためにリソースに必要なタグ。スペースを割り当てた後にリソースのタグが変更された場合、またはプールで割り当てのタグ付けルールが変更された場合、リソースは非準拠としてマークされることがあります。
- [ロケール]: このプールの CIDR を使用するリソースに必要なロケール。このロケールが設定されていない、自動的にインポートされたリソースは、非準拠としてマークされます。プールに自動的にインポートされないリソースは、このロケールでない限り、プールからスペースを割り当てることはできません。

12. (オプション) プールのタグを選択します。
13. プールの設定が完了したら、[Create pool] (プールの作成) を選択します。

続行する前に、この CIDR のプロビジョンが完了したことを確認してください。プロビジョニングの状態は、プールの詳細ページの CIDR タブで確認できます。

ステップ 3. リージョンプールを共有する

このセクションのステップに従い、AWS Resource Access Manager (RAM) を使用して IPAM プールを共有します。

AWS RAM 内でリソース共有を有効にする

IPAM を作成したら、リージョンプールを組織内の他のアカウントと共有する必要があります。IPAM プールを共有する前に、このセクションのステップを完了し、AWS RAM とのリソース共有を有効にします。AWS CLI を使用してリソース共有を有効にする場合は、`--profile` **`management-account`** オプションを使用します。

リソース共有を有効にするには

1. AWS Organizations 管理アカウントを使って AWS RAM コンソール (https://console.aws.amazon.com/ram/) を開きます。

2. ナビゲーションペインで [設定] を選択し、[AWS Organizations との共有を有効にする] を選択し、[設定の保存] を選択します。

これで、IPAM プールを組織の他のメンバーと共有できるようになりました。

AWS RAM を使用して IPAM プールを共有する

このセクションでは、リージョンプールを他の AWS Organizations メンバーアカウントと共有します。必要な IAM アクセス許可に関する情報を含め、IPAM プールの共有に関する詳細な手順については、「AWS RAM を使用して IPAM プールを共有する」を参照してください。AWS CLI を使用してリソース共有を有効にする場合は、`--profile` **`ipam-account`** オプションを使用します。

AWS RAM を使用して IPAM プールを共有するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択し、IPAM プールを選択して、[アクション] > [詳細を表示] の順に選択します。
4. [Resource sharing] (リソース共有) で [Create resource share] (リソース共有の作成) を選択します。AWS RAM コンソールが開きます。AWS RAM を使用してプールを共有します。
5. [リソースの共有の作成] を選択します。
6. AWS RAM コンソールで、[リソースの共有を作成] を再度選択します。
7. 共有リソースの [名前] を追加します。
8. [リソースタイプを選択] で [IPAM プール] を選択し、次に共有したいプールの ARN を選択します。
9. [次へ] を選択します。
10. AWSRAMPermissionIpamPoolByoipCidrImport 許可を選択します。アクセス許可オプションの詳細は本チュートリアルの対象外ですが、このオプションの詳細は「AWS RAM を使用して IPAM プールを共有する」にてご覧いただけます。
11. [次へ] を選択します。
12. [プリンシパル] > [プリンシパルタイプを選択] で、[AWS アカウント] を選択し、IPAM に IP アドレス範囲を取り込むアカウントのアカウント ID を入力して、[追加] を選択します。
13. [次へ] を選択します。
14. リソース共有オプションと共有先のプリンシパルを確認し、[作成] を選択します。

15. IPAM プールからの IP アドレス CIDR の割り当てを **member-account** アカウントに許可するには、`AWSRAMDefaultPermissionsIpamPool` を使用して 2 つ目のリソース共有を作成します。`--resource-arns` の値は、前のセクションで作成した IPAM プールの ARN です。`--principals` の値は、**member-account** のアカウント ID です。`--permission-arns` の値は、`AWSRAMDefaultPermissionsIpamPool` アクセス許可の ARN です。

ステップ 4: VPC の作成

Amazon VPC ユーザーガイドの「VPC を作成する」にあるステップに従います。

このステップは、メンバーアカウントで実行する必要があります。

> **Note**
>
> - AWS マネジメントコンソールで VPC を開くときには、VPC を作成した AWS リージョンが、BYOIP CIDR に使用するプールを作成したときに選択した `Locale` オプションと一致している必要があります。
> - VPC の CIDR を選択する手順に達すると、IPAM プールから CIDR を使用するオプションが表示されます。このチュートリアルで作成したリージョンプールを選択します。

VPC を作成するときに、AWS が IPAM プール内の CIDR を VPC に割り当てます。割り当ては、IPAM コンソールのコンテンツペインでプールを選択し、そのプールの [Allocations] (割り当て) タブを表示することで確認できます。

ステップ 5: CIDR のアドバタイズ

このセクションのステップは、IPAM アカウントで実行する必要があります。VPC を作成したら、Service EC2 (EIP/VPC) が設定されているプールにある、AWS で使用することにした CIDR のアドバタイズを開始できます。このチュートリアルでは、これはリージョンプールです。デフォルトでは、CIDR はアドバタイズされません。つまり、インターネット経由でパブリックにアクセスできません。

このステップは、IPAM アカウントで実行する必要があります。

CIDR をアドバタイズするには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。

3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。パブリックスコープを選択します。スコープの詳細については、IPAM の仕組みを参照してください。
4. このチュートリアルで作成したリージョンプールを選択します。
5. [CIDRs] (CIDR) タブを選択します。
6. BYOIP CIDR を選び、[Actions] (アクション) > [Advertise] (アドバタイズ) を選択します。
7. [Advertise CIDR] (CIDR のアドバタイズ) を選択します。

その結果、BYOIP CIDR がアドバタイズされ、[Advertising] (アドバタイズ) 列の値が [Withdrawn] (取り消し) から [Advertised] (アドバタイズ済み) に変わります。

ステップ 6: クリーンアップ

このセクションのステップに従って、このチュートリアルでプロビジョンし、作成したリソースをクリーンアップします。

ステップ 1: CIDR のアドバタイズを取り消す

このステップは、IPAM アカウントで実行する必要があります。

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. デフォルトでは、プールを作成すると、デフォルトのプライベートスコープが選択されます。パブリックスコープを選択します。
4. このチュートリアルで作成したリージョンプールを選択します。
5. [CIDRs] (CIDR) タブを選択します。
6. BYOIP CIDR を選び、[Actions] (アクション) > [Withdraw from advertising] (アドバタイズの取り消し) を選択します。
7. [Withdraw CIDR] (CIDR の取り消し) を選択します。

その結果、BYOIP CIDR のアドバタイズが取り消され、[Advertising] (アドバタイズ) 列の値が [Advertised] (アドバタイズ済み) から [Withdrawn] (取り消し) に変わります。

ステップ 2: VPC を削除する

このステップは、メンバーアカウントで実行する必要があります。

- Amazon VPC ユーザーガイドの「VPC を削除する」にあるステップを完了して VPC を削除します。AWS マネジメントコンソールで VPC を開くときに、VPC を削除した AWS リージョンが、BYOIP CIDR に使用するプールを作成したときに選択した `Locale` オプションと一致している必要があります。このチュートリアルでは、このプールはリージョンプールになります。

  VPC を削除すると、IPAM がリソースが削除されたことを検出し、VPC に割り当てられた CIDR の割り当てを解除するまでに時間がかかります。プール詳細 [Allocations] (割り当て) タブで、IPAM がプールから割り当てを削除したことを確認できるまでは、クリーンアップの次のステップに進むことはできません。

ステップ 3: RAM 共有を削除して、RAM の AWS Organizations との統合を無効にする

このステップは、IPAM アカウントと管理アカウントのそれぞれで実行する必要があります。

- 「AWS RAM ユーザーガイド」内にある「AWS RAM のリソース共有を削除」と「AWS Organizations とのリソース共有を無効化」に記載されているステップをこの順序で行い、RAM 共有を削除して、AWS Organizations との RAM 統合を無効にします。

ステップ 4: リージョンプールと最上位プールから CIDR のプロビジョニングを解除する

このステップは、IPAM アカウントで実行する必要があります。

- プールから CIDR のプロビジョニングを解除するには のステップを実行して、リージョンプール、次に最上位プールの順序で、CIDR のプロビジョニングを解除します。

ステップ 5: リージョンプールと最上位プールを削除する

このステップは、IPAM アカウントで実行する必要があります。

- プールを削除する のステップを実行して、リージョンプール、次に最上位プールの順序で、リージョンプールを削除します。

AWS CLI のみを使用した IPAM への独自の IP CIDR の持ち込み

IPAM に自分の IP を導入 (BYOIP) すると、AWS で組織の既存の IPv4 および IPv6 アドレス範囲を使用できます。これにより、独自の IP アドレス空間でオンプレミス環境とクラウド環境を統一することで、一貫したブランドを維持し、ネットワークパフォーマンスを改善するとともに、セキュリティを強化して、管理を簡素化できます。

AWS CLI のみを使用して、IPv4 または IPv6 CIDR を IPAM に取り込む方法については、次のステップを実行してください。

> **Note**
>
> 開始する前に、まずドメインコントロールを検証する必要があります。

IPv4 アドレス範囲を AWS に設定すると、最初のアドレス (ネットワークアドレス) と最後のアドレス (ブロードキャストアドレス) を含む、その範囲内のすべての IP アドレスを使用できます。

内容

AWS CLI のみを使用した IPAM への自分のパブリック IPv4 CIDR の取り込み

AWS CLI のみを使用して、IPAM に IPv4 CIDR を取り込み、Elastic IP アドレス (EIP) を CIDR に割り当てる手順は次のとおりです。

> **Important**
>
> - このチュートリアルでは、次のセクションのステップがすでに完了していることを前提としています。
>   - IPAM を AWS Organizations 内のアカウントと統合する.
>   - IPAM を作成する.
> - このチュートリアルの各ステップを、3 つの AWS Organizations アカウントのいずれかで実行する必要があります。
>   - 管理アカウント。
>   - IPAM を AWS Organizations 内のアカウントと統合する で IPAM 管理者として設定されるメンバーアカウント。このチュートリアルでは、このアカウントを IPAM アカウントと呼びます。
>   - IPAM プールから CIDR を割り当てる組織内のメンバーアカウント。このチュートリアルでは、このアカウントをメンバーアカウントと呼びます。

内容

ステップ 1: AWS CLI の名前付きプロファイルと IAM ロールを作成する

このチュートリアルをシングル AWS ユーザーとして完了するには、AWS CLI の名前付きプロファイルを使用して、1 つの IAM ロールから別のアカウントへと切り替えることができます。名前付きプロファイルは、AWS CLI を使用して `--profile` オプションを使用するときに参照する設定と認証情報の集まりです。AWS アカウントの IAM ロールと指定したプロファイルを作成する方法の詳細については、の「AWS CLI での IAM ロールの使用」を参照してください。

このチュートリアルで使用する 3 つの AWS アカウントごとに、1 つのロールと 1 つの名前付きプロファイルを作成します。

- AWS Organizations 管理アカウント向けの `management-account` と呼ばれるプロファイル。
- IPAM 管理者として設定された AWS Organizations メンバーアカウント向けの、`ipam-account` と呼ばれるプロファイル。
- IPAM プールから CIDR を割り当てる自分の組織の AWS Organizations メンバーアカウント向けの、`member-account` と呼ばれるプロファイル。

IAM ロールと名前付きプロファイルを作成した後、このページに戻り次のステップに進みます。なお、このチュートリアルの残りの部分では、サンプルの AWS CLI コマンドで `--profile` オプショ

ンを名前付きプロファイルのうちの 1 つとともに使用することにより、どのアカウントでコマンドを実行する必要があるのかを示しています。

ステップ 2: IPAM を作成する

この手順は省略可能です。us-east-1 と us-west-2 の運用リージョンで作成された IPAM が既にある場合は、このステップをスキップできます。IPAM を作成し、us-east-1 と us-west-2 の運用リージョンを指定します。運用リージョンを選択する必要があるのは、IPAM プールの作成時にロケールオプションを使用できるようにするためです。IPAM を BYOIP と統合するには、BYOIP CIDR に使用されるプールにロケールを設定する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

次のコマンドを実行します。

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

出力に、作成した IPAM が示されます。PublicDefaultScopeId の値を書き留めます。パブリックスコープ ID は、次のステップで必要になります。BYOIP CIDR はパブリック IP アドレスであるため、パブリックスコープを使用しています。パブリックスコープはこのために存在します。

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

```
}
```

ステップ 3: 最上位の IPAM プールの作成する

このセクションのステップに従って、最上位の IPAM プールを作成します。

このステップは、IPAM アカウントで実行する必要があります。

AWS を使用してすべての AWS CLI リソースの IPv4 アドレスプールを作成するには

1. 次のコマンドを実行して、IPAM プールを作成します。前のステップで作成した IPAM のパブリックスコープの ID を使用します。

   このステップは、IPAM アカウントで実行する必要があります。

   ```
   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
   ```

   出力に、create-in-progress と表示されます。これは、プールの作成が進行中であることを示します。

   ```
   {
       "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. 出力に create-complete という状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

次の出力例は、プールの状態を示しています。

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

ステップ 4: CIDR を最上位プールにプロビジョニングする

最上位プールに CIDR ブロックをプロビジョンします。IPv4 CIDR を最上位のプール内のプールにプロビジョニングするとき、プロビジョンできる最小の IPv4 CIDR は /24 です。より具体的な CIDR (/25 など) は許可されません。

> **Note**
>
> - X.509 証明書でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR と BYOIP メッセージおよびそのステップで作成した証明書署名を含める必要があります。

- DNS TXT レコード でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR およびそのステップで作成した IPAM 検証トークンを含める必要があります。

BYOIP CIDR を最上位プールにプロビジョンする場合は、ドメインコントロールを検証するだけで済みます。最上位プール内のリージョンプールについては、ドメイン所有者検証オプションを省略できます。

このステップは、IPAM アカウントで実行する必要があります。

> **Important**
>
> BYOIP CIDR を最上位プールにプロビジョンする場合は、ドメインコントロールを検証するだけで済みます。最上位プール内のリージョンプールについては、ドメインコントロールオプションを省略できます。BYOIP を IPAM にオンボードすると、リージョンとアカウントとの間で BYOIP を分割するときに、所有権の検証を実行する必要がなくなります。

AWS CLI を使用して CIDR ブロックをプールにプロビジョニングするには

1. 証明書情報を使用して CIDR をプロビジョニングするには、次のコマンド例を使用します。この例で必要に応じて値を置き換えるだけでなく、Message および Signature の値を、X.509 証明書を使用してドメインを検証する で取得した text_message および signed_message の値に置き換えてください。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-
pool-id ipam-pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --
verification-method remarks-x509 --cidr-authorization-context
 Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsMaU0P7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRYOdRaNx8yt-uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

   検証トークン情報を使用して CIDR をプロビジョニングするには、次のコマンド例を使用します。この例で必要に応じて値を置き換えるだけでなく、ipam-ext-res-ver-

token-0309ce7f67a768cf0 を DNS TXT レコードを使用してドメインを検証する で取得した IpamExternalResourceVerificationTokenId トークン ID に置き換えてください。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --verification-method dns-
token --ipam-external-resource-verification-token-id ipam-ext-res-ver-
token-0309ce7f67a768cf0 --profile ipam-account
```

出力に、CIDR のプロビジョンが保留されていることが示されます。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. 続行する前に、この CIDR のプロビジョンが完了したことを確認してください。

> **Important**
>
> ほとんどのプロビジョニングは 2 時間以内に完了しますが、パブリックにアドバタイズ可能な範囲のプロビジョニングプロセスが完了するまでに最大 1 週間かかる場合があります。

出力に provisioned という状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

次の出力例に、その状態が示されています。

```
{
    "IpamPoolCidrs": [
        {
```

```
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

ステップ 5: 最上位プール内にリージョンプールを作成する

最上位プール内にリージョンプールを作成する

プールのロケールは、以下のいずれかにする必要があります。

- この IPAM プールを割り当て可能にする AWS リージョン。
- この IPAM プールを割り当て可能にする AWS Local Zone のネットワーク境界グループ (サポートされるローカルゾーン)。このオプションを利用できるのは、パブリックスコープ内の IPAM IPv4 プールのみです。
- AWS Dedicated Local Zone。AWS Dedicated Local Zone 内にプールを作成するには、セレクタ入力に AWS Dedicated Local Zone を入力します。
- `Global` CloudFront ロケーションなど、すべての AWS リージョンで IP アドレスをグローバルに使用する場合。`Global` ロケールはパブリック IPv4 プールでのみ使用できます。

例えば、VPC の CIDR は、VPC のリージョンとロケールを共有する IPAM プールからしか割り当てることができません。プールのロケールを選択したら、変更はできないことに注意してください。停止が原因で IPAM のホームリージョンが使用できなくなり、プールのロケールが IPAM のホームリージョンと異なる場合でも、プールを使用して IP アドレスを割り当てることができます。

このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールの作成時に入力した `--locale` オプションが `--region` の値に含まれている必要があります。例えば、us-east-1 のロケールで BYOIP プールを作成した場合、`--region` は us-east-1 にする必要があります。us-east-1-scl-1 (Local Zone に使用されるネットワーク境界グループ) のロケールで BYOIP プールを作成した場合は、`--region` を us-east-1 にする必要があります。これは、このリージョンがロケール us-east-1-scl-1 を管理するからです。

このステップは、IPAM アカウントで実行する必要があります。

ロケールを選択すると、プールとそのプールから割り当てられるリソースの間にクロスリージョン依存関係がないことが保証されます。使用可能なオプションは、IPAM を作成したときに選択した運用

リージョンによって提供されます。このチュートリアルでは、us-west-2 をリージョンプールの口ケールとして使用します。

> **Important**
>
> プールを作成するときは、--aws-service ec2 を含める必要があります。選択したサービスによって、CIDR がアドバタイズ可能になる AWS サービスが決定します。現在、唯一の選択肢は ec2 であり、このプールから割り当てられた CIDR は、Amazon EC2 サービス (Elastic IP アドレスの場合) と Amazon VPC サービス (VPC に関連付けられている CIDR の場合) に対してアドバタイズできるようになります。

AWS CLI を使用してリージョンプールを作成するには

1. 次のコマンドを実行して、プールを作成します。

```
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
```

出力に、IPAM がプールを作成していることが表示されます。

```
{
     "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. 出力に create-complete という状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

出力には、IPAM にあるプールが表示されます。このチュートリアルでは、最上位プールとリージョンプールを作成したので、両方が表示されます。

ステップ 6: リージョンプールに CIDR をプロビジョニングする

リージョンプールに CIDR ブロックをプロビジョンします。

> **Note**
>
> CIDR を最上位プール内のリージョンプールにプロビジョニングする場合、プロビジョニングできる最も具体的な IPv4 CIDR は /24 です。より具体的な CIDR (/25 など) は許可されません。リージョンプールを作成すると、リージョンプール内に小さなプール (/25 など) を作成できます。リージョンプールまたはリージョンプール内のプールを共有する場合、これらのプールは同じリージョンプールで設定されたロケールでのみ使用できることに注意してください。

このステップは、IPAM アカウントで実行する必要があります。

AWS CLI を使用して CIDR ブロックをリージョンプールに割り当てるには

1. 以下のコマンドを実行して CIDR をプロビジョニングします。

```
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
```

出力に、CIDR のプロビジョンが保留されていることが示されます。

```
{
    "IpamPoolCidr": {
```

```
        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. 出力に、provisioned の状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

次の出力例に、正しい状態が示されています。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

ステップ 7: CIDR をアドバタイズする

このセクションのステップは、IPAM アカウントで実行する必要があります。Elastic IP アドレス (EIP) をインスタンスまたは Elastic Load Balancer に関連付けると、--aws-service ec2 が定義されているプール内にある、AWS に取り込んだ CIDR のアドバタイズを開始できます。このチュートリアルでは、これはリージョンプールです。デフォルトでは、CIDR はアドバタイズされません。つまり、インターネット経由でパブリックにアクセスできません。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールを作成したときに入力した --locale オプションと --region の値が一致する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

> **Note**
>
> アドバタイズメントステータスによって Elastic IP アドレスを割り当てる機能が制限されることはありません。BYOIPv4 CIDR がアドバタイズされていなくても、IPAM プールから EIP を作成できます。

AWS CLI を使用して CIDR のアドバタイズを開始するには

- 次のコマンドを実行して、CIDR をアドバタイズします。

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
profile ipam-account
```

出力に、CIDR がアドバタイズされたことが示されます。

```
{
    "ByoipCidr": {
        "Cidr": "130.137.245.0/24",
        "State": "advertised"
    }
}
```

ステップ 8: リージョンレベルのプールを共有する

このセクションのステップに従い、AWS Resource Access Manager (RAM) を使用して IPAM プールを共有します。

AWS RAM 内でリソース共有を有効にする

IPAM を作成したら、リージョンプールを組織内の他のアカウントと共有する必要があります。IPAM プールを共有する前に、このセクションのステップを完了し、AWS RAM とのリソース共有を有効にします。AWS CLI を使用してリソース共有を有効にする場合は、`--profile management-account` オプションを使用します。

リソース共有を有効にするには

1. AWS Organizations 管理アカウントを使って AWS RAM コンソール (https://console.aws.amazon.com/ram/) を開きます。

2. ナビゲーションペインで [設定] を選択し、[AWS Organizations との共有を有効にする] を選択し、[設定の保存] を選択します。

これで、IPAM プールを組織の他のメンバーと共有できるようになりました。

AWS RAM を使用して IPAM プールを共有する

このセクションでは、リージョンプールを他の AWS Organizations メンバーアカウントと共有します。必要な IAM アクセス許可に関する情報を含め、IPAM プールの共有に関する詳細な手順については、「AWS RAM を使用して IPAM プールを共有する」を参照してください。AWS CLI を使用してリソース共有を有効にする場合は、`--profile` **`ipam-account`** オプションを使用します。

AWS RAM を使用して IPAM プールを共有するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択し、IPAM プールを選択して、[アクション] > [詳細を表示] の順に選択します。
4. [Resource sharing] (リソース共有) で [Create resource share] (リソース共有の作成) を選択します。AWS RAM コンソールが開きます。AWS RAM を使用してプールを共有します。
5. [リソースの共有の作成] を選択します。
6. AWS RAM コンソールで、[リソースの共有を作成] を再度選択します。
7. 共有リソースの [名前] を追加します。
8. [リソースタイプを選択] で [IPAM プール] を選択し、次に共有したいプールの ARN を選択します。
9. [次へ] を選択します。
10. AWSRAMPermissionIpamPoolByoipCidrImport 許可を選択します。アクセス許可オプションの詳細は本チュートリアルの対象外ですが、このオプションの詳細は「AWS RAM を使用して IPAM プールを共有する」にてご覧いただけます。
11. [次へ] を選択します。
12. [プリンシパル] > [プリンシパルタイプを選択] で、[AWS アカウント] を選択し、IPAM に IP アドレス範囲を取り込むアカウントのアカウント ID を入力して、[追加] を選択します。
13. [次へ] を選択します。
14. リソース共有オプションと共有先のプリンシパルを確認し、[作成] を選択します。

15. IPAM プールからの IP アドレス CIDR の割り当てを **member-account** アカウントに許可するには、AWSRAMDefaultPermissionsIpamPool を使用して 2 つ目のリソース共有を作成します。--resource-arns の値は、前のセクションで作成した IPAM プールの ARN です。--principals の値は、**member-account** のアカウント ID です。--permission-arns の値は、AWSRAMDefaultPermissionsIpamPool アクセス許可の ARN です。

ステップ 9: プールから Elastic IP アドレスを割り当てる

プールから Elastic IP アドレスを割り当てるには、このセクションのステップを実行します。パブリック IPv4 プールを使用して Elastic IP アドレスを割り当てる場合は、このセクションのステップではなく、ステップ 9 の代替方法 の代替ステップを使用できます。

> **Important**
>
> ec2:AllocateAddress を呼び出す許可がないことに関するエラーが表示される場合は、共有された IPAM プールに現在割り当てられているマネージド許可を更新する必要があります。リソース共有の作成者に連絡して、マネージド許可 AWSRAMPermissionIpamResourceDiscovery をデフォルトバージョンに更新するよう依頼してください。詳細については、AWS RAM ユーザーガイドの「リソース共有の更新」を参照してください。

AWS Management Console

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを割り当てる」のステップに従ってアドレスを割り当てます。ただし、次の点に注意してください。

- このステップは、メンバーアカウントで実行する必要があります。
- EC2 コンソールで使用している AWS リージョンが、リージョンレベルのプールの作成時に選択したロケールオプションと一致しているようにします。
- アドレスプールを選択する際には、[IPv4 IPAM プールを使用して割り当てる] オプションを選択し、作成したリージョンレベルのプールを選択します。

Command line

allocate-address コマンドを使用して、プールからアドレスを割り当てます。使用する --region は、ステップ 2 でプールを作成した際に選択した -locale オプションと一致する必要

があります。--ipam-pool-id のステップ 2 で作成した IPAM プールの ID を含めます。オプションで、--address オプションを使用して IPAM プール内の特定の /32 を選択することもできます。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

レスポンスの例:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを割り当てる」を参照してください。

ステップ 10: Elastic IP アドレスと EC2 インスタンスの関連付け

Elastic IP アドレスを EC2 インスタンスに関連付けるには、このセクションのステップを実行します。

AWS Management Console

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを関連付ける」のステップに従って、IPAM プールから Elastic IP アドレスを割り当てます。ただし、次に注意してください: AWS マネジメントコンソールオプションを使用する場合、Elastic IP アドレスを関連付ける AWS リージョンは、リージョンレベルのプールの作成時に選択したロケールオプションと一致する必要があります。

このステップは、メンバーアカウントで実行する必要があります。

Command line

このステップは、メンバーアカウントで実行する必要があります。--profile **member-account** オプションを使用する

associate-address コマンドを使用して、Elastic IP アドレスをインスタンスに関連付けます。Elastic IP アドレスを関連付ける --region は、リージョンレベルのプールを作成した際に選択した --locale オプションと一致する必要があります。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

レスポンスの例:

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスをインスタンスまたはネットワークインターフェイスに関連付ける」を参照してください。

ステップ 11: クリーンアップ

このセクションのステップに従って、このチュートリアルでプロビジョンし、作成したリソースをクリーンアップします。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールの作成時に入力した --locale オプションが --region の値に含まれている必要があります。

AWS CLI を使用したクリーンアップ

1. IPAM で管理されている EIP 割り当てを表示します。

   このステップは、IPAM アカウントで実行する必要があります。

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   出力に、IPAM での割り当てが示されます。

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "130.137.245.0/24",
   ```

```
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

2. IPv4 CIDR のアドバタイズを停止します。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
profile ipam-account
```

   出力に、CIDR の状態が [advertised] (アドバタイズ済) から [provisioned] (プロビジョン済) に変更されていることが示されます。

```
{
    "ByoipCidr": {
        "Cidr": "130.137.245.0/24",
        "State": "provisioned"
    }
}
```

3. Elastic IP アドレスを解放します。

   このステップは、メンバーアカウントで実行する必要があります。

```
aws ec2 release-address --region us-west-2 --allocation-
id eipalloc-0db3405026756dbf6 --profile member-account
```

   このコマンドの実行では出力は表示されません。

4. IPAM で管理されていない EIP 割り当てを表示します。IPAM が Elastic IP アドレスが削除されたことを検出するには、しばらく時間がかかる場合があります。割り当てが IPAM から削除されたことが表示されるまでは、IPAM プール CIDR のクリーンアップとプロビジョン解除を続行できません。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールの作成時に入力した `--locale` オプションが `--region` の値に含まれている必要があります。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

出力に、IPAM での割り当てが示されます。

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

5. リージョンプール CIDR のプロビジョンを解除します。このステップのコマンドを実行するときは、IPAM のリージョンと `--region` の値が一致する必要があります。

   このステップは、IPAM アカウントで実行する必要があります。

```
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
```

   出力に、CIDR のプロビジョン解除が保留されていることが示されます。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }

}
```

   プロビジョン解除の完了には、しばらく時間がかかります。プロビジョニング解除のステータスをチェックします。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   [deprovisioned] (プロビジョン解除済) が表示されるまで待ってから、次のステップに進みます。

```
{
```

```
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

6. RAM 共有を削除し、AWS Organizations との RAM 統合を無効にします。「AWS RAM ユーザーガイド」内にある「AWS RAM のリソース共有を削除」と「AWS Organizations とのリソース共有を無効化」に記載されているステップをこの順序で行い、RAM 共有を削除して、AWS Organizations との RAM 統合を無効にします。

   このステップは、IPAM アカウントと管理アカウントのそれぞれで実行する必要があります。AWS CLI を使用して RAM 共有を削除し、RAM 統合を無効にする場合は、 `--profile` **`ipam-account`** および `--profile` **`management-account`** オプションを使用します。

7. リージョンプールを削除します。このステップのコマンドを実行するときは、IPAM のリージョンと `--region` の値が一致する必要があります。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   出力に、削除状態が表示されます。

```
{
   "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
        "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0d8f3646b61ca5987",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
```

```
        "State": "delete-in-progress",
        "Description": "reg-ipv4-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

8. 最上位プール CIDR のプロビジョンを解除します。このステップのコマンドを実行するときは、IPAM のリージョンと `--region` の値が一致する必要があります。

   このステップは、IPAM アカウントで実行する必要があります。

```
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
```

   出力に、CIDR のプロビジョン解除が保留されていることが示されます。

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }

}
```

   プロビジョン解除の完了には、しばらく時間がかかります。次のコマンドを実行して、プロビジョン解除のステータスを確認します。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

   [deprovisioned] (プロビジョン解除済) が表示されるまで待ってから、次のステップに進みます。

```
{
    "IpamPoolCidr": {
```

```
        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. 最上位プールを削除します。このステップのコマンドを実行するときは、IPAM のリージョンと --region の値が一致する必要があります。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

   出力に、削除状態が表示されます。

```
{
  "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

10. IPAM を削除します。このステップのコマンドを実行するときは、IPAM のリージョンと --region の値が一致する必要があります。

    このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

出力に、IPAM 応答が示されます。これは、IPAM が削除されたことを示します。

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

ステップ 9 の代替方法

パブリック IPv4 プールを使用して Elastic IP アドレスを割り当てる場合は、ステップ 9: プールから Elastic IP アドレスを割り当てる のステップではなく、このセクションのステップを使用できます。

内容

- ステップ 1: パブリック IPv4 プールの作成
- ステップ 2: パブリック IPv4 CIDR のパブリック IPv4 プールへのプロビジョン

- ステップ 3: パブリック IPv4 プールからの Elastic IP アドレスの作成
- ステップ 9 の代替方法 クリーンアップ

ステップ 1: パブリック IPv4 プールの作成

このステップは通常、Elastic IP アドレスをプロビジョンしようとする別の AWS アカウントで行います (メンバーアカウントなど)。

> **Important**
>
> パブリック IPv4 プールと IPAM プールは、別個の AWS リソースによって管理されます。パブリック IPv4 プールは、パブリック所有の CIDR を Elastic IP アドレスに変換できるようにする単一のアカウントリソースです。IPAM プールは、パブリック空間をパブリック IPv4 プールに割り当てるために使用できます。

AWS CLI を使用してパブリック IPv4 プールを作成するには

- 以下のコマンドを実行して CIDR をプロビジョニングします。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールを作成したときに入力した `--locale` オプションと `--region` の値が一致する必要があります。

```
aws ec2 create-public-ipv4-pool --region us-west-2 --profile member-account
```

出力に、パブリック IPv4 プール ID が示されます。この ID は次のステップで必要になります。

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

ステップ 2: パブリック IPv4 CIDR のパブリック IPv4 プールへのプロビジョン

パブリック IPv4 CIDR をパブリック IPv4 プールにプロビジョンします。BYOIP CIDR に使用されるプールを作成したときに入力した `--locale` 値と `--region` の値が一致する必要があります。定義できる最も具体的でない `--netmask-length` は 24 です。

このステップは、メンバーアカウントで実行する必要があります。

AWS CLI を使用してパブリック IPv4 プールを作成するには

1. 以下のコマンドを実行して CIDR をプロビジョニングします。

```
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
```

出力に、プロビジョンされた CIDR が示されます。

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. 次のコマンドを実行して、パブリック IPv4 プールにプロビジョンされた CIDR を表示します。

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-
account
```

出力に、プロビジョンされた CIDR が示されます。デフォルトでは、CIDR はアドバタイズされません。つまり、インターネット経由でパブリックにアクセスできません。このチュートリアルの最後のステップで、この CIDR をアドバタイズするように設定できます。

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

ステップ 3: パブリック IPv4 プールからの Elastic IP アドレスの作成

パブリック IPv4 プールから Elastic IP アドレス (EIP) を作成します。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールを作成したときに入力した `--locale` オプションと `--region` の値が一致する必要があります。

このステップは、メンバーアカウントで実行する必要があります。

AWS CLI を使用してパブリック IPv4 プールから EIP を作成する

1. 次のコマンドを実行して、EIP を作成します。

```
aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
ec2-0019eed22a684e0b2 --profile member-account
```

出力に、割り当てが示されます。

```
{
    "PublicIp": "130.137.245.100",
    "AllocationId": "eipalloc-0db3405026756dbf6",
    "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

2. 次のコマンドを実行して、IPAM の EIP 割り当てを表示します。

このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

出力に、IPAM での割り当てが示されます。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
```

```
            "ResourceOwner": "123456789012"
        }
    ]
}
```

ステップ 9 の代替方法 クリーンアップ

ステップ 9 の代替方法を使用して作成されたパブリック IPv4 プールをクリーンアップするには、次のステップを実行します。これらのステップは、ステップ 10: クリーンアップ の標準クリーンアッププロセス中に Elastic IP アドレスを解放した後に実行する必要があります。

1. BYOIP CIDR を表示します。

   このステップは、メンバーアカウントで実行する必要があります。

   ```
   aws ec2 describe-public-ipv4-pools --region us-west-2 --profile member-account
   ```

   出力に、BYOIP CIDR の IP アドレスが示されます。

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
               "Description": "",
               "PoolAddressRanges": [
                   {
                       "FirstAddress": "130.137.245.0",
                       "LastAddress": "130.137.245.255",
                       "AddressCount": 256,
                       "AvailableAddressCount": 256
                   }
               ],
               "TotalAddressCount": 256,
               "TotalAvailableAddressCount": 256,
               "NetworkBorderGroup": "us-east-1",
               "Tags": []
           }
       ]
   }
   ```

2. パブリック IPv4 プールから CIDR を解放します。このセクションのコマンドを実行するときは、`--region` の値が IPAM のリージョンと一致する必要があります。

   このステップは、メンバーアカウントで実行する必要があります。

   ```
   aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.0/24 --profile member-account
   ```

3. BYOIP CIDR を再度表示して、プロビジョンされたアドレスがないことを確認します。このセクションのコマンドを実行するときは、`--region` の値が IPAM のリージョンと一致する必要があります。

   このステップは、メンバーアカウントで実行する必要があります。

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
   ```

   出力に、パブリック IPv4 プール内の IP アドレス数が示されます。

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
               "Description": "",
               "PoolAddressRanges": [],
               "TotalAddressCount": 0,
               "TotalAvailableAddressCount": 0,
               "NetworkBorderGroup": "us-east-1",
               "Tags": []
           }
       ]
   }
   ```

AWS CLI のみを使用した IPAM への IPv6 CIDR の取り込み

IPAM に IPv6 CIDR を取り込み、AWS CLI のみを使用して VPC を割り当てるには、次のステップに従います。

インターネット経由で IPv6 アドレスをアドバタイズする必要がない場合は、プライベート GUA IPv6 アドレスを IPAM にプロビジョニングできます。詳細については、「プライベート IPv6 GUA CIDR のプロビジョニングを有効にする」を参照してください。

Important

- このチュートリアルでは、次のセクションのステップがすでに完了していることを前提としています。
  - IPAM を AWS Organizations 内のアカウントと統合する.
  - IPAM を作成する.
- このチュートリアルの各ステップを、3 つの AWS Organizations アカウントのいずれかで実行する必要があります。
  - 管理アカウント。
  - IPAM を AWS Organizations 内のアカウントと統合する で IPAM 管理者として設定されるメンバーアカウント。このチュートリアルでは、このアカウントを IPAM アカウントと呼びます。
  - IPAM プールから CIDR を割り当てる組織内のメンバーアカウント。このチュートリアルでは、このアカウントをメンバーアカウントと呼びます。

内容

ステップ 1: AWS CLI の名前付きプロファイルと IAM ロールを作成する

このチュートリアルをシングル AWS ユーザーとして完了するには、AWS CLI の名前付きプロファイルを使用して、1 つの IAM ロールから別のアカウントへと切り替えることができます。名前付きプロファイルは、AWS CLI を使用して `--profile` オプションを使用するときに参照する設定と認

証情報の集まりです。AWS アカウントの IAM ロールと指定したプロファイルを作成する方法の詳細については、の「AWS CLI での IAM ロールの使用」を参照してください。

このチュートリアルで使用する 3 つの AWS アカウントごとに、1 つのロールと 1 つの名前付きプロファイルを作成します。

- AWS Organizations 管理アカウント向けの `management-account` と呼ばれるプロファイル。
- IPAM 管理者として設定された AWS Organizations メンバーアカウント向けの、`ipam-account` と呼ばれるプロファイル。
- IPAM プールから CIDR を割り当てる自分の組織の AWS Organizations メンバーアカウント向けの、`member-account` と呼ばれるプロファイル。

IAM ロールと名前付きプロファイルを作成した後、このページに戻り次のステップに進みます。なお、このチュートリアルの残りの部分では、サンプルの AWS CLI コマンドで `--profile` オプションを名前付きプロファイルのうちの 1 つとともに使用することにより、どのアカウントでコマンドを実行する必要があるのかを示しています。

ステップ 2: IPAM を作成する

この手順は省略可能です。`us-east-1` と `us-west-2` の運用リージョンで作成された IPAM が既にある場合は、このステップをスキップできます。IPAM を作成し、`us-east-1` と `us-west-2` の運用リージョンを指定します。運用リージョンを選択する必要があるのは、IPAM プールの作成時に ロケールオプションを使用できるようにするためです。IPAM を BYOIP と統合するには、BYOIP CIDR に使用されるプールに ロケールを設定する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

次のコマンドを実行します。

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

出力に、作成した IPAM が示されます。`PublicDefaultScopeId` の値を書き留めます。パブリックスコープ ID は、次のステップで必要になります。

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

ステップ 3: IPAM プールを作成する

内部に 1 つのリージョンプールが含まれる最上位の IPAM プールを作成し、リージョンプールからリソース (VPC) にスペースを割り当てるため、最上位のプールではなくリージョンプールにロケールを設定します。後のステップでリージョンプールを作成するときに、リージョンプールにロケールを追加します。IPAM を BYOIP と統合するには、BYOIP CIDR に使用されるプールにロケールを設定する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

この IPAM プールの CIDR を、AWS がパブリックインターネット (`--publicly-advertisable` または `--no-publicly-advertisable`) でアドバタイズ可能にするかどうかを選択します。

> **Note**
>
> なお、スコープ ID にはパブリックスコープの ID を、アドレスファミリーには `ipv6` を指定する必要があります。

AWS CLI を使用してすべての AWS リソースの IPv6 アドレスプールを作成するには

1. 次のコマンドを実行して、IPAM プールを作成します。前のステップで作成した IPAM のパブリックスコープの ID を使用します。

```
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
```

出力に、create-in-progress と表示されます。これは、プールの作成が進行中であることを示します。

```
{
    "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. 出力に create-complete という状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

次の出力例は、プールの状態を示しています。

```
{
    "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": []

    }

}
```

ステップ 4: CIDR を最上位プールにプロビジョニングする

最上位プールに CIDR ブロックをプロビジョンします。IPv6 CIDR をトップレベルのプール内にあるプールにプロビジョニングする際、持ち込みできる最も具体的な IPv6 アドレス範囲は、パブリックにアドバタイズ可能な CIDR の場合は /48 であり、パブリックにアドバタイズ可能でない CIDR の場合は /60 であることに注意してください。

> **Note**
>
> - X.509 証明書でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR と BYOIP メッセージおよびそのステップで作成した証明書署名を含める必要があります。
> - DNS TXT レコード でドメインコントロールを検証した場合は、パブリックスペースがユーザーによって制御されていることを確認できるように、CIDR およびそのステップで作成した IPAM 検証トークンを含める必要があります。

BYOIP CIDR を最上位プールにプロビジョンする場合は、ドメインコントロールを検証するだけで済みます。最上位プール内のリージョンプールについては、ドメイン所有者オプションを省略できます。

このステップは、IPAM アカウントで実行する必要があります。

AWS CLI を使用して CIDR ブロックをプールにプロビジョニングするには

1. 証明書情報を使用して CIDR をプロビジョニングするには、次のコマンド例を使用します。この例で必要に応じて値を置き換えるだけでなく、`Message` および `Signature` の値を、X.509 証明書を使用してドメインを検証する で取得した `text_message` および `signed_message` の値に置き換えてください。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-
x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|
20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

検証トークン情報を使用して CIDR をプロビジョニングするには、次のコマンド例を使用します。この例で必要に応じて値を置き換えるだけでなく、ipam-ext-res-ver-token-0309ce7f67a768cf0 を DNS TXT レコードを使用してドメインを検証する で取得した IpamExternalResourceVerificationTokenId トークン ID に置き換えてください。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method
 dns-token --ipam-external-resource-verification-token-id ipam-ext-res-ver-token-0309ce7f67a768cf0 --profile ipam-account
```

出力に、CIDR のプロビジョンが保留されていることが示されます。

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "pending-provision"

    }

}
```

2. 続行する前に、この CIDR のプロビジョンが完了したことを確認してください。

> **Important**
>
> ほとんどのプロビジョニングは 2 時間以内に完了しますが、パブリックにアドバタイズ可能な範囲のプロビジョニングプロセスが完了するまでに最大 1 週間かかる場合があります。

出力に provisioned という状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --profile ipam-account
```

次の出力例に、その状態が示されています。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

ステップ 5: 最上位プール内にリージョンプールを作成する

最上位プール内にリージョンプールを作成します。プールには `--locale` が必須であり、IPAM を作成したときに構成した運用リージョンのいずれかを指定する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

> **Important**
>
> プールを作成するときは、`--aws-service ec2` を含める必要があります。選択したサービスによって、CIDR がアドバタイズ可能になる AWS サービスが決定します。現在、唯一の選択肢は `ec2` であり、このプールから割り当てられた CIDR は、Amazon EC2 サービスと Amazon VPC サービス (VPC に関連付けられている CIDR の場合) に対してアドバタイズできるようになります。

AWS CLI を使用してリージョンプールを作成するには

1. 次のコマンドを実行して、プールを作成します。

```
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
```

出力に、IPAM がプールを作成していることが表示されます。

```
{
    "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. 出力に `create-complete` という状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

出力には、IPAM にあるプールが表示されます。このチュートリアルでは、最上位プールとリージョンプールを作成したので、両方が表示されます。

ステップ 6: リージョンプールに CIDR をプロビジョニングする

リージョンプールに CIDR ブロックをプロビジョンします。CIDR をトップレベルのプール内にあるプールにプロビジョニングする際、持ち込みできる最も具体的な IPv6 アドレス範囲は、パブリックにアドバタイズ可能な CIDR の場合は /48 であり、パブリックにアドバタイズ可能でない CIDR の場合は /60 であることに注意してください。

このステップは、IPAM アカウントで実行する必要があります。

AWS CLI を使用して CIDR ブロックをリージョンプールに割り当てるには

1. 以下のコマンドを実行して CIDR をプロビジョニングします。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

出力に、CIDR のプロビジョンが保留されていることが示されます。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
}
```

2. 出力に、provisioned の状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

次の出力例に、正しい状態が示されています。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

ステップ 7. リージョンプールを共有する

このセクションのステップに従い、AWS Resource Access Manager (RAM) を使用して IPAM プールを共有します。

AWS RAM 内でリソース共有を有効にする

IPAM を作成したら、リージョンプールを組織内の他のアカウントと共有する必要があります。IPAM プールを共有する前に、このセクションのステップを完了し、AWS RAM とのリソース共有を有効にします。AWS CLI を使用してリソース共有を有効にする場合は、`--profile` **`management-account`** オプションを使用します。

リソース共有を有効にするには

1. AWS Organizations 管理アカウントを使って AWS RAM コンソール (https://console.aws.amazon.com/ram/) を開きます。
2. ナビゲーションペインで [設定] を選択し、[AWS Organizations との共有を有効にする] を選択し、[設定の保存] を選択します。

これで、IPAM プールを組織の他のメンバーと共有できるようになりました。

AWS RAM を使用して IPAM プールを共有する

このセクションでは、リージョンプールを他の AWS Organizations メンバーアカウントと共有します。必要な IAM アクセス許可に関する情報を含め、IPAM プールの共有に関する詳細な手順については、「AWS RAM を使用して IPAM プールを共有する」を参照してください。AWS CLI を使用してリソース共有を有効にする場合は、`--profile` **`ipam-account`** オプションを使用します。

AWS RAM を使用して IPAM プールを共有するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択し、IPAM プールを選択して、[アクション] > [詳細を表示] の順に選択します。
4. [Resource sharing] (リソース共有) で [Create resource share] (リソース共有の作成) を選択します。AWS RAM コンソールが開きます。AWS RAM を使用してプールを共有します。
5. [リソースの共有の作成] を選択します。
6. AWS RAM コンソールで、[リソースの共有を作成] を再度選択します。
7. 共有リソースの [名前] を追加します。
8. [リソースタイプを選択] で [IPAM プール] を選択し、次に共有したいプールの ARN を選択します。
9. [次へ] を選択します。
10. AWSRAMPermissionIpamPoolByoipCidrImport 許可を選択します。アクセス許可オプションの詳細は本チュートリアルの対象外ですが、このオプションの詳細は「AWS RAM を使用して IPAM プールを共有する」にてご覧いただけます。
11. [次へ] を選択します。

12. [プリンシパル] > [プリンシパルタイプを選択] で、[AWS アカウント] を選択し、IPAM に IP アドレス範囲を取り込むアカウントのアカウント ID を入力して、[追加] を選択します。
13. [次へ] を選択します。
14. リソース共有オプションと共有先のプリンシパルを確認し、[作成] を選択します。
15. IPAM プールからの IP アドレス CIDR の割り当てを **member-account** アカウントに許可するには、`AWSRAMDefaultPermissionsIpamPool` を使用して 2 つ目のリソース共有を作成します。`--resource-arns` の値は、前のセクションで作成した IPAM プールの ARN です。`--principals` の値は、**member-account** のアカウント ID です。`--permission-arns` の値は、`AWSRAMDefaultPermissionsIpamPool` アクセス許可の ARN です。

ステップ 8: IPv6 CIDR を使用して VPC を作成する

IPAM プール ID を使用して VPC を作成します。`--cidr-block` オプションを使用して IPv4 CIDR ブロックも VPC に関連付ける必要があります。関連付けを行わないとリクエストは失敗します。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるプールを作成したときに入力した `--locale` オプションと `--region` の値が一致する必要があります。

このステップは、メンバーアカウントで実行する必要があります。

AWS CLI を使用して IPv6 の CIDR で VPC を作成する

1. 以下のコマンドを実行して CIDR をプロビジョニングします。

```
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
```

出力には、作成されている VPC が表示されます。

```
{
    "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. IPAM で VPC 割り当てを表示します。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

出力には、IPAM の割り当てが表示されます。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

ステップ 9: CIDR のアドバタイズ

IPAM で CIDR を割り当てた VPC を作成したら、--aws-service ec2 が定義されたプールにある AWS に、取り込まれた CIDR のアドバタイズを開始できます。このチュートリアルでは、これはリージョンプールです。デフォルトでは、CIDR はアドバタイズされません。つまり、インターネット経由でパブリックにアクセスできません。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるリージョンプールを作成したときに入力した --locale オプションと --region の値が一致する必要があります。

このステップは、IPAM アカウントで実行する必要があります。

AWS CLI を使用して CIDR のアドバタイズを開始するには

- 次のコマンドを実行して、CIDR をアドバタイズします。

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

出力に、CIDR がアドバタイズされたことが示されます。

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "advertised"
    }
}
```

ステップ 10: クリーンアップ

このセクションのステップに従って、このチュートリアルでプロビジョンし、作成したリソースをクリーンアップします。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるリージョンプールを作成したときに入力した --locale オプションと --region の値が一致する必要があります。

AWS CLI を使用したクリーンアップ

1. 次のコマンドを実行して、IPAM の VPC 割り当てを表示します。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

出力に、IPAM での割り当てが示されます。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

2. 次のコマンドを実行して、CIDR のアドバタイズを停止します。このステップのコマンドを実行するときは、BYOIP CIDR に使用されるリージョンプールを作成したときに入力した `--locale` オプションと `--region` の値が一致する必要があります。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

   出力に、CIDR の状態が advertised から provisioned に変更されていることが示されます。

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "provisioned"
    }
}
```

3. 次のコマンドを実行して、VPC を削除します。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるリージョンプールを作成したときに入力した `--locale` オプションと `--region` の値が一致する必要があります。

このステップは、メンバーアカウントで実行する必要があります。

```
aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
profile member-account
```

このコマンドの実行では出力は表示されません。

4. 次のコマンドを実行して、IPAM の VPC 割り当てを表示します。IPAM が、VPC が削除されたことを検出してこの割り当てを削除するまでには、少し時間がかかることがあります。このセクションのコマンドを実行するときは、BYOIP CIDR に使用されるリージョンプールを作成したときに入力した `--locale` オプションと `--region` の値が一致する必要があります。

   このステップは、IPAM アカウントで実行する必要があります。

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   出力に、IPAM での割り当てが示されます。

   ```
   {
      "IpamPoolAllocations": [

           {

               "Cidr": "2605:9cc0:409::/56",

               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
               "ResourceId": "vpc-00b5573ffc3b31a29",

               "ResourceType": "vpc",

               "ResourceOwner": "123456789012"

           }

       ]

   }
   ```

コマンドを再実行し、削除する割り当てを探します。割り当てが IPAM から削除されたことが表示されるまでは、IPAM プール CIDR のクリーンアップとプロビジョン解除を続行できません。

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

出力に、IPAM から削除された割り当てが表示されます。

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

5. RAM 共有を削除し、AWS Organizations との RAM 統合を無効にします。「AWS RAM ユーザーガイド」内にある「AWS RAM のリソース共有を削除」と「AWS Organizations とのリソース共有を無効化」に記載されているステップをこの順序で行い、RAM 共有を削除して、AWS Organizations との RAM 統合を無効にします。

   このステップは、IPAM アカウントと管理アカウントのそれぞれで実行する必要があります。AWS CLI を使用して RAM 共有を削除し、RAM 統合を無効にする場合は、 `--profile ipam-account` および `--profile management-account` オプションを使用します。

6. 次のコマンドを実行して、リージョンプール CIDR のプロビジョンを解除します。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

出力に、CIDR のプロビジョン解除が保留されていることが示されます。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

プロビジョン解除の完了には、しばらく時間がかかります。CIDR の状態が deprovisioned と表示されるまで、コマンドを実行し続けます。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

出力に、CIDR のプロビジョン解除が保留されていることが示されます。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "deprovisioned"
    }
}
```

7. 次のコマンドを実行して、リージョンプールを削除します。

このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

出力に、削除状態が表示されます。

```
{
    "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. 次のコマンドを実行して、最上位プール CIDR のプロビジョンを解除します。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   出力に、CIDR のプロビジョン解除が保留されていることが示されます。

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   プロビジョン解除の完了には、しばらく時間がかかります。次のコマンドを実行して、プロビジョン解除のステータスを確認します。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

   [deprovisioned] (プロビジョン解除済) が表示されるまで待ってから、次のステップに進みます。

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. 次のコマンドを実行して、最上位プールを削除します。

   このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

出力に、削除状態が表示されます。

```
{
    "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. 次のコマンドを実行して、IPAM を削除します。

    このステップは、IPAM アカウントで実行する必要があります。

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

出力に、IPAM 応答が示されます。これは、IPAM が削除されたことを示します。

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

IPAM を使用して独自の IP を CloudFront に持ち込む

グローバルサービス用の IPAM の BYOIP を使用すると、CloudFront などの AWS グローバルサービスで独自の IPv4 アドレスを使用できます。リージョン BYOIP とは異なり、IP アドレスはエニーキャストルーティングを通じて複数のエッジロケーションから同時にアドバタイズされます。

この機能を使用する理由

- IP 許可リストの維持 – ファイアウォール設定を更新する代わりに、既存の承認済み IP アドレスを使用します。
- 移行の簡素化 – IP インフラストラクチャを変更せずに他の CDN から移行します
- 一貫したブランディング – AWS に移行するときは既存の IP アドレス空間を維持します

この機能を使用すべきユーザー

グローバルコンテンツ配信で独自の IP アドレスを必要とする組織:

- IP 許可リストの要件を持つ大規模なエンタープライズ
- 既存の IP アドレスを保持したまま、他の CDN から移行する企業
- 特定の IP 範囲を必要とする厳格なセキュリティポリシーを持つ組織

この機能を使用するタイミング

以下の場合は、グローバルサービスに BYOIP を使用します。

- パートナー/クライアントとの既存の IP 許可リストを維持する必要がある場合
- IP アドレスを使用して別の CDN から移行する場合
- 特定の IP 範囲のコンプライアンス要件を満たす必要がある場合

> **Note**
>
> /24 IPv4 CIDR ブロックが必要です。現在、CloudFront でのみ使用できます。

前提条件

開始する前に、次のステップを完了します。

- IPAM のセットアップ – IPAM を AWS Organizations 内のアカウントと統合する および IPAM を作成する
- ドメインの検証 – ドメインコントロールの検証
- 最上位プールを作成する – 「独自の IPv4 CIDR を IPAM に持ち込む」のステップ 1～2 に従います

グローバルサービス設定ステップ

次の手順は、標準のリージョン BYOIP プロセスとは異なり、グローバルサービスのパターンを確立します。

ステップ 1: エニーキャストサービスのグローバルプールを作成する

リージョンプールを作成する代わりに、エニーキャストサービスのグローバルプールを作成します。

コンソール

コンソールを使用してグローバルプールを作成するには:

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します

3. [プールを作成] を選択します
4. [ソース]: 最上位の BYOIP プールを選択します
5. [ロケール]: [グローバル] を選択します
6. [サービス]: [グローバルサービス] を選択します ([グローバル] が選択されている場合に表示されます)
7. [パブリック IP ソース]: [BYOIP] を選択します
8. [プロビジョニングする CIDR]: /24 CIDR 範囲を指定します
9. [プールを作成] を選択します

CLI

ロケールを [グローバル] に、アドレスファミリーを [ipv4] にそれぞれ設定して、`aws ec2 create-ipam-pool` を使用します。

次に、`aws ec2 provision-ipam-pool-cidr` を使用して CIDR をプロビジョニングします。

> **Important**
>
> このプールには完全な /24 ブロックを割り当てる必要があります。さまざまな用途に合わせて、このブロック内でより具体的な範囲をプロビジョニングできます。

ステップ 2: サービス固有のリソースを作成する

CloudFront の場合は、IPAM プールを使用するエニーキャスト IP リストを作成します。詳細な手順については、CloudFront BYOIP ドキュメント (リンクは後日追加予定) を参照してください。

IPAM 統合の主要なパラメータ:

- IP アドレスタイプ – [BYOIP] を選択します
- IPAM プール – ステップ 1 のグローバルプールを選択します
- IP 数 – 3 を入力します (CloudFront に必要)

ステップ 3: サービスリソースに関連付ける

エニーキャスト静的 IP リストを CloudFront ディストリビューションに関連付けます。詳細な手順については、CloudFront BYOIP ドキュメント (リンクは後日追加予定) を参照してください。

設定キー:

- ディストリビューション設定で、ステップ 2 のエニーキャスト IP リストを選択します

ステップ 4: 移行の準備をする

- DNS TTL を下げる – レコードの DNS TTL を 60 秒以下に設定します
- 伝播を待つ – 新しい TTL がインターネット全体に反映されるまで待ちます

ステップ 5: CIDR をグローバルにアドバタイズする

IPAM グローバルアドバタイズコマンドを使用します。

コンソール

コンソールを使用して CIDR をアドバタイズするには:

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します
3. グローバルプールを選択します
4. [CIDR] タブを選択します
5. CIDR を選択し、[アクション] > [CIDR をアドバタイズ] を選択します
6. アドバタイズを確認します

CLI

IPAM プール ID と CIDR で `aws ec2 advertise-ipam-byoip-cidr` を使用します。

> **Important**
>
> - このコマンドを実行する前に、以前のプロバイダーからアドバタイズを取り消します
> - CloudFront を参照するように DNS レコードを更新して移行を完了します

クリーンアップ

このチュートリアルで作成したリソースをクリーンアップするには:

- CloudFront リソースの削除 – CloudFront BYOIP ドキュメント (リンクは後日追加予定) のクリーンアップ手順に従います
- CIDR の取り消しと IPAM プールの削除 — ステップ 8: クリーンアップ の標準クリーンアッププロセスに従います

> **Important**
>
> サービスの中断を避けるために、まず CloudFront リソースを削除してから、IPAM クリーンアップに進みます。

チュートリアル: BYOIP IPv4 CIDR を IPAM に転送する

既存の IPv4 CIDR を IPAM に転送するには、次のステップに従います。AWS を使用した IPv4 BYOIP CIDR を既に使用している場合は、CIDR をパブリック IPv4 プールから IPAM に移動できます。IPv6 CIDR を IPAM に移動することはできません。

このチュートリアルでは、「Amazon EC2 で自分の IP アドレスを使用する (BYOIP)」で説明されているプロセスを使用して IP アドレス範囲を既に AWS に正常に移行済みで、その IP アドレス範囲を IPAM に転送することを前提としています。新しい IP アドレスを初めて AWS に持ち込む場合、チュートリアル: IP アドレスを IPAM に移行する の手順を完了してください。

パブリック IPv4 プールを IPAM に転送しても、既存の割り当てには影響しません。パブリック IPv4 プールを IPAM に転送すると、リソースタイプによっては、既存の割り当てをモニタリングできる場合があります。詳細については、「リソースごとに CIDR の使用状況をモニタリングする」を参照してください。

> **Note**
>
> - このチュートリアルでは、IPAM を作成する のステップが完了していることを前提としています。
> - このチュートリアルの各ステップを、2 つの AWS アカウントのいずれかで実行する必要があります。
>   - IPAM 管理者用のアカウント。このチュートリアルでは、このアカウントを IPAM アカウントと呼びます。

- BYOIP CIDR を所有する組織内のアカウント。このチュートリアルでは、このアカウントを BYOIP CIDR 所有者アカウントと呼びます。

内容

ステップ 1: AWS CLI の名前付きプロファイルと IAM ロールを作成する

このチュートリアルをシングル AWS ユーザーとして完了するには、AWS CLI の名前付きプロファイルを使用して、1 つの IAM ロールから別のアカウントへと切り替えることができます。名前付きプロファイルは、AWS CLI を使用して `--profile` オプションを使用するときに参照する設定と認証情報の集まりです。AWS アカウントの IAM ロールと指定したプロファイルを作成する方法の詳細については、の「AWS CLI での IAM ロールの使用」を参照してください。

このチュートリアルで使用する 3 つの AWS アカウントごとに、1 つのロールと 1 つの名前付きプロファイルを作成します。

- IPAM 管理者である AWS アカウント向けの `ipam-account` と呼ばれるプロファイル。
- BYOIP CIDR を所有する組織内の AWS アカウント向けの `byoip-owner-account` と呼ばれるプロファイル。

IAM ロールと名前付きプロファイルを作成した後、このページに戻り次のステップに進みます。なお、このチュートリアルの残りの部分では、サンプルの AWS CLI コマンドで `--profile` オプションを名前付きプロファイルのうちの 1 つとともに使用することにより、どのアカウントでコマンドを実行する必要があるのかを示しています。

ステップ 2: IPAM のパブリックスコープ ID を取得する

IPAM のパブリックスコープ ID を取得するには、このセクションのステップに従います。このステップは、**ipam-account** アカウントで実行する必要があります。

次のコマンドを実行して、パブリックスコープ ID を取得します。

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

出力に、パブリックスコープ ID が表示されます。PublicDefaultScopeId の値を書き留めます。これは次のステップで必要になります。

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

ステップ 3: IPAM プールを作成する

IPAM プールを編集するには、このセクションのステップに従います。このステップは、**ipam-account** アカウントで実行する必要があります。作成する IPAM プールは、BYOIP CIDR AWS リージョンに一致した --locale オプションを持つ最上位プールである必要があります。BYOIP は、最上位の IPAM プールにのみ転送できます。

> **Important**
>
> プールを作成するときは、`--aws-service ec2` を含める必要があります。選択したサービスによって、CIDR がアドバタイズ可能になる AWS サービスが決定します。現在、唯一の選択肢は `ec2` であり、このプールから割り当てられた CIDR は、Amazon EC2 サービス (Elastic IP アドレスの場合) と Amazon VPC サービス (VPC に関連付けられている CIDR の場合) に対してアドバタイズできるようになります。

AWS CLI を使用して、転送された BYOIP CIDR の IPv4 アドレスプールを作成するには

1. 次のコマンドを実行して、IPAM プールを作成します。前のステップで作成した IPAM の Public スコープの ID を使用します。

```
aws ec2 create-ipam-pool --region us-east-1 --profile ipam-account --ipam-scope-
id ipam-scope-0087d83896280b594 --description "top-level-pool" --locale us-west-2
 --aws-service ec2 --address-family ipv4
```

出力に、`create-in-progress` と表示されます。これは、プールの作成が進行中であることを示します。

```
{
    "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. 出力に create-complete という状態が表示されるまで、次のコマンドを実行します。

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

次の出力例は、プールの状態を示しています。次のステップでは OwnerId が必要になります。

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

ステップ 4: AWS RAM を使用して IPAM プールを共有する

このセクションのステップに従って、別の AWS アカウントが既存の BYOIP IPV4 CIDR を IPAM プールに転送し、その IPAM プールを使用できるように、AWS RAM を使用して IPAM プールを共有します。このステップは、**ipam-account** アカウントで実行する必要があります。

AWS CLI を使用して IPv4 アドレスプールを共有するには

1. IPAM プールで使用可能な AWS RAM アクセス許可を表示します。このセクションのステップを実行するには両方の ARN が必要です。

```
aws ram list-permissions --region us-east-1 --profile ipam-account --resource-type
 ec2:IpamPool
```

```
{
    "permissions": [
        {
           "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool",
           "version": "1",
           "defaultVersion": true,
           "name": "AWSRAMDefaultPermissionsIpamPool",
           "resourceType": "ec2:IpamPool",
           "status": "ATTACHABLE",
           "creationTime": "2022-06-30T13:04:29.335000-07:00",
           "lastUpdatedTime": "2022-06-30T13:04:29.335000-07:00",
           "isResourceTypeDefault": true
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionIpamPoolByoipCidrImport",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMPermissionIpamPoolByoipCidrImport",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:55.032000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:55.032000-07:00",
            "isResourceTypeDefault": false
        }
    ]
}
```

2. リソース共有を作成し、**byoip-owner-account** アカウントが BYOIP CIDR を IPAM にインポートできるようにします。--resource-arns の値は、前のセクションで作成した IPAM プールの ARN です。--principals の値は、BYOIP IP CIDR の所有者アカウントの、アカウント ID です。--permission-arns の値は、AWSRAMPermissionIpamPoolByoipCidrImport アクセス許可の ARN です。

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare2 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
```

```
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMPermissionIpamPoolByoipCidrImport
```

```
{

    "resourceShare": {

        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7993758c-a4ea-43ad-be12-b3abaffe361a",
        "name": "PoolShare2",

        "owningAccountId": "123456789012",

        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:32:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:32:25.536000-07:00"

        }

}
```

3. (オプション) 転送の完了後に、IP アドレスの CIDR を IPAM プールからパブリック IPv4 プールへ割り当てることを **byoip-owner-account** アカウントに許可するには、AWSRAMDefaultPermissionsIpamPool の ARN をコピーして 2 つ目のリソース共有を作成します。--resource-arns の値は、前のセクションで作成した IPAM プールの ARN です。--principals の値は、BYOIP IP CIDR の所有者アカウントの、アカウント ID です。--permission-arns の値は、AWSRAMDefaultPermissionsIpamPool アクセス許可の ARN です。

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare1 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool
```

```
{
```

```
    "resourceShare": {

        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f",
        "name": "PoolShare1",

        "owningAccountId": "123456789012",

        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:31:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:31:25.536000-07:00"

        }

}
```

RAM でリソース共有を作成した結果、byoip-owner-account アカウントは、CIDR を IPAM へ移動できるようになりました。

ステップ 5: 既存の BYOIP IPV4 CIDR を IPAM に転送する

既存の BYOIP IPV4 CIDR を IPAM に転送するには、このセクションのステップに従います。このステップは、**byoip-owner-account** アカウントで実行する必要があります。

> **Important**
>
> IPv4 アドレス範囲を AWS に設定すると、最初のアドレス (ネットワークアドレス) と最後のアドレス (ブロードキャストアドレス) を含む、その範囲内のすべての IP アドレスを使用できます。

BYOIP CIDR を IPAM に転送するには、BYOIP CIDR 所有者が IAM ポリシーで次の許可を得ている必要があります。

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> この手順には、AWS マネジメントコンソール または AWS CLI を使用できます。

AWS Management Console

BYOIP CIDR を IPAM プールに転送するには:

1. **byoip-owner-account** アカウントで IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. このチュートリアルで作成して共有した最上位プールを選択してください
4. [アクション] > [BYOIP CIDR の転送] を選択します。
5. [BYOIP CIDR の転送]を選択します。
6. BYOIP CIDR を選択してください。
7. [プロビジョニング] を選択します。

Command line

次の AWS CLI コマンドを実行すると、AWS CLI を使用して BYOIP CIDR を IPAM プールに転送します。

1. 次のコマンドを実行して、CIDR を転送します。`--region` 値が BYOIP CIDR の AWS リージョンであることを確認します。

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

出力に、CIDR のプロビジョンが保留されていることが示されます。

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",
```

```
        "State": "pending-transfer"

    }

}
```

2. CIDR が転送されていることを確認します。出力に、complete-transfer の状態が表示されるまで、次のコマンドを実行します。

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

次の出力例に、その状態が示されています。

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

ステップ 6: IPAM の CIDR を表示する

IPAM の CIDR を表示するには、このセクションのステップに従います。このステップは、**ipam-account** アカウントで実行する必要があります。

AWS CLI を使用して IPAM プール内の転送された BYOIP CIDR を表示するには

- 次のコマンドを実行して、IPAM で管理されている割り当てを表示します。--region 値が BYOIP CIDR の AWS リージョンであることを確認します。

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

出力に、IPAM での割り当てが示されます。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

ステップ 7: クリーンアップ

このチュートリアルで作成したリソースを削除するには、このセクションのステップに従います。このステップは、**ipam-account** アカウントで実行する必要があります。

AWS CLI を使用してこのチュートリアルで作成したリソースをクリーンアップするには

1. IPAM プールの共有されたリソースを削除するには、次のコマンドを実行して最初のリソース共有 ARN を取得します。

```
aws ram get-resource-shares --region us-east-1 --profile ipam-account --
name PoolShare1 --resource-owner SELF
```

```
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f",
            "name": "PoolShare1",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2023-04-28T07:31:25.536000-07:00",
            "lastUpdatedTime": "2023-04-28T07:31:25.536000-07:00",
            "featureSet": "STANDARD"
        }
    ]
```

```
}
```

2. リソース共有 ARN をコピーし、それを使用して IPAM プールリソース共有を削除します。

```
aws ram delete-resource-share --region us-east-1 --profile ipam-account
 --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f
```

```
{
    "returnValue": true
}
```

3. 「ステップ 4: AWS RAM を使用して IPAM プールを共有する」で追加のリソース共有を作成した場合は、上記 2 つのステップを繰り返し、PoolShare2 の 2 番目のリソース共有 ARN を取得して、2 番目のリソース共有を削除します。

4. 次のコマンドを実行して、BYOIP CIDR の割り当て ID を取得します。--region 値が BYOIP CIDR の AWS リージョンと一致していることを確認します。

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

出力に、IPAM での割り当てが示されます。

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

5. パブリック IPv4 プールから CIDR を解放します。このセクションのコマンドを実行するときは、--region の値が IPAM のリージョンと一致する必要があります。

このステップは、**byoip-owner-account** アカウントで実行する必要があります。

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1  --profile byoip-
owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.0/24
```

6. BYOIP CIDR を再度表示して、プロビジョンされたアドレスがないことを確認します。このセクションのコマンドを実行するときは、--region の値が IPAM のリージョンと一致する必要があります。

   このステップは、**byoip-owner-account** アカウントで実行する必要があります。

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
```

   出力に、パブリック IPv4 プール内の IP アドレス数が示されます。

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

7. 次のコマンドを実行して、最上位プールを削除します。

```
aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
id ipam-pool-0a03d430ca3f5c035
```

   出力に、削除状態が表示されます。

```
{
    "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"
    }
}
```

チュートリアル: サブネット IP 割り当て用の VPC IP アドレス空間を計画する

このチュートリアルを完了して、VPC サブネットに IP アドレスを割り当てるための VPC IP アドレス空間を計画し、サブネットと VPC レベルで IP アドレス関連のメトリクスを監視します。

> **Note**
>
> このチュートリアルでは、プライベート IP アドレス範囲内のプライベート IPv4 アドレス空間を VPC とサブネットに割り当てる方法について説明します。VPC コンソールで Amazon 提供の IPv6 CIDR ブロックオプションにより VPC を作成することで、IPv6 CIDR 範囲を使用してこのチュートリアルを完了することもできます。

サブネットの VPC IP アドレス空間を計画すると、次のことが可能になります。

- サブネットに割り当てる VPC の IP アドレスを計画して整理する: VPC の IP アドレス空間を小さな CIDR ブロックに分割し、それらの CIDR ブロックを、開発サブネットまたは本番サブネットでワークロードを実行する場合など、ビジネスニーズの異なるサブネットにプロビジョニングできます。
- VPC サブネットの IP アドレス割り当てを簡素化する: VPC のアドレス空間を計画して整理すると、CIDR を手動で入力することなくネットマスク長を選択できます。例えば、デベロッパーが開

発ワークロードをホストするサブネットを作成する場合、サブネットのプールとネットマスク長を選択する必要があります。IPAM は自動的に CIDR ブロックをサブネットに割り当てます。

次の例は、このチュートリアルで作成するプールとリソース構造の階層を示しています。

- プライベートスコープ
  - リソース計画プール (10.0.0.0/20)
    - 開発サブネットプール (10.0.0.0/24)
      - 開発サブネット (10.0.0.0/28)
    - プロダクトサブネットプール (10.0.1/24)
      - プロダクトサブネット (10.0.0.16/28)

> **Important**
>
> - リソース計画プールは、CIDR をサブネットに割り当てるために使用することも、他のプールを作成するためのソースプールとして使用することもできます。このチュートリアルでは、リソース計画プールをサブネットプールのソースプールとして使用します。
> - VPC に複数の CIDR がプロビジョニングされている場合は、同じ VPC を使用して複数のリソース計画プールを作成できます。例えば、VPC に 2 つの CIDR が割り当てられている場合、各 CIDR から 1 つずつ、合計 2 つのリソース計画プールを作成できます。各 CIDR は、一度に 1 つのプールに割り当てることができます。

ステップ 1: VPC を作成する

このセクションのステップに従って、サブネット IP アドレス計画に使用する VPC を作成します。VPC の作成に必要な IAM アクセス許可の詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC ポリシーの例」を参照してください。

> **Note**
>
> 新しい VPC を作成する代わりに既存の VPC を使用することもできますが、このチュートリアルでは、IPAM によって自動的に割り当てられた CIDR ブロックではなく、手動で割り当てられた CIDR ブロックで VPC を構成するシナリオに焦点を当てます。

VPC を作成するには

1. IPAM の管理者アカウントを使用して VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. [Create VPC (VPC の作成)] を選択します。
3. VPC の名前を入力します。例えば、「tutorial-vpc」などです。
4. [IPv4 CIDR 手動入力] を選択し、IPv4 CIDR ブロックを入力します。このチュートリアルでは、「10.0.0.0/20」を使用します。
5. IPv6 CIDR ブロックを追加するオプションをスキップします。
6. [Create VPC (VPC の作成)] を選択します。
7. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
8. 左側のナビゲーションペインで [リソース] を選択します。
9. 作成した VPC が表示されるまで待ちます。この処理にはしばらく時間がかかり、表示されるまでウィンドウを更新する必要がある場合があります。次のステップに進む前に、VPC を IPAM で検出する必要があります。

ステップ 2: リソース計画プールを作成する

このセクションのステップに従って、リソース計画プールを作成します。

リソース計画プールを作成するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択します。
4. [プールを作成] を選択します。
5. [IPAM スコープ] では、プライベートスコープを選択したままにします。
6. (オプション)「Resource-planning-pool」のように、プールの [名前タグ] を追加します。
7. [ソース] で [IPAM スコープ]を選択します。
8. [リソース計画] で [VPC 内の IP スペースを計画] を選択し、前のステップで作成した VPC を選択します。VPC は、リソース計画プールに CIDR をプロビジョニングするために使用されるリソースです。

9. [プロビジョニングする CIDR] で、リソースプールにプロビジョニングする VPC CIDR を選択します。リソース計画プールにプロビジョニングする CIDR は、VPC にプロビジョニングされた CIDR と一致する必要があります。このチュートリアルでは、「10.0.0.0/20」を使用します。
10. [プールを作成] を選択します。
11. プールが作成されたら、[CIDR] タブを選択して、プロビジョニングされた CIDR の状態を確認します。ページを更新し、CIDR の状態が「プロビジョニング待ち」から「プロビジョニング済み」に変わるのを待ってから、次のステップに進みます。

ステップ 3: サブネットプールを作成する

このセクションのステップを完了して、サブネットに IP スペースを割り当てるのに使用する 2 つのサブネットプールを作成します。

サブネットプールを作成するには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択します。
4. [プールを作成] を選択します。
5. [IPAM スコープ] では、プライベートスコープを選択したままにします。
6. (オプション)「dev-subnet-pool」のように、プールの [名前タグ] を追加します。
7. [ソース] で [IPAM pool] を選択し、ステップ 3 で作成したリソース計画プールを選択します。アドレスファミリ、リソース計画設定、およびロケールは、ソースプールから自動的に継承されます。
8. [プロビジョニングする CIDR] で、サブネットプールにプロビジョニングする CIDR を選択します。このチュートリアルでは、「10.0.0.0/24」を使用します。
9. [プールを作成] を選択します。
10. プールが作成されたら、[CIDR] タブを選択して、プロビジョニングされた CIDR の状態を確認します。ページを更新し、CIDR の状態が「プロビジョニング待ち」から「プロビジョニング済み」に変わるのを待ってから、次のステップに進みます。
11. このプロセスを繰り返して、「prod-subnet-pool」というサブネットをもう 1 つ作成します。

この時点で、このサブネットプールを他の AWS アカウントが使用できるようにしたい場合は、サブネットプールを共有できます。これを行う方法については、「AWS RAM を使用して IPAM プールを共有する」を参照してください。その後、ここに戻ってチュートリアルを完了させます。

ステップ 4: サブネットを作成する

以下のステップを実行して、2 つのサブネットを作成します。

サブネットを作成するには

1. 適切なアカウントを使用して [https://console.aws.amazon.com/vpc/] で VPC コンソールを開きます。
2. [サブネット]、[サブネットの作成] の順に選択します。
3. このチュートリアル開始時に作成した VPC を選択します。
4. 「tutorial-subnet」のように、サブネットの名前を入力します。
5. (オプション)[アベイラビリティーゾーン] を選択します。
6. [IPv4 CIDR ブロック]で、[IPAM が割り当てる IPV4 CIDR ブロック]を選択し、開発サブネットプールと/28 ネットマスクを選択します。
7. [サブネットの作成] を選択します。
8. このプロセスを繰り返して、サブネットをもう 1 つ作成します。今回は prod サブネットプールと/28 ネットマスクを選択します。
9. IPAM コンソールに戻り、左側のナビゲーションペインで [リソース] を選択します。
10. 作成したサブネットプールを探し、作成したサブネットがその下に表示されるのを待ちます。この処理にはしばらく時間がかかり、表示されるまでウィンドウを更新する必要がある場合があります。

これでチュートリアルは完了です。必要に応じて追加のサブネットプールを作成することも、EC2 インスタンスをサブネットの 1 つに起動することもできます。

IPAM は、サブネット内の IP アドレスの使用状況に関するメトリクスを公開します。SubnetIPUsage メトリクスに CloudWatch アラームを設定して、IP 使用率のしきい値を超えた場合に対処できます。例えば、サブネットに/24 CIDR (256 の IP アドレス) が割り当てられていて、IP の 80% が使用されたら通知を受け取りたい場合は、CloudWatch アラームを設定して、このしきい値に達したときにアラートを受け取ることができます。サブネット IP の使用状況に関するアラームの作成方法の詳細については、「アラーム作成のクイックヒント」を参照してください。

ステップ 5: クリーンアップ

このチュートリアルで作成したリソースを削除するには、次の手順を実行します。

リソースをクリーンアップするには

1. IPAM の管理者アカウントを使って IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プライベートスコープを選択します。
4. リソース計画プールを選択し、[アクション]、[削除] の順に選択します。
5. [カスケード削除] を選択します。リソース計画プールとサブネットプールは削除されます。これによってサブネット自体は削除されません。CIDR は IPAM プールからのものではなくなりますが、プロビジョニングされた CIDR はそのまま残ります。
6. [削除] を選択します。
7. サブネットを削除します。
8. VPC を削除します。

これで、クリーンアップは完了です。

IPAM プールからシーケンシャル Elastic IP アドレスを割り当てる

IPAM を使用すると、Amazon 所有のパブリック IPv4 ブロックを IPAM プールにプロビジョニングし、それらのプールから AWS リソースにシーケンシャル Elastic IP アドレスを割り当てることができます。

連続して割り当てられた Elastic IP アドレスは、順次割り当てられたパブリック IPv4 アドレスです。例えば、Amazon が `192.0.2.0/30` のパブリック IPv4 CIDR ブロックを提供し、ユーザーがその CIDR ブロックから使用可能な 4 つのパブリック IPv4 アドレスを割り当てる場合、4 つのシーケンシャル Elastic IP アドレスの例は、`192.0.2.0`、`192.0.2.1`、`192.0.2.2`、`192.0.2.3` です。

連続して割り当てられた Elastic IP アドレスを使用すると、次の方法でセキュリティルールとネットワークルールを簡素化できます。

- セキュリティ管理: シーケンシャル IPv4 アドレスを使用すると、ファイアウォール管理のオーバーヘッドが軽減されます。単一のルールでプレフィックス全体を追加し、スケールする際に同じプレフィックスから IP を関連付けることで、時間と労力を節約できます。

- エンタープライズアクセス: 多数の個別のパブリック IPv4 アドレスの代わりに CIDR ブロック全体を使用することで、クライアントと共有されるアドレス空間を簡素化できます。これにより、アプリケーションが AWS でスケールする際に IP の変更を常に伝達する必要がなくなります。
- IP 管理の簡素化: シーケンシャル IPv4 アドレスを使用すると、中心的なネットワークチームのパブリック IP 管理が簡素化されます。これは、個別のパブリック IP を追跡する必要性が軽減され、代わりに限られた数の IP プレフィックスに注力できるためです。

このチュートリアルでは、IPAM プールからシーケンシャル Elastic IP アドレスを割り当てるために必要なステップについて説明します。Amazon 提供の連続したパブリック IPv4 CIDR ブロックを使用して IPAM プールを作成し、プールから Elastic IP アドレスを割り当て、IPAM プールの割り当てをモニタリングする方法について説明します。

> **Note**
>
> - Amazon 所有のパブリック IPv4 CIDR ブロックのプロビジョニングには料金がかかります。詳細については、Amazon VPC の料金ページの「Amazon 提供の連続した IPv4 ブロック」のタブを参照してください。
> - このチュートリアルは、ユーザーが IPAM を 1 つのアカウントで使用する IPAM の作成を希望していることを前提としています。Amazon 所有の連続したパブリック IPv4 ブロックを複数のアカウントで共有する場合は、まず IPAM を AWS Organizations 内のアカウントと統合する し、次に AWS RAM を使用して IPAM プールを共有する します。AWS Organizations と統合する場合、プールに割り当てられた連続 IPv4 ブロックのプロビジョニングが解除されないようにするためのサービスコントロールポリシーを作成するオプションがあります。
> - IPAM プールから割り当てられたシーケンシャル Elastic IP アドレスを、他の AWS アカウントに転送することはできません。代わりに、IPAM では、IPAM を AWS Organizations と統合することで、複数の AWS アカウント間で IPAM プールを共有できます (上記を参照)。
> - プロビジョニングできる Amazon 所有のパブリック IPv4 CIDR ブロックの数とそのサイズには制限があります。詳細については、「IPAM のクォータ」を参照してください。

内容

ステップ 1: IPAM を作成する

このセクションのステップを実行して IPAM プールを作成します。

AWS Management Console

IPAM を作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. AWS マネジメントコンソールで、IPAM を作成する AWS リージョンを選択します。オペレーションの主要リージョンに IPAM を作成します。
3. サービスホームページで [IPAM の作成] を選択します。
4. [Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account] (Amazon VPC IP Address Manager がソースアカウントから IPAM 委任アカウントにデータをレプリケートするのを許可する) を選択します。このオプションを選択しないと、IPAM を作成できません。
5. IPAM 階層を選択します。各利用枠で利用できる機能と利用枠に関連するコストの詳細については、「Amazon VPC の料金」で [IPAM] タブを参照してください。
6. [運用リージョン] で、この IPAM がリソースを管理および検出できる AWS リージョンを選択します。IPAM を作成している AWS リージョンは、デフォルトで運用リージョンの 1 つとして選択されています。たとえば、この IPAM を AWS リージョン `us-east-1` で作成しているが、`us-west-2` の VPC に CIDR を提供するリージョン IPAM プールを後で作成したい場合は、ここで `us-west-2` を選択します。運用リージョンを忘れた場合は、後で戻って IPAM の設定を編集できます。

> **Note**
>
> 無料利用枠で IP アドレス管理を作成する場合、IP アドレス管理用に複数の運用地域を選択できますが、運用リージョン全体で利用できる IP アドレス管理機能はPublic IP Insightsだけです。無料利用枠の他の機能 (BYOIP など) を IP アドレス管理の対象リージョン全体で使用することはできません。IPAM のホームリージョンを通じての

み使用できます。運用リージョン全体ですべての IP アドレス管理機能を使用するには、アドバンスト枠で [IP アドレス管理] を作成してください。

7. [Create IPAM] (IPAM を作成) を選択します。

Command line

このセクションのコマンドは、AWS CLI リファレンスドキュメントにリンクされています。ドキュメントには、コマンドの実行時に使用できるオプションの詳しい説明が記載されています。

create-ipam コマンドを使用して IPAM を作成します。

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

レスポンスの例:

```
{
    "Ipam": {
        "OwnerId": "320805250157",
        "IpamId": "ipam-0755477df834ea06b",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-01bc7290e4a9202f9",
        "PrivateDefaultScopeId": "ipam-scope-0a50983b97a7a583a",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "State": "create-in-progress",
        "Tags": [],
        "DefaultResourceDiscoveryId": "ipam-res-disco-02cc5b34cc3f04f09",
        "DefaultResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-06b3a4dccfc81f7c1",
        "ResourceDiscoveryAssociationCount": 1,
        "Tier": "advanced"
    }
}
```

PublicDefaultScopeId は次のステップで必要になります。スコープの詳細については、IPAM の仕組みを参照してください。

ステップ 2: IPAM プールを作成して CIDR をプロビジョニングする

Elastic IP アドレスの割り当て元とする IPAM プールを作成するには、このセクションのステップを実行します。

AWS Management Console

プールを作成するには

1. IPAM コンソール (https://console.aws.amazon.com/ipam/) を開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. パブリックスコープを選択します。スコープの詳細については、「IPAM の仕組み」を参照してください。
4. [プールを作成] を選択します。
5. (オプション) プールの [名前タグ] とプールの [説明] を追加します。
6. [ソース] で [IPAM 範囲] を選択します。
7. [アドレスファミリー] には [IPv4] を選択します。
8. [リソース計画] で、[範囲内のIP 空間計画] は選択したままにしておきます。
9. [Locale] (ロケール) で、プールのロケールを選択します。ロケールは、この IPAM プールを割り当てることができるようにする AWS リージョンです。使用可能なオプションは、IPAM を作成したときに選択した運用リージョンによって提供されます。
10. [Service] (サービス) で、[EC2 (EIP/VPC)] を選択します。選択したサービスによって、CIDR がアドバタイズされる AWS サービスが決定します。現在、唯一の選択肢は EC2 (EIP/VPC) であり、このプールから割り当てられた CIDR は、Amazon EC2 サービス (Elastic IP アドレスの場合) に対してアドバタイズできるようになります。
11. [パブリック IP ソース] で、[Amazon 所有] を選択します。
12. [プロビジョニングする CIDR] で、[Amazon 所有のパブリック CIDR を追加] を選択します。/29 (8 つの IP アドレス) から /30 (4 つの IP アドレス) までのネットマスク長を選択します。デフォルトでは、最大 2 つの CIDR を追加できます。Amazon 提供の連続したパブリック IPv4 CIDR の制限の引き上げに関する詳細については、「IPAM のクォータ」を参照してください。

13. [このプールの割り当てルールを設定する] は選択しません。
14. (オプション) プールのタグを選択します。
15. [プールを作成] を選択します。

続行する前に、この CIDR のプロビジョンが完了したことを確認してください。プロビジョニングの状態は、プールの詳細ページの CIDR タブで確認できます。

Command line

プールを作成するには

1. create-ipam-pool コマンドを使用して IPAM プールを作成します。ロケールは、この IPAM プールを割り当てることができるようにする AWS リージョンです。使用可能なオプションは、IPAM を作成したときに選択した運用リージョンによって提供されます。

```
aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-
scope-01bc7290e4a9202f9 --address-family ipv4 --locale us-east-1 --aws-service
 ec2 --public-ip-source amazon
```

create-in-progress 状態の応答例:

```
{

    "IpamPool": {

        "OwnerId": "320805250157",

        "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",

        "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-07ccc86aa41bef7ce",
        "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-01bc7290e4a9202f9",
        "IpamScopeType": "public",

        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",

        "IpamRegion": "us-east-1",

        "Locale": "us-east-1",
```

```
        "PoolDepth": 1,

        "State": "create-in-progress",

        "AutoImport": false,

        "AddressFamily": "ipv4",

        "Tags": [],

        "AwsService": "ec2",

        "PublicIpSource": "amazon"

    }

}
```

2. describe-ipam-pools コマンドを使用して、プールが正常に作成されたことを確認します。

```
aws ec2 describe-ipam-pools --region us-east-1 --ipam-pool-ids ipam-
pool-07ccc86aa41bef7ce
```

create-complete 状態の応答例:

```
{

    "IpamPools": [
        {
            "OwnerId": "320805250157",
            "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",
            "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-07ccc86aa41bef7ce",
            "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-01bc7290e4a9202f9",
            "IpamScopeType": "public",
            "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
            "IpamRegion": "us-east-1",
            "Locale": "us-east-1",
            "PoolDepth": 1,
            "State": "create-complete",
            "AutoImport": false,
            "AddressFamily": "ipv4",
```

```
            "Tags": [],
            "AwsService": "ec2",
            "PublicIpSource": "amazon"
        }
    ]
}
```

3. provision-ipam-pool-cidr コマンドを使用して、CIDR をプールにプロビジョニングします。/29 (8 個の IP アドレス) から /30 (4 個の IP アドレス) までの --netmask-length を選択します。デフォルトでは、最大 2 つの CIDR を追加できます。Amazon 提供の連続したパブリック IPv4 CIDR の制限の引き上げに関する詳細については、「IPAM のクォータ」を参照してください。

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce --netmask-length 29
```

pending-provision 状態の応答例:

```
{

    "IpamPoolCidr": {
        "State": "pending-provision",
        "IpamPoolCidrId": "ipam-pool-cidr-01856e43994df4913b7bc6aac47adf983",
        "NetmaskLength": 29
    }
}
```

4. 続行する前に、この CIDR のプロビジョンが完了したことを確認してください。プロビジョニングの状態は、get-ipam-pool-cidrs コマンドを使用して確認できます。

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

provisioned 状態の応答例:

```
{

    "IpamPoolCidrs": [
        {
            "Cidr": "18.97.0.40/29",
            "State": "provisioned",
```

```
            "IpamPoolCidrId": "ipam-pool-
cidr-01856e43994df4913b7bc6aac47adf983",
            "NetmaskLength": 29
        }
    ]
}
```

ステップ 3: プールから Elastic IP アドレスを割り当てる

プールから Elastic IP アドレスを割り当てるには、このセクションのステップを実行します。

AWS Management Console

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを割り当てる」のステップに従ってアドレスを割り当てます。ただし、次の点に注意してください。

- EC2 コンソールで使用している AWS リージョンが、ステップ 2 でプールを作成したときに選択したロケールオプションと一致していることを確認してください。
- アドレスプールを選択する際には、[IPv4 IPAM プールを使用して割り当てる] オプションを選択し、ステップ 1 で作成したプールを選択します。

Command line

allocate-address コマンドを使用して、プールからアドレスを割り当てます。使用する `--region` は、ステップ 2 でプールを作成した際に選択した `-locale` オプションと一致する必要があります。`--ipam-pool-id` のステップ 2 で作成した IPAM プールの ID を含めます。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

レスポンスの例:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

オプションで、--address オプションを使用して IPAM プール内の特定の /32 を選択することもできます。

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce --address 18.97.0.41
```

レスポンスの例:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを割り当てる」を参照してください。

ステップ 4: Elastic IP アドレスと EC2 インスタンスの関連付け

Elastic IP アドレスを EC2 インスタンスに関連付けるには、このセクションのステップを実行します。

AWS Management Console

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを関連付ける」にあるステップに従って、IPAM プールから Elastic IP アドレスを割り当てます。ただし、AWS マネジメントコンソールオプションを使用する場合は、Elastic IP アドレスを関連付ける AWS リージョンが、ステップ 2 でプールを作成したときに選択したロケールオプションと一致する必要があることに注意してください。

Command line

associate-address コマンドを使用して、Elastic IP アドレスをインスタンスに関連付けます。Elastic IP アドレスを関連付ける --region は、ステップ 2 でプールを作成したときに選択した --locale オプションと一致する必要があります。

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

レスポンスの例:

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスをインスタンスまたはネットワークインターフェイスに関連付ける」を参照してください。

ステップ 5: プールの使用状況を追跡およびモニタリングする

IPAM プールから Elastic IP アドレスを割り当てたら、IPAM プールの割り当てを追跡してモニタリングすることができます。

AWS Management Console

- IPAM コンソールで IPAM プールの詳細の [割り当て] タブを表示します。IPAM プールから割り当てられた Elastic IP アドレスの [リソースタイプ] は [EIP] です。
- Public IP Insights を使用する:
  - [パブリック IP タイプ] で、[Amazon 所有の EIP] でフィルタリングします。これは、Amazon 所有の Elastic IP アドレスに割り当てられたパブリック IPv4 アドレスの合計数を示します。このメジャーでフィルタリングし、ページの下部にある [パブリック IP アドレス] までスクロールすると、割り当てた Elastic IP アドレスを確認できます。
  - [EIP の使用状況] で、[関連付けられた Amazon 所有の EIP] または [関連付けられていない Amazon 所有の EIP] でフィルタリングします。これは、AWS アカウントで割り当てた Elastic IP アドレスのうち、EC2 インスタンス、ネットワークインターフェイス、または AWS リソースに関連付けられている、または関連付けられていないものの合計数を示します。このメジャーでフィルタリングし、ページの下部にある [パブリック IP アドレス] までスクロールすると、フィルタリングされたリソースの詳細を確認できます。
  - [Amazon 所有の IPv4 連続した IP の使用状況] で、シーケンシャルパブリック IPv4 アドレスの使用状況を経時的にモニタリングするとともに、関連する Amazon 所有の IPv4 IPAM プールをモニタリングします。
- Amazon CloudWatch を利用して、IPAM プールにプロビジョニングされた Amazon 提供の連続したパブリック IPv4 ブロックに関連するメトリクスを追跡およびモニタリングします。連続したする IPv4 ブロックに固有の使用可能なメトリクスについては、「IPAM メトリクス」の「パブリック IP メトリクス」を参照してください。メトリクスの表示に加えて、Amazon

CloudWatch でアラームを作成して、しきい値に達したときに通知を受け取ることができます。Amazon CloudWatch を使用したアラームの作成と通知の設定は、このチュートリアルの範囲外です。詳細については、『Amazon CloudWatch ユーザーガイド』の「Amazon CloudWatch アラームの使用」を参照してください。

Command line

- get-ipam-pool-allocations コマンドを使用して、IPAM プールの割り当てを表示します。IPAM プールから割り当てられた Elastic IP アドレスの [リソースタイプ] は [eip] です。

```
aws ec2 get-ipam-pool-allocations --region us-east-1 --ipam-pool-id ipam-pool-07ccc86aa41bef7ce
```

レスポンスの例:

```
{
     "IpamPoolAllocations": [
        {
            "Cidr": "18.97.0.40/32",
            "IpamPoolAllocationId": "ipam-pool-alloc-0bd07df786e8148aba2763e2b6c1c44bd",
            "ResourceId": "eipalloc-0c9decaa541d89aa9",
            "ResourceType": "eip",
            "ResourceRegion": "us-east-1",
            "ResourceOwner": "320805250157"
        }
    ]
}
```

- Amazon CloudWatch を利用して、IPAM プールにプロビジョニングされた Amazon 提供の連続したパブリック IPv4 ブロックに関連するメトリクスを追跡およびモニタリングします。連続したする IPv4 ブロックに固有の使用可能なメトリクスについては、「IPAM メトリクス」の「パブリック IP メトリクス」を参照してください。メトリクスの表示に加えて、Amazon CloudWatch でアラームを作成して、しきい値に達したときに通知を受け取ることができます。Amazon CloudWatch を使用したアラームの作成と通知の設定は、このチュートリアルの範囲外です。詳細については、『Amazon CloudWatch ユーザーガイド』の「Amazon CloudWatch アラームの使用」を参照してください。

これでチュートリアルは完了しました。Amazon 提供の連続したパブリック IPv4 CIDR ブロックを使用して IPAM プールを作成し、プールから Elastic IP アドレスを割り当て、IPAM プールの割り当てをモニタリングする方法について学習しました。このチュートリアルで作成したリソースを削除するには、次のセクションに進みます。

クリーンアップ

このセクションのステップに従って、このチュートリアルで作成したリソースをクリーンアップします。

ステップ 1: Elastic IP アドレスの関連付けを解除する

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスの関連付けを解除する」にあるステップを実行して、Elastic IP アドレスの関連付けを解除します。

ステップ 2: Elastic IP アドレスを解放する

「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを解放する」にあるステップを実行して、パブリック IPv4 プールから Elastic IP アドレスを解放します。

ステップ 3: IPAM プールから CIDR のプロビジョニングを解除する

プールから CIDR のプロビジョニングを解除するには のステップを実行して、Amazon 所有のパブリック CIDR のプロビジョニングを IPAM プールから解除します。このステップは、プールの削除に必要なステップです。このステップが完了するまでは、Amazon 提供の連続する IPv4 ブロックの料金が請求されます。

ステップ 4: IPAM プールを削除する

プールを削除する のステップを実行して IPAM プールを削除します。

ステップ 5: IPAM を削除する

IPAM を削除する のステップを実行して IPAM を削除します。

これで、チュートリアルのクリーンアップは完了です。

IPAM での Identity and Access Management

AWS ではセキュリティ認証情報を使用して、ユーザーを識別し、AWS リソースへのアクセスを付与します。AWS Identity and Access Management (IAM)の機能を使用して、他のユーザー、サービス、およびアプリケーションが完全にまたは制限付きでお客様の AWS リソースを使用できるようにします。その際、お客様のセキュリティ認証情報は共有されません。

このセクションでは、IPAM のために作成された AWS サービスリンクロール、および IPAM サービスリンクロールにアタッチされたマネージドポリシーについて説明します。AWS IAM ロールおよびポリシーについての詳細については、IAM ユーザーガイドのロールに関する用語と概念を参照してください。

VPC の Identity and Access Management に関する詳細については、Amazon VPC ユーザーガイドの「Amazon VPC の Identity and Access Management」を参照してください。

内容

IPAM のサービスリンクロール

IPAM は、AWS Identity and Access Management (IAM) のサービスリンクロールを使用します。サービスリンクロールとは、一意のタイプの IAM ロールです。サービスリンクロールは、IPAM による事前定義済みのロールであり、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可を備えています。

サービスにリンクされたロールを使用することで、必要なアクセス権限を手動で追加する必要がなくなるため、IPAM の設定が簡単になります。IPAM は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、IPAM のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールのアクセス許可

IPAM は、AWSServiceRoleForIPAM サービスリンクロールを使用して、AWSIPAMServiceRolePolicy マネージドポリシーにアタッチされているアクションを呼び出

します。そのポリシーで許可されるアクションの詳細については、IPAM の AWS マネージドポリシーを参照してください。

このサービスリンクロールには、ipam.amazonaws.com サービスがサービスリンクロールを継承することを可能にする IAM 信頼ポリシーもアタッチされています。

サービスにリンクされたロールの作成

IPAM は、アカウント内のサービスがリンクされたロールを引継ぎ、リソースとその CIDR を検出し、リソースを IPAM に統合することによって、1 つ以上のアカウントの IP アドレスの使用状況をモニタリングします。

サービスにリンクされたロールは、次の 2 つの方法のいずれかで作成されます。

- AWS Organizations と統合する場合

  IPAM コンソールまたは enable-ipam-organization-admin-account AWS CLI コマンドを使用して IPAM を AWS Organizations 内のアカウントと統合する する場合、各 AWS Organizations メンバーのアカウントに対して、AWSServiceRoleForIPAM サービスにリンクされたロールが自動的に作成されます。その結果、すべてのメンバーアカウント内のリソースは、IPAM によって検出されます。

  > **Important**
  >
  > IPAM がユーザーに代わってサービスにリンクしたロールを作成する場合
  >
  > - IPAM と AWS 組織の統合を可能にする AWS 組織の管理アカウントには、次のアクションを許可する IAM ポリシーがアタッチされている必要があります。
  >   - ec2:EnableIpamOrganizationAdminAccount
  >   - organizations:EnableAwsServiceAccess
  >   - organizations:RegisterDelegatedAdministrator
  >   - iam:CreateServiceLinkedRole
  > - IPAM アカウントには、iam:CreateServiceLinkedRole アクションを許可する IAM ポリシーがアタッチされている必要があります。

- 1 つの AWS アカウントを使用して IPAM を作成する場合

  IPAM を 1 つのアカウントで使用する の場合、そのアカウントとして IPAM を作成すると、AWSServiceRoleForIPAM サービスにリンクされたロールが自動的に作成されます。

> **Important**
>
> 1 つの AWS アカウントで IPAM を使用する場合は、IPAM を作成する前に、使用する AWS アカウントに `iam:CreateServiceLinkedRole` アクションを許可する IAM ポリシーがアタッチされていることを確認する必要があります。IPAM を作成した場合、AWSServiceRoleForIPAM サービスにリンクされたロールが自動的に作成されます。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの説明の編集」を参照してください。

サービスにリンクされたロールを編集する

AWSServiceRoleForIPAM サービスリンクロールを編集することはできません。

サービスにリンクされたロールを削除する

IPAM を使用する必要がなくなった場合は、AWSServiceRoleForIPAM サービスリンクロールを削除することをお勧めします。

> **Note**
>
> サービスリンクロールを削除するには、AWS アカウントの IPAM リソースをすべて削除する必要があります。これにより、IPAM のモニタリング機能を誤って削除することがなくなります。

AWS CLI を使用して、サービスにリンクされたロールを削除するには、次のステップを実行します。

1. deprovision-ipam-pool-cidr および delete-ipam を使用して IPAM を削除します。詳細については、「プールから CIDR のプロビジョニングを解除するには」および「IPAM を削除する」を参照してください。
2. disable-ipam-organization-admin-account を使用して、IPAM アカウントを無効化します。
3. disable-aws-service-access で `--service-principal ipam.amazonaws.com` オプションを使用して、IPAM サービスを無効化します。

4. delete-service-linked-role を使用して、サービスリンクロールを削除します。サービスリンクロールを削除すると、IPAM ポリシーも削除されます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

IPAM の AWS マネージドポリシー

IPAM を 1 つの AWS アカウント使用している状況で IPAM を作成する場合、AWSIPAMServiceRolePolicy マネージドポリシーは自動的に IAM アカウントに作成され、AWSServiceRoleForIPAM サービスにリンクされたロールにアタッチされます。

AWS 組織との IPAM 統合を有効にすると、AWSIPAMServiceRolePolicy 管理ポリシーが IAM アカウントと各 AWS の組織メンバーアカウントに自動的に作成され、管理ポリシーが AWSServiceRoleForIPAM サービスにリンクされたロールにアタッチされます。

このマネージドポリシーによって、IPAM で以下のことが実行できるようになります。

- AWS Organizations のすべてのメンバーで、EC2 ネットワークリソースに関連付けられた CIDR を監視します。
- IPAM プールで使用可能な IP アドレス空間や、割り当てルールに準拠しているリソース CIDR の数など、IPAM に関連するメトリクスを Amazon CloudWatch に保存する。
- マネージドプレフィックスリストを変更して読み取ります。

次の例は、作成されるマネージドポリシーの詳細を表示したものです。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "IPAMDiscoveryDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:ListByoipCidrs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsPublishActions",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

前の例の最初のステートメントにより、IPAM は、1 つの AWS アカウントまたは AWS 組織のメンバーによって使用される CIDR を監視できます。

上記の例の 2 番目のステートメントでは、`cloudwatch:PutMetricData` 条件キーを使用して、IPAM が `AWS/IPAM` Amazon CloudWatch 名前空間 に IPAM メトリクスを保存できるようにし

ます。これらのメトリクスは、IPAM プールとスコープ内の割り当てに関するデータを表示するために、AWS マネジメントコンソール で使用されます。詳細については、「IPAM ダッシュボードで CIDR の使用状況をモニタリングする」を参照してください。

AWS マネージドポリシーに対する更新

IPAM の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。

変更	説明	日付
AWSIPAMServiceRolePolicy	AWSIPAMServiceRolePolicy マネージドポリシー (ec2:ModifyManagedPrefixList、ec2:DescribeManagedPrefixLists、および ec2:GetManagedPrefixListEntries) にアクションが追加され、IPAM でプレフィックスリストの変更と読み取りができるようになりました。	2025 年 10 月 31 日
AWSIPAMServiceRolePolicy	AWSIPAMServiceRolePolicy マネージドポリシー (`organizations:ListChildren` 、`organizations:ListParents` 、`organizations:DescribeOrganizationalUnit`) に追加されたアクション。これにより、お客様が OU レベルで IPAM を使用できるよう、IPAM は AWS Organizations の組織単位 (OU) の詳細を取得できます。	2024 年 11 月 21 日

変更	説明	日付
AWSIPAMServiceRolePolicy	リソース検出中に IPAM がパブリック IP アドレスを取得できるようにするアクションが awSipamServiceRolePolicy 管理ポリシー (`ec2:GetIpamDiscoveredPublicAddresses`) に追加されました。	2023 年 11 月 13 日
AWSIPAMServiceRolePolicy	リソース検出時に IP アドレス管理がパブリック IP アドレスを取得できるように、awSipAmServiceRolePolicy 管理ポリシー (`ec2:DescribeAccountAttributes` 、`ec2:DescribeNetworkInterfaces` 、`ec2:DescribeSecurityGroups` 、`ec2:DescribeSecurityGroupRules` 、`ec2:DescribeVpnConnections` 、`globalaccelerator:ListAccelerators` 、および `globalaccelerator:ListByoipCidrs`) にアクションが追加されました。	2023 年 11 月 1 日

変更	説明	日付
AWSIPAMServiceRolePolicy	AWSIPAMServiceRolePolicy マネージドポリシーに 2 つのアクション (`ec2:GetIpamDiscoveredAccounts` および `ec2:GetIpamDiscoveredResourceCidrs`) が追加され、IPAM がリソース検出中に監視対象の AWS アカウントとリソース CIDR を取得できるようになりました。	2023 年 1 月 25 日
IPAM が変更の追跡を開始しました	IPAM が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 12 月 2 日

ポリシーの例

このセクションのポリシーの例には、IPAM をフルに使用するための関連する AWS Identity and Access Management (IAM) アクションがすべて含まれています。IPAM の使用方法によっては、すべての IAM アクションを含める必要はない場合があります。IPAM コンソールを十分に活用するには、AWS Organizations、AWS Resource Access Manager (AWS RAM)、Amazon CloudWatch などのサービスに追加の IAM アクションを含める必要がある場合があります。

JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIpamByoasn",
                "ec2:DeprovisionIpamByoasn",
                "ec2:DescribeIpamByoasn",
```

```
                "ec2:DisassociateIpamByoasn",
                "ec2:ProvisionIpamByoasn",
                "ec2:CreateIpam",
                "ec2:DescribeIpams",
                "ec2:ModifyIpam",
                "ec2:DeleteIpam",
                "ec2:CreateIpamScope",
                "ec2:DescribeIpamScopes",
                "ec2:ModifyIpamScope",
                "ec2:DeleteIpamScope",
                "ec2:CreateIpamPool",
                "ec2:DescribeIpamPools",
                "ec2:ModifyIpamPool",
                "ec2:DeleteIpamPool",
                "ec2:ProvisionIpamPoolCidr",
                "ec2:GetIpamPoolCidrs",
                "ec2:DeprovisionIpamPoolCidr",
                "ec2:AllocateIpamPoolCidr",
                "ec2:GetIpamPoolAllocations",
                "ec2:ReleaseIpamPoolAllocation",
                "ec2:CreateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveries",
                "ec2:ModifyIpamResourceDiscovery",
                "ec2:DeleteIpamResourceDiscovery",
                "ec2:AssociateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveryAssociations",
                "ec2:DisassociateIpamResourceDiscovery",
                "ec2:GetIpamResourceCidrs",
                "ec2:ModifyIpamResourceCidr",
                "ec2:GetIpamAddressHistory",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ipam.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

IPAM のクォータ

このセクションでは、IPAM に関連するクォータの一覧を示します。Service Quotas コンソールには、IPAM のクォータに関する情報も表示されます。Service Quotas コンソールを使用して、デフォルトのサービスクォータを表示したり、調整可能なクォータのクォータの引き上げをリクエストしたりすることができます。詳細については、「Service Quotas ユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

名前	デフォルト	引き上げ可能
Amazon 提供の連続したパブリック IPv4 CIDR ブロック	2	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
Amazon 提供の連続したパブリック IPv4 CIDR ブロックネットマスクの長さ	/29	許容サイズは /29 ~ /30 です。引き上げをリクエストするには、「AWS 全般のリファレンス」の「AWS Service Quotas」にある説明に従って、AWS サポートセンターに問い合わせてください。
Amazon 提供の IPv6 CIDR ブロックのネットマスク長	/52	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに

名前	デフォルト	引き上げ可能
		問い合わせてください。
リージョンプールあたりの Amazon 提供の IPv6 CIDR ブロック	1	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
IPAM に持ち込めるAS 番号 (ASN)	5	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
プールごとの CIDR	50	はい
IPAM ポリシーごとに有効なターゲット	100	はい。クォータの調整をリクエストするには、「AWS 全般のリファレンス」の「AWS Service Quotas」にある説明に従って、AWS サポートセンターに問い合わせてください。
組織あたりの IPAM 管理者	1	不可

名前	デフォルト	引き上げ可能
リージョンあたりの IPAM	1	いいえ
IPAM あたりの IPAM ポリシー	10	はい。クォータの調整をリクエストするには、「AWS 全般のリファレンス」の「AWS Service Quotas」にある説明に従って、AWS サポートセンターに問い合わせてください。
リソースとロケールのペアあたりの IPAM ポリシー割り当てルール*	10	はい。クォータの調整をリクエストするには、「AWS 全般のリファレンス」の「AWS Service Quotas」にある説明に従って、AWS サポートセンターに問い合わせてください。
リソース検出あたりの組織単位の除外	10	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
プールの深さ (プール内のプール数)	10	あり
スコープあたりのプール数	50	はい

名前	デフォルト	引き上げ可能
IPAM あたりのプレフィックスリストリゾルバー数	10	あり
プレフィックスリストリゾルバーあたりのプレフィックスリストリゾルバーターゲット数	50	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
プレフィックスリストリゾルバーあたりのルール数	100	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
プレフィックスリストリゾルバーバージョンあたりの CIDR エントリ数	1,000	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
IPAM あたりのリソース検出の関連付け	5	あり
リージョンあたりのリソース検出	1	いいえ

名前	デフォルト	引き上げ可能
リソース使用率メトリクス	50	はい。「AWS 全般のリファレンス」の「AWS サービスクォータ」にある説明に従って、AWS サポートセンターに問い合わせてください。
IPAM あたりのスコープ数	5	はい。IPAM を作成すると、プライベートとパブリックのデフォルトスコープが自動的に作成されます。追加のスコープを作成する場合、それらはプライベートスコープになります。パブリックスコープは追加で作成できません。

* リソースとロケールのペア: 割り当てルールを設定するときは、リソースタイプ (EIP、ALB、RDS クラスターなどの AWS リソース) とロケール (ルールが適用される AWS リージョンまたはローカルゾーン) の両方を指定する必要があります。割り当てルールは、このリソースタイプとロケールの組み合わせにスコープされます。例えば、us-east-1 で EIP のポリシーを設定する場合、その特定のリソースとロケールのペアに最大 10 個のルールを設定できます*。

IPAM の料金

Amazon VPC IP Address Manager (IPAM) は、AWS リソースとオンプレミスネットワーク全体で IP アドレス空間を管理するのに役立つサービスです。IPAM は、AWS およびオンプレミスリソースによって使用される IP アドレスを一元的に計画、モニタリング、制御する方法を提供します。

このセクションでは、価格に関連する情報および、現在の IPAM コストを表示する方法を説明します。

内容

料金情報の表示

IPAM には無料利用枠とアドバンス利用枠の 2 つの階層があります。無料利用枠で利用できる機能とアドバンスト利用枠に関連するコストの詳細については、[Amazon VPC の料金] ページで [IPAM] タブを参照してください。

AWS Cost Explorer を使用して現在のコストと使用量を確認できます。

IPAM Advanced Tier を使用する場合、IPAM が管理するアクティブな IP アドレスごとに時間単位の料金を支払います。IPAM コストと使用状況を表示して分析するには、AWS Cost Explorer を使用します。

1. AWS Cost Management コンソール (https://console.aws.amazon.com/cost-management/home) を開きます。
2. Cost Explorer を起動します。
3. [使用状況タイプ] を選択して **`IPAddressManager`** を入力すると、IPAM の使用状況をフィルタリングできます。
4. 1 つまたは複数のチェックボックスを選択します。それぞれが異なる AWS リージョンを表しています。
5. [適用] をクリックします。

たとえば、USE1-IPAddressManager-IP-Hours(Hrs) を選択しており、us-east-1 リージョンが IPAM のホームリージョンである場合、IPAM によって請求されるアクティブな IP 時間数と費用が表示されます。たとえば、時間単位の使用量が 18 時間であれば、1 つのアクティブな IP アドレスを 18 時間、または 3 つの異なるリージョンにおける 3 つの IP アドレスをそれぞれ 6 時間アクティブにすることができます。また、他にも合計 18 時間となる任意の組み合わせを取ることができます。

AWS Cost Explorer の詳細については、AWS Cost Management ユーザーガイドの「AWS Cost Explorer によるコストの分析」を参照してください。

関連情報

AWS 技術ドキュメントサイトは包括的なリソースですが、AWS サービスに関する情報を見つける場所は他にも多数あります。AWS ブログ、ホワイトペーパー、導入事例、コミュニティフォーラムは、公式の技術的な詳細情報以外にも、有益なインサイト、実例、代替的な視点を提供できます。これらのさまざまなソースを詳しく見ることで、AWS オファリングをより良く理解できます。

Amazon VPC IP Address Manager を利用する際は、次の関連リソースが役立ちます。

- Amazon VPC IP Address Manager のベストプラクティス: Amazon VPC IP Address Manager を使用して、スケーラブルなアドレススキームを計画および作成するためのベストプラクティスを紹介する AWS ブログです。
- Amazon VPC IP Address Manager による大規模なネットワークアドレス管理および監査: Amazon VPC IP Address Manager の紹介や、AWS コンソールでのサービスの使用方法について記載した AWS ブログです。
- Configure fine-grained access to your resources shared using AWS Resource Access Manager: AWS 組織単位のアカウントと IPAM プールを共有する方法を説明する AWS ブログです。
- CIDR マップを使用してエンタープライズ IP アドレス管理および計画を視覚化する: IPAM コンソールで IPAM CIDR マップを使用して IPv4 および IPv6 ランドスケープ全体を視覚化する方法を説明する AWS ブログ。

IPAM のドキュメント履歴

以下は、IPAM のリリースを説明する表です。

機能	説明	リリース日
IPAM を使用して独自の IP を CloudFront に持ち込む	IPAM を使用して、CloudFront エニーキャストサービスを含む AWS グローバルサービスの BYOIP CIDR を管理します。	2025 年 11 月 21 日
IPAM ポリシーを使用してパブリック IPv4 割り当て戦略を定義する	IPAM ポリシーを使用して、AWS サービスを特定の IPAM プールにマッピングするルールを定義できるようになりました。これにより、パブリック IPv4 割り当て戦略を定義できます。	2025 年 11 月 19 日
IPAM と Infoblox インフラストラクチャを統合する	IPAM を Infoblox インフラストラクチャと統合できるようになりました。これにより、クラウドネイティブ AWS 機能を取得しながら、既存の Infoblox ワークフローを通じて AWS IP アドレスを管理できます。この統合はプライベートスコープで利用でき、IPAM Advanced Tier が必要です。	2025 年 11 月 7 日
プレフィックスリストの更新を自動化する	IPAM プレフィックスリストリゾルバーを使用して、IPAM プール CIDR に基づいてプレフィックスリストの更新を自動化できるようになりました。	2025 年 10 月 31 日
IPAM コンソールからアラームを管理する	Amazon CloudWatch アラームの作成と管理を、IPAM コンソールから直接実行できるようになりました。IPAM 関連のアラームは、INSUFFICIENT_DATA または ALARM 状態になったときに、警告バーおよびビジュアルインジケータとして表示されます。	2025 年 8 月 21 日
コスト分散を有効にする	コスト配分を有効にすると、アクティブな IP アドレスの料金を IPAM 所有者ではなく IP アドレスを使用しているアカウントに分配しま	2025 年 5 月 1 日

機能	説明	リリース日
	す。これは、委任された IPAM 管理者が IPAM を使用して IP アドレスを一元的に管理しており、各アカウントがそれぞれの使用料金を負担する大規模な組織に有用な機能で、請求額の手動計算が不要になります。	
IPAM から組織単位を除外する	IPAM が AWS Organizations と統合される場合、IPAM から組織単位を除外できるようになりました。IPAM は、組織単位の除外に含まれるアカウントの IP アドレスを管理しません。	2024 年 11 月 21 日
AWS 管理ポリシーの更新の更新 – 既存ポリシーの更新	既存の AWSIPAMServiceRolePolicy が更新されました。	2024 年 11 月 21 日
IPAM プールからシーケンシャル Elastic IP アドレスを割り当てる	IPAM を使用すると、Amazon 所有のパブリック IPv4 ブロックを IPAM プールにプロビジョニングし、それらのプールから AWS リソースにシーケンシャル Elastic IP アドレスを割り当てることができるようになりました。シーケンシャル Elastic IP アドレスを使用すると、ネットワークとセキュリティの許可リスト作成のニーズを簡素化できます。	2024 年 8 月 28 日
プライベート IPv6 GUA と ULA	プライベート IPv6 GUA および ULA 範囲をプライベートスコープの IPAM プールにプロビジョニングできるようになりました。プライベート IPv6 アドレスは IPAM でのみ使用できます。プライベート IPv6 アドレス指定の詳細については、「Amazon VPC ユーザーガイド」の「プライベート IPv6 アドレス」を参照してください。	2024 年 8 月 8 日
IPAM の無料利用枠とアドバンストティア	IPAM の無料利用枠とアドバンストティアから選択できるようになりました。	2023 年 11 月 17 日

機能	説明	リリース日
Public IP Insights	以前は、Public IP Insights は 1 つのリージョンのみで表示できました。リージョンの Public IP Insights を表示できるようになりました。さらに、Amazon CloudWatch でパブリック IP アドレスのインサイトを表示できるようになりました。	2023 年 11 月 17 日
サブネット IP 割り当て用の VPC IP アドレススペースを計画する	IPAM を使用して VPC 内のサブネット IP スペースを計画し、サブネットと VPC レベルで IP アドレス関連のメトリクスを監視できるようになりました。	2023 年 11 月 17 日
Bring-Your-Own-ASN (BYOASN)	ユーザ は AWS に対し Autonomous System number (ASN) です。	2023 年 11 月 17 日
AWS 管理ポリシーの更新の更新 – 既存ポリシーの更新	既存の AWSIPAMServiceRolePolicy が更新されました。	2023 年 11 月 17 日
AWS 管理ポリシーの更新の更新 – 既存ポリシーの更新	既存の AWSIPAMServiceRolePolicy が更新されました。	2023 年 11 月 1 日
リソース使用率メトリクス	IPAM が、IPAM で監視するリソースの IP 使用率メトリクスを Amazon CloudWatch に発行するようになりました。	2023 年 8 月 2 日
Public IP Insights	Public IP Insights には、このリージョンのサービスで使用されている、アカウント内のすべてのパブリック IPv4 アドレスが表示されます。これらのインサイトを利用して、パブリック IPv4 アドレスの使用状況を特定し、未使用の Elastic IP アドレスを解放するための推奨事項を確認できます。	2023 年 7 月 28 日

機能	説明	リリース日
AWS 管理ポリシーの更新の更新 – 既存ポリシーの更新	既存の AWSIPAMServiceRolePolicy が更新されました。	2023 年 1 月 25 日
IPAM を組織外のアカウントに統合する	単一の IPAM アカウントから組織外の IP アドレスを管理し、他の AWS Organizations のアカウントと IPAM プールを共有できるようになりました。	2023 年 1 月 25 日
IPAM プールのための Amazon 提供の IPv6 連続 CIDR ブロック	パブリックスコープで IPAM プールを作成するときに、Amazon 提供の IPv6 連続 CIDR ブロックをプールにプロビジョニングできるようになりました。詳細については、「IPAM で IPv6 アドレスプールを作成する」を参照してください。	2023 年 1 月 25 日
初回リリース	このリリースでは、Amazon VPC IP Address Manager が導入されています。	2021 年 12 月 2 日