Amazon Virtual Private Cloud

IP Address Manager

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

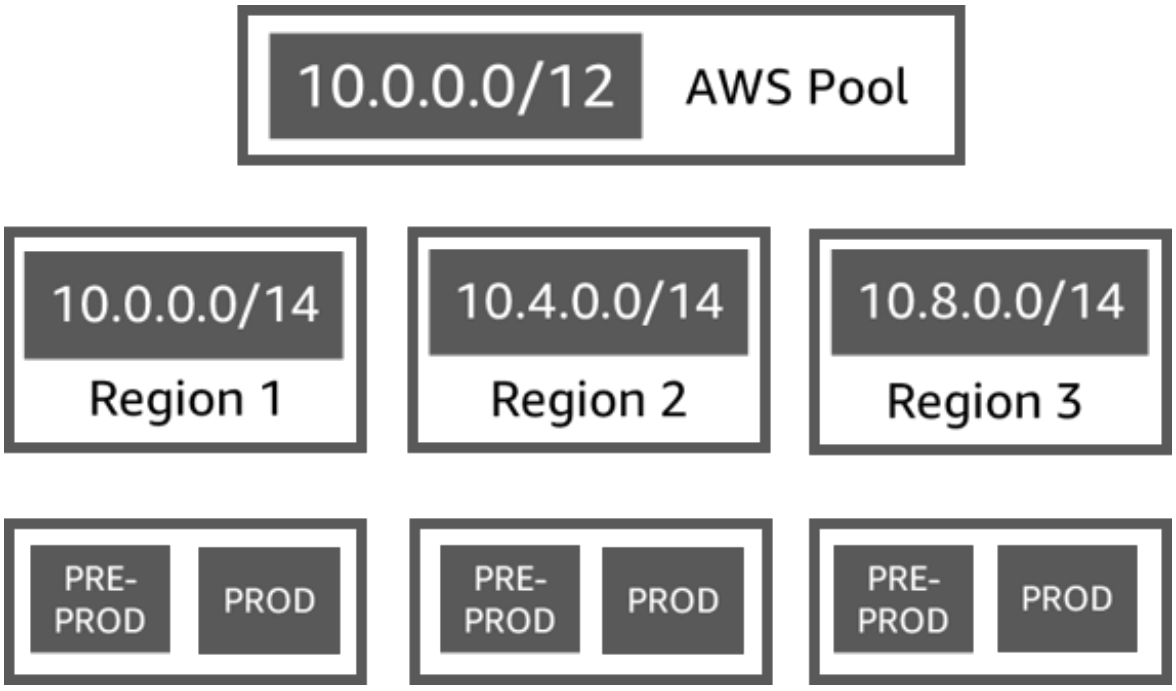
このガイドには以下のセクションがあります。

- IPAM の仕組み (p. 2): IPAM の概念と用語
- IPAM の開始方法 (p. 4): 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 (p. 18): 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 (p. 31): 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。
- チュートリアル (p. 39): 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 には、2 つのデフォルトスコープが含まれています。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、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。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、割り当てをモニタリングおよび管理できます。

IPAM は、お客様が所有するプライベート IPv4 CIDR および公開 IPv4/IPv6 CIDR を管理およびモニタリングできます。IPAM は、Amazon が所有する公開 IP 空間のみを (管理ではなく) モニタリングすることができます。

開始して IPAM を作成するには、IPAM の開始方法 (p. 4)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。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。

目次

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 コマンドラインインターフェイス (AWS CLI): Amazon VPC を含む一連のさまざまな AWS 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。AWS CLI を取得するには、AWS Command Line Interfaceを参照してください。
- 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、同じ操作を行う方法を示す AWS CLI ドキュメントへのリンクが含まれています。

IPAM を初めて使用する場合は、IPAM の仕組み (p. 2) を参照して Amazon VPC での IPAM のロールについて学習し、IPAM のアクセス許可を設定する (p. 4) の手順に進みます。

IPAM のアクセス許可を設定する

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 組織と統合して、すべての AWS 組織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 Amazon VPC IPAM サービスが管理およびモニタリングできるようにするには、IPAM を AWS Organizations と統合する (p. 5) 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モニタリング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 (p. 6) 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モニタリングできません。

目次

IPAM を AWS Organizations 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モニタリングします。

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 使用状況をモニタリングする 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。

Important

- 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。

Note

AWS Organizations と統合する場合:

- IPAM を使用して、複数の AWS Organizations のIP アドレスを管理することはできません。
- IPAM では、組織のメンバーアカウントでモニタリングするアクティブな 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 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。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 IAM ユーザーアカウントは、次の IAM ポリシーアクション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`

  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 Management Console

IPAM アカウントを選択するには

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 [Settings] (設定) をクリックします。
4. [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。
5. [Delegate] (委任) 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。

- 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モニタリングします。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 1 つのアカウントで使用する

IPAM を AWS Organizations と統合する (p. 5) 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 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。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 (p. 105)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 IAM ポリシーがアタッチされているか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 (p. 7) 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 組織と統合するには、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 (p. 109) 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。
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、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。
6. [Create] (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。

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 (p. 2) 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。

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。詳細については、「IPAM を AWS Organizations と統合する (p. 5)」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 (p. 109)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。1 つの IPAM プールを作成する場合は、トップレベルプールを作成する (p. 10) のステップを完了してから CIDR を割り当てる (p. 15) に進みます。

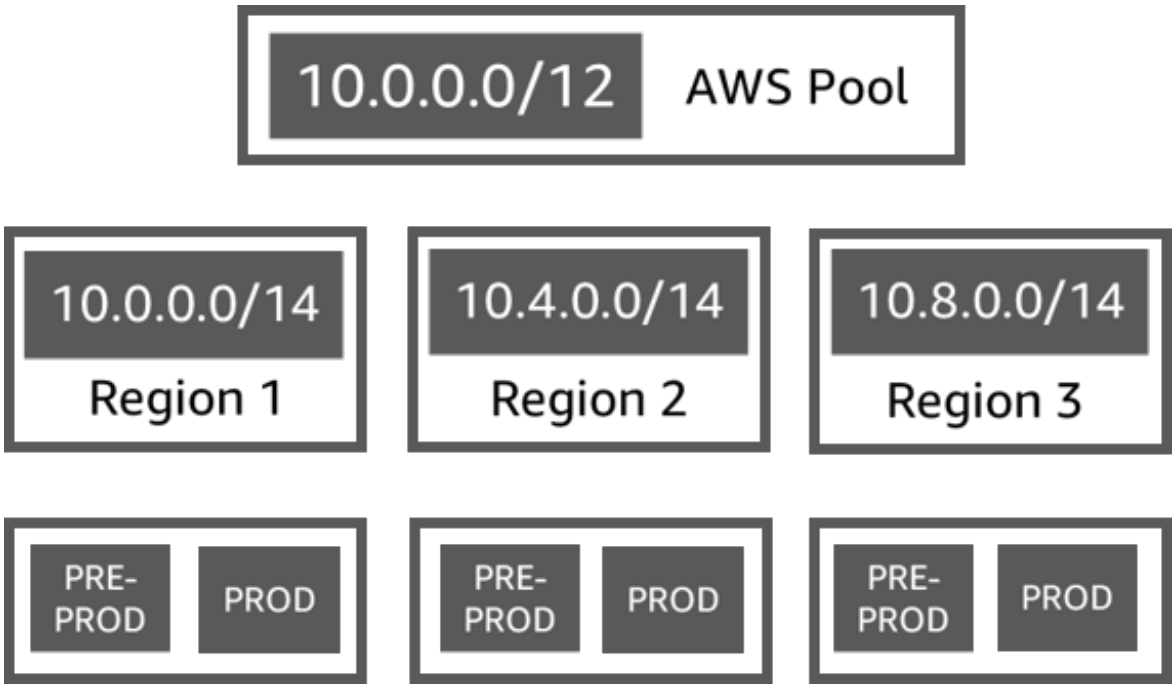
目次

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。

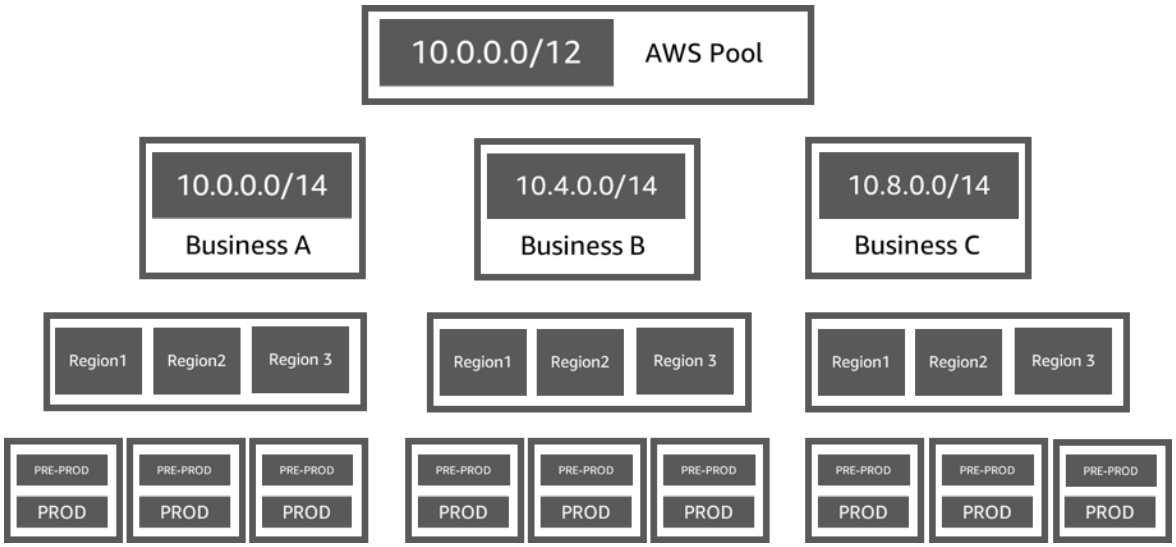
複数の AWS リージョンのプール

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。



複数の事業部門用のプール

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。



トップレベルプールを作成する

このセクションの手順に従って、トップレベル 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。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。

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 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。

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 (p. 32) 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 (p. 19) 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、スペースが利用可能であれば、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できますが、そのようにするとプールの割り当てルールに違反するため、IPAM はこのリソースに非準拠のフラグを立てます。

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、[Pools] (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 (p. 2)」を参照してください。
4. [Create pool] (プールの作成) 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. [No source pool] (ソースプールなし) を選択します。
7. [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。

   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。
8. このプール用のアドレスファミリーを選択します。このプール内の IP アドレスが IPv4 アドレスになる場合は、[IPv4] を選択します。IPv6 アドレスになる場合は [IPv6] を選択します。このプー

ルに選択したスコープがパブリックスコープである場合は、IPv4 または IPv6 のいずれかを使用するオプションがあります。このプールに選択したスコープがプライベートの場合、IPv4 が唯一のオプションです。

9. (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。
10. 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。以下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て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。
      - IPAM が重複する複数の CIDR を検出した場合、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。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`** の場合に、ここに **`16`** を入力すると、このプールの新しい割り当ては、デフォルトでネットマスク長が **`/16`** 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] (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。
11. (オプション) プールのタグを選択します。
12. [Create pool] (プールの作成) を選択します。

Command line

このセクションのコマンドは、AWS CLI リファレンスドキュメントに関連しています。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。

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、CIDR を割り当てる (p. 15) に進んでください。

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 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。

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、[Pools] (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 (p. 2)」を参照してください。
4. [Create pool] (プールの作成) 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. [Source pool] (ソースプール) の下で、前のセクションで作成したトップレベルプールを選択します。
7. 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。
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。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、トップレベルプールを作成する (p. 10) 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。
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。

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。

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、CIDR を割り当てる (p. 15) 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)
        - 実稼働 VPC の開発プール (10.0.1.0/24)
      - AWS リージョン 2 のリージョンプール (10.1.0.0/16)

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、[Pools] (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 (p. 2)」を参照してください。
4. [Create pool] (プールの作成) 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. [ソースプール] で、[Regional pool] (リージョンプール) を選択します。
7. 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。ここで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。

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、トップレベルプールを作成する (p. 10) 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。

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。

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。

CIDR を割り当てる

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。

次の例は、このセクションの手順で作成できるプール構造の階層を示しています。

- 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
    - 最上位の IPAM プール (10.0.0.0/8)
      - AWS リージョン 2 のリージョン IPAM プール (10.0.0.0/16)
        - 開発プール (10.0.0.0/24)
          - 割り当て - VPC (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。

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 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、チュートリアル (p. 39) 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。

> Important
>
> パブリックスコープのプールから CIDR を手動で割り当てることはできません。

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 (p. 2)」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)、[Allocate CIDR] (CIDR を割り当てる) の順に選択します。
6. 割り当てる正確な CIDR (たとえば、`10.0.0.0/24`) を定義するかどうかを選択するか、ネットマスクの長さ (たとえば、`/24`) のみを選択します。

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 リファレンスドキュメントに関連しています。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。

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 (p. 27)」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。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。

目次

VPC 作成に対して 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 と統合する (p. 5)」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[Creating an SCP] (SCP 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。

```
{
 "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「サービスコントロールポリシーのアタッチとデタッチ」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[Creating an SCP] (SCP 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。

```
{
 "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「サービスコントロールポリシーのアタッチとデタッチ」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

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、IAM ユーザー、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 と統合する (p. 5)」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、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。

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 (p. 2) 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. [Next] 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: 既存の BYOIP IPv4 CIDR を IPAM に転送する (p. 99) 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 リファレンスドキュメントに関連しています。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 (p. 32) 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。

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 (p. 31) 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。

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 (p. 2) 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. 追加したい CIDR を入力し、さらに CIDR を追加する場合は [Add new CIDR] (新しい CIDR の追加) を選択します。

   Note

   CIDR をプールにプロビジョニングするには、次の条件を満たす必要があります。

   - 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. [Request provisioning] (プロビジョニングのリクエスト) 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 リファレンスドキュメントに関連しています。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。

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

プールから CIDR のプロビジョニングを解除するには

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。

> **Important**
>
> 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、割り当ての解除 (p. 27) を参照してください。

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 (p. 2)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 リファレンスドキュメントに関連しています。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。

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 (p. 22) 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 (p. 23) を参照してください。

プールを編集する

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。プールを編集して、プールの割り当てルールを変更することもできます。割り当てルールの詳細については、トップレベルプールを作成する (p. 10)を参照してください。

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 (p. 2)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、トップレベルプールを作成する (p. 10)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

プールを削除する

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。

Important

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 (p. 22)を行う必要があります。

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 (p. 2)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 リファレンスドキュメントに関連しています。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。

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、トップレベルプールを作成する (p. 10) を参照してください。

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 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は表示されません。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、「スコープ間でリソース CIDR を移動する (p. 25)」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 リファレンスドキュメントに関連しています。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。

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

スコープ間でリソース CIDR を移動する

リソース CIDR を、あるスコープから別のスコープに移動するには、このセクションのステップに従います。

Important

- リソース CIDR 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移動できます。リソース 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。
- CIDR を移動できるのは、IPAM が管理可能なリソースに対してのみです。
- 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リソース CIDR が現在割り当てられている場合、移動要求は成功しますが、リソース CIDR は、現在のプールからリソース CIDR 割り当てをリリースするまで移動されません。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

リソースに割り当てられた単一の 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、[Resources] (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、リソースを選択し、リソースの詳細を表示します。
5. [Associated CIDRs] (関連付けられた 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) を選択します。
6. リソース CIDR の移動先のスコープを選択します。
7. [Change scope] (スコープの変更) を選択します。

リソースに割り当てられたすべての 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、[Resources] (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、CIDR を移動するリソースを選択します。
5. [Actions] (アクション) > [Move all associated CIDRs to different scope] (関連するすべての CIDR を別のスコープに移動) を選択します。
6. リソース CIDR の移動先のスコープを選択します。
7. [Move scope] (スコープの移動) を選択します。

Command line

プールを変更するには、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. 現在のスコープ内のリソース CIDR を取得: get-ipam-pool-cidrs
3. リソース CIDR を移動: modify-ipam-resource-cidr
4. 他のスコープ内のリソース CIDR を取得: get-ipam-pool-cidrs

リソース 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、リソース CIDR のモニタリング状態を変更します。IPAM でリソースを管理またはモニタリングせず、リソースに割り当てられた CIDR を使用できるようにする場合は、リソース CIDR をモニタリング対象から無視に変更できます。IPAM でリソース CIDR を管理またはモニタリングする場合は、リソース CIDR を無視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リソースを無視することはできません。

リソース CIDR のモニタリング状態を、モニタリング対象または無視に変更できます。

- モニタリング対象：リソース 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: 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、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。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)。

AWS Management Console

リソースに割り当てられた単一の CIDR のモニタリングステータスを変更するには以下のようにします。

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、[Resources] (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、リソースを選択し、リソースの詳細を表示します。
5. [関連付けられた CIDR] で、リソースに割り当てられた CIDR の 1 つを選択し、[アクション]、[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] 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。

リソースに割り当てられたすべての CIDR のモニタリングステータスを変更するには以下のようにします。

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、[Resources] (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、モニタリング状態を変更するリソースを選択します。
5. [アクション]、[関連付けられているすべての CIDR を無視対象としてマークする] または [関連付けられているすべての CIDR の無視対象のマークを解除する] 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

以下の AWS CLI コマンドを使用して、リソース 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. リソースの現在のモニタリング状態を表示します。get-ipam-resource-cidrs

3. リソース CIDR の状態を変更します。modify-ipam-resource-cidr
4. リソースの新しいモニタリング状態を表示します。get-ipam-resource-cidrs

スコープを削除する

IPAM スコープを削除するには、このセクションのステップに従います。

Important

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 (p. 23)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 リファレンスドキュメントに関連しています。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。

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 (p. 24) 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 (p. 29) を参照してください。

割り当ての解除

IPAM プールから CIDR 割り当てを解除するには、このセクションのステップに従います。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。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。詳細については、「リソース CIDR のモニタリング状態を変更する (p. 26)」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

  の例

  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 (p. 71) 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 (p. 86) 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 (p. 6)または複数アカウント使用 (p. 5)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。CIDR が次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。プールと割り当ての詳細については、IPAM の仕組み (p. 2) 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 (p. 2) 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 つ以上の割り当てを選択し、[Deallocate CIDRs] (CIDR の割り当て解除) を選択します。
7. [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 リファレンスドキュメントに関連しています。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。

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、CIDR を割り当てる (p. 15) 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 (p. 22) を実行する必要があります。

IPAM を削除する

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 (p. 109) を参照してください。

Important

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. 次のいずれかを実行します。
   - [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 (p. 27)」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 (p. 22)」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 (p. 27)」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 (p. 23)」を参照してください。
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 リファレンスドキュメントに関連しています。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。

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 (p. 7) を参照してください。

IPAM での IP アドレス使用状況の追跡

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。

IP アドレス使用率を IPAM で追跡するには、このセクションのステップに従います。

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

このセクションのステップに従って、IPAM ダッシュボードにアクセスし、特定の IPAM スコープ内のすべての CIDR のステータスを表示します。

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 (p. 2)を参照してください。
4. 次のセクションでモニタリングデータを表示します。

   - [Scope] (スコープ): このスコープの詳細。
     - [Scope ID] (スコープ ID): このスコープのID。
     - [Description] (説明): スコープの説明 (オプション)
     - [IPAM ID]: スコープが属している IPAM の ID。
     - [Scope type] (スコープタイプ): スコープのタイプ。
   - [Summary] (概要): カテゴリごとの CIDR の数。
     - [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。
     - [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)。
  - [Pools] (プール): スコープ内のプールの数。
  - [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。
  - [Overlapping CIDRs] (重複しているCIDR): スコープ内のプール内で重複しているリソース 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。
- [Compliant vs. noncompliant CIDRs] (準拠 CIDR と非準拠 CIDR): スコープ内の準拠している CIDR と準拠していない CIDR の数
- [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。
- [Pool assignment] (プール割り当て): スコープ内のリソースおよび手動割り当てに割り当てられた IP スペースの割合。
- [Pool allocation] (プール割り振り) : スコープ内の他のプールに割り振られているプールの 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。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。詳細については、「CIDR をプールにプロビジョニングする (p. 21)」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

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、他のリソースのみをモニタリングします。

- 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。
  - VPC
  - パブリック IPv4 プール

    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。
- 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。

- VPC
- パブリック IPv4 プール
- VPC サブネット
- Elastic IP アドレス
- サブネット予約

次のステップは、リソースごとの CIDR の使用状況および割り当てルールのコンプライアンスをモニタリングする方法を示しています。

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、[Resources] (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。スコープの詳細については、IPAM の仕組み (p. 2)を参照してください。
4. 次のセクションでモニタリングデータを表示します。

   - [Resource ID] (リソース ID): スコープの ID。
   - [Management state] (管理状態): リソースの状態。
     - [Managed] (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。
     - [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をモニタリングされていません。CIDR は重複についてモニタリングされます。
     - [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。
   - [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。
     - [Compliant] (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をモニタリングされていません。CIDR は重複についてモニタリングされます。
     - [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。
- [Overlap status] (重複ステータス): CIDR の重複ステータス。
    - [Nonoverlapping] (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。
    - [overlapping] (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、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、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。
- [Resource name] (リソース名): リソースの名前。
- [IP usage] (IP 使用状況): VPC のリソースの場合、これはサブネット CIDR によって使用されている VPC 内の IP アドレス空間の割合です。サブネットのリソースで、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。
- [CIDR]: リソースに関連付けられている CIDR。
- [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。
- [Pool ID] (プール ID): リソースが存在する IPAM プールの ID。

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、IPAM の IP アドレス使用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。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。アラームの作成と通知の設定は、このユーザーガイドの範囲外です。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 プールメトリクス

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、トップレベルプールを作成する (p. 10)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、トップレベルプールを作成する (p. 10)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

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。
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	スコープ内のプール内で重複しているリソース CIDR の数。
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 メトリクスをフィルタリングするため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。
[Locale] (国)	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。
ScopeID	スコープの ID。

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 履歴インサイト機能を使用して 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。

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 historical insights] (IP 履歴インサイト) を選択します。
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。

   > **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。
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。

- 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 履歴インサイト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 履歴インサイト内でこの VPC の ID を検索する場合、VPC の CIDR のサンプル終了時間は午後 5 時 5 分であり、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。
  - [Compliant] (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をモニタリングされていません。CIDR は重複についてモニタリングされます。
  - [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。
- [Overlap status] (重複ステータス): CIDR の重複ステータス。
  - [Nonoverlapping] (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。
  - [overlapping] (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、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、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)。
- [CIDR]: このリソースに関連付けられている CIDR。
- [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)。

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 を取得するには、IPAM へのアクセス (p. 4)を参照してください。これらのチュートリアルで説明されている IPAM の概念の詳細については、IPAM の仕組み (p. 2)を参照してください。

内容

チュートリアル: AWS CLI を使用して IPAM を作成し、プールを作成し、VPC を割り当てる

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、プールを作成し、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 (p. 109)」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。

目次

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 と統合する (p. 5) 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 (p. 7)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。プールのロケールが `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 (p. 21)」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"
        }
    ]
}
```

[Step 5.](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 と統合する (p. 5)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 (p. 19)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 を削除する。

```
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 履歴インサイト機能を使用して 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 (p. 35) 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 (p. 35)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 (p. 35)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 (p. 35)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 (p. 35)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 (p. 35)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 (p. 35)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 組織の一部ではない 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 組織の一部ではない 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: BYOIP アドレス CIDR を IPAM へ

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 を配布することがで

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。

Important

このチュートリアルのステップを完了するには、まず Linux インスタンス用 Amazon EC2 ユーザーガイドを使用して、AWS および IPAM に取り込みたい CIDR 範囲に対して次のステップを完了する必要があります。これらのステップが完了したら、このチュートリアルを続けてください。

Amazon がお客様の IP アドレス範囲をアドバタイズすることを許可するには、次の手順に従います。

1. RIR に ROA オブジェクトを作成します。これには、「キーペアと証明書を作成する」の説明に従ってキーペアを作成する必要がある場合があります。

   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。仮に最大長を `/23` に設定した場合、大きなブロックから `/24` を分割してアドバタイズ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. RIR の RDAP レコードを更新します。

これらの手順に従って、証明書を作成し、お客様が Amazon で使用したい IP アドレス範囲を所有していることを、Amazon が確認できるようにします。

1. キーペアと証明書を作成します。これは、ROA オブジェクトの作成に使用されるキーペアと同じものではなく、Amazon の検証のみを目的とした新しいキーペアです。
2. RIR に ROA オブジェクトを作成します。

   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。仮に最大長を `/23` に設定した場合、大きなブロックから `/24` を分割してアドバタイズ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。

目次

AWS マネジメントコンソールと AWS CLI の両方を使用して、独自のパブリック 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、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。

Important

このチュートリアルのステップを完了するには、まず Linux インスタンス用 Amazon EC2 ユーザーガイドを使用して、AWS および IPAM に取り込みたい CIDR 範囲に対して次のステップを完了する必要があります。これらのステップが完了したら、このチュートリアルを続けてください。

Amazon がお客様の IP アドレス範囲をアドバタイズすることを許可するには、次の手順に従います。

1. RIR に ROA オブジェクトを作成します。これには、「キーペアと証明書を作成する」の説明に従ってキーペアを作成する必要がある場合があります。

   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。仮に最大長を `/23` に設定した場合、大きなブロックから `/24` を分割してアドバタイズ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. RIR の RDAP レコードを更新します。

これらの手順に従って、証明書を作成し、お客様が Amazon で使用したい IP アドレス範囲を所有していることを、Amazon が確認できるようにします。

1. キーペアと証明書を作成します。これは、ROA オブジェクトの作成に使用されるキーペアと同じものではなく、Amazon の検証のみを目的とした新しいキーペアです。
2. RIR に ROA オブジェクトを作成します。

   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。仮に最大長を `/23` に設定した場合、大きなブロックから `/24` を分割してアドバタイズ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。

目次

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 と統合する (p. 5).
  - IPAM を作成する (p. 7).
- 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 と統合する (p. 5) 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。

目次

ステップ 1: AWS CLI 名前付きプロファイルを作成

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 名前付きプロファイルを使用して、1 つの AWS アカウント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 IAM アクセスキー ID とシークレットアクセスキーのコレクションであり、ローカルに保存し、AWS CLI を使用するときに `--profile` オプションを使用して参照します。AWS アカウントの IAM アクセスキーを作成または取得する方法の詳細については、AWS Identity and Access Management ユーザーガイドの IAM ユーザーのアクセスキーの管理を参照してください。

AWS コマンドラインインターフェイスユーザーガイドの名前付きプロファイルを作成に記載されているステップを実行して、このチュートリアルで使用する 3 つの AWS アカウントのそれぞれに対して名前付きプロファイルを 1 つずつ作成します。

- 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。

名前付きプロファイルを作成したら、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、[Pools] (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 (p. 2)」を参照してください。
4. [Create pool] (プールの作成) を選択します。
5. (オプション) プールの [Name tag] (名前タグ) とプールの [Description] (説明) を追加します。
6. [Source pool] (ソースプール) で、[No source pool] (ソースプールなし) を選択します。
7. [Address family] (アドレスファミリー) で、IPv4 を選択します。
8. [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。

   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。
9. [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。IPv4 CIDR を最上位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。パブリックスペースを所有していることを確認できるように、リクエストに CIDR と BYOIP メッセージ、および証明書の署名を含める必要があります。この BYOIP メッセージと証明書署名の取得方法を含めた、BYOIP の前提条件の一覧については AWS マネジメントコンソールと AWS CLI の両方を使用して、独自のパブリック IPv4 CIDR を IPAM に取り込む (p. 55) を参照してください。
10. [Use this pool to allocate CIDRs to resources such as VPCs] (このプールを使用して、VPC などのリソースに CIDR を割り当てる) のチェックを外します。
11. (オプション) プールのタグを選択します。

12. [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。BYOIP CIDR がプロビジョンされるまでに最大 1 週間かかることがあります。

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 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である必要があります。

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、[Pools] (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 (p. 2)」を参照してください。
4. [Create pool] (プールの作成) を選択します。
5. (オプション) プールの [Name tag] (名前タグ) とプールの [Description] (説明) を追加します。
6. [Source pool] (ソースプール) の下で、前のセクションで作成したトップレベルプールを選択します。
7. [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。

   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。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。
8. [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。
9. [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。CIDR を最上位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。
10. [Use this pool to allocate CIDRs to resources such as VPCs] (このプールを使用して、VPC などのリソースに CIDR を割り当てる) を選択します。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、トップレベルプールを作成する (p. 10) 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。
11. [Use this pool to allocate CIDRs to resources such as VPCs] (このプールを使用して、VPC などのリソースに CIDR を割り当てる) を選択し、このプール向け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。この

オプションを選択すると、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て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。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`** の場合に、ここに **`16`** を入力すると、このプールの新しい割り当ては、デフォルトでネットマスク長が `/16` 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] (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 4: AWS RAM を使用して AWS Organizations とのリソース共有を有効にする

AWS RAM を使用して、リージョンプールからの CIDR を Elastic IP アドレス (EIP) に割り当てたい AWS Organizations メンバーアカウントとリージョンプールを共有します。これを行う前に、AWS Organizations と RAM の統合を有効にする必要があります。

管理アカウントを使用して、AWS RAM ユーザーガイド内にあるAWS Organizations 内でリソース共有を有効にするに記載されているステップを完了します。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。RAM でリソース共有を有効にしたら、このチュートリアルの次のステップに進みます。

ステップ 5: AWS RAM を使用して、AWS Organizations メンバーアカウントとリージョンプールを共有する

AWS RAM を使用して IPAM プールを共有する (p. 19) のプロセスを完了し、AWS Organizations メンバーアカウントとリージョンプールを共有します。

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 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。

Important

リソース共有を作成する際には、以下を確認してください。

- プリンシパルが、Elastic IP アドレス向けプールから CIDR を割り当てるメンバーアカウントのアカウント ID になっている。
- AWSRAMPermissionIpamPoolByoipCidrImport 許可をプールに割り当てている。

ステップ 6: パブリック IPv4 プールの作成

パブリック IPv4 プールの作成は、IPAM で管理するためにパブリック IPv4 アドレスを AWS に取り込むのに必須のステップです。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。

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。

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 7: 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。

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-byoip-cidrs --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。

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

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 8: パブリック IPv4 プールからの Elastic IP アドレスの作成

Linux インスタンス用 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 Elastic IP アドレス (EIP) を作成します。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。

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。

ステップ 9: Elastic IP アドレスと EC2 インスタンスを関連付けます。

Linux インスタンス用 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にあるステップを実行し、EIP を EC2 インスタンスに関連付けます。AWS マネジメントコンソールで EC2 を開くときには、EC2 を関連付けた 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。

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。

ステップ 10: 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。

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、[Pools] (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 (p. 2)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 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。

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、[Pools] (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。

- Linux インスタンス用 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。

- Linux インスタンス用 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: 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

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 の最後の IP アドレスをパブリック IPv4 プールから解放します。ネットマスクに `/32` を指定して、IP アドレスを入力します。

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

出力に、プロビジョンを解除された CIDR が示されます。

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

Important

CIDR 範囲内の IP アドレスごとに、このコマンドを再実行する必要があります。CIDR が /24 の場合は、このコマンドを実行して、/24 CIDR 内に 256 個ある各 IP アドレスのプロビジョンを解除する必要があります。

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 5: 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。

ステップ 6: 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 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 7: 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。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 (p. 22) 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 8: 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。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 (p. 23) 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 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。

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 と統合する (p. 5).
  - IPAM を作成する (p. 7).
- 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 と統合する (p. 5) 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。

目次

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 (Elastic IP アドレス) 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、[Pools] (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 (p. 2)」を参照してください。
4. [Create pool] (プールの作成) を選択します。
5. (オプション) プールの [Name tag] (名前タグ) とプールの [Description] (説明) を追加します。
6. [Source pool] (ソースプール) で、[No source pool] (ソースプールなし) を選択します。
7. [Address family] (アドレスファミリー) で、IPv6 を選択します。
8. [Allow CIDRs in this pool to be publicly advertisable] (このプール内の CIDR をパブリックにアドバタイズできるようにする) が選択されていることを確認します。
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。

   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. [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 を最上位プール内のプールにプロビジョニングする場合、アドバタイズ可能な IPAM プールにプロビジョンできる最小 IPv6 CIDR は `/48` です。より具体的な CIDR (`/49` など) は許可されません。アドバタイズできない IPAM プールに取り込むことができる最小 CIDR は `/56;` です。より具体的な CIDR (`/57` など) は許可されません。パブリックスペースを所有していることを確認できるように、リクエストに CIDR と BYOIP メッセージ、および証明書の署名を含める必要があります。この BYOIP メッセージと証明書署名の取得方法を含めた、BYOIP の前提条件の一覧については AWS マネジメントコンソールと AWS CLI の両方を使用して、独自のパブリック IPv4 CIDR を IPAM に取り込む (p. 55) を参照してください。
11. [Use this pool to allocate CIDRs to resources such as VPCs] (このプールを使用して、VPC などのリソースに CIDR を割り当てる) のチェックを外します。
12. (オプション) プールのタグを選択します。
13. [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。BYOIP CIDR がプロビジョンされるまでに最大 1 週間かかることがあります。

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、[Pools] (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 (p. 2)」を参照してください。
4. [Create pool] (プールの作成) 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. [Source pool] (ソースプール) の下で、前のセクションで作成したトップレベルプールを選択します。
7. 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。
8. [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。
9. [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 を最上位プール内のプールにプロビジョニングする場合、アドバタイズ可能な IPAM プールにプロビジョンできる最小 IPv6 CIDR は `/48` です。より具体的な CIDR (`/49` など) は許可されません。アドバタイズできない IPAM プールに取り込むことができる最小 CIDR は `/56` です。より具体的な CIDR (`/57` など) は許可されません。
10. [Use this pool to allocate CIDRs to resources such as VPCs] (このプールを使用して、VPC などのリソースに CIDR を割り当てる) を選択し、このプール向け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。
      - 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。
- [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] (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。

11. (オプション) プールのタグを選択します。
12. 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: AWS RAM を使用して AWS Organizations とのリソース共有を有効にする

AWS RAM を使用して、リージョンプールからの CIDR を VPC に割り当てたい AWS Organizations メンバーアカウントとリージョンプールを共有します。これを行う前に、AWS Organizations と RAM の統合を有効にする必要があります。

このチュートリアルを続行する前に、管理アカウントで、AWS RAM ユーザーガイド内にあるAWS Organizations 内でのリソース共有の有効化にあるステップを完了しておく必要があります。RAM でリソース共有を有効にしたら、このチュートリアルの次のステップに進みます。

ステップ 4: AWS RAM を使用して、AWS Organizations メンバーアカウントとリージョンプールを共有する

AWS RAM を使用して IPAM プールを共有する (p. 19) のプロセスを完了し、AWS Organizations メンバーアカウントとリージョンプールを共有します。

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。

> **Important**
>
> リソース共有を作成する際には、以下を確認してください。
>
> - プリンシパルが、プールから CIDR を割り当てるメンバーアカウントのアカウント ID になっている。
> - AWSRAMPermissionIpamPoolByoipCidrImport 許可をプールに割り当てている。

ステップ 5: VPC を作成する

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 6: 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、[Pools] (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 (p. 2)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 7: 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、[Pools] (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 ユーザーガイド内の VPC を削除するに記載されてい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 (p. 22) 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 (p. 23) 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 への自分のパブリック IPv4 CIDR の取り込み

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。

> **Important**
>
> このチュートリアルのステップを完了するには、まず Linux インスタンス用 Amazon EC2 ユーザーガイドを使用して、AWS および IPAM に取り込みたい CIDR 範囲に対して次のステップを完了する必要があります。これらのステップが完了したら、このチュートリアルを続けてください。

Amazon がお客様の IP アドレス範囲をアドバタイズすることを許可するには、次の手順に従います。

1. RIR に ROA オブジェクトを作成します。これには、「キーペアと証明書を作成する」の説明に従ってキーペアを作成する必要がある場合があります。

   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。仮に最大長を `/23` に設定した場合、大きなブロックから `/24` を分割してアドバタイズ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. RIR の RDAP レコードを更新します。

これらの手順に従って、証明書を作成し、お客様が Amazon で使用したい IP アドレス範囲を所有していることを、Amazon が確認できるようにします。

1. キーペアと証明書を作成します。これは、ROA オブジェクトの作成に使用されるキーペアと同じものではなく、Amazon の検証のみを目的とした新しいキーペアです。
2. RIR に ROA オブジェクトを作成します。

   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。仮に最大長を `/23` に設定した場合、大きなブロックから `/24` を分割してアドバタイズ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。

目次

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 と統合する (p. 5).

  - IPAM を作成する (p. 7).
- 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 と統合する (p. 5) 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。

目次

ステップ 1: AWS CLI 名前付きプロファイルを作成

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 名前付きプロファイルを使用して、1 つの AWS アカウント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 IAM アクセスキー ID とシークレットアクセスキーのコレクションであり、ローカルに保存し、AWS CLI を使用するときに `--profile` オプションを使用して参照します。AWS アカウントの IAM アクセスキーを作成または取得する方法の詳細については、AWS Identity and Access Management ユーザーガイドの IAM ユーザーのアクセスキーの管理を参照してください。

AWS コマンドラインインターフェイスユーザーガイドの名前付きプロファイルを作成に記載されているステップを実行して、このチュートリアルで使用する 3 つの AWS アカウントのそれぞれに対して名前付きプロファイルを 1 つずつ作成します。

- 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。

名前付きプロファイルを作成したら、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 プールの作成時に口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口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。パブリックスペースを所有していることを確認できるように、リクエストに CIDR と BYOIP メッセージ、および証明書の署名を含める必要があります。この BYOIP メッセージと証明書署名の取得方法を含めた、BYOIP の前提条件の一覧については 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 (p. 70) を参照してください。

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。

Important

`--cidr-authorization-context` を追加する必要があるのは、BYOIP CIDR を最上位プールにプロビジョンするときのみです。最上位のプール内のリージョンプールについては、`--cidr-authorization-context` 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. 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-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --cidr-authorization-
context Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsMaUOP7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d65uyZZiD
hApR89Kt6GxRYOdRaNx8yt~uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --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。BYOIP CIDR がプロビジョンされるまでに最大 1 週間かかることがあります。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。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。

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 ロ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。CIDR を最上位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。

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
```

   以下の出力の例は、正しい状態を示しています。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

ステップ 7: AWS RAM を使用して AWS Organizations でのリソース共有を有効にする

AWS RAM を使用して、リージョンプールからの CIDR を VPC に割り当てたい AWS Organizations メンバーアカウントとリージョンプールを共有します。これを行う前に、AWS Organizations と RAM の統合を有効にする必要があります。

管理アカウントを使用して、AWS RAM ユーザーガイド内にあるAWS Organizations 内でリソース共有を有効にするに記載されているステップを完了します。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。RAM でリソース共有を有効にしたら、このチュートリアルの次のステップに進みます。

ステップ 8: AWS RAM を使用して、リージョンプールを AWS Organizations メンバーアカウントと共有する

AWS RAM を使用して IPAM プールを共有する (p. 19) のプロセスを完了し、リージョンプールを AWS Organizations メンバーアカウントと共有します。

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 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。

> Important
>
> リソース共有を作成する際には、以下を確認してください。
>
> - プリンシパルが、Elastic IP アドレス向けプールから CIDR を割り当てるメンバーアカウントのアカウント ID になっている。
> - AWSRAMPermissionIpamPoolByoipCidrImport 許可をプールに割り当てている。

ステップ 9: パブリック IPv4 プールの作成

パブリック IPv4 プールの作成は、IPAM で管理するためにパブリック IPv4 アドレスを AWS に取り込むのに必須のステップです。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。

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。

> 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 10: 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。

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 11: 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 12: 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 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。

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 13: 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. 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. 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": []
        }
    ]
}
```

5. CIDR の最後の IP アドレスをパブリック IPv4 プールから解放します。ネットマスクに /32 を指定して、IP アドレスを入力します。CIDR 範囲内の IP アドレスごとに、このコマンドを再実行する必要があります。CIDR が `/24` の場合は、このコマンドを実行して、`/24` CIDR 内に 256 個ある各 IP アドレスのプロビジョンを解除する必要があります。このセクションのコマンドを実行するときは、`--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 130.137.245.255/32 --profile member-account
```

   出力に、プロビジョンを解除された CIDR が示されます。

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

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、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": []
        }
    ]
}
```

7. 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-0d8f3646b61ca5987 --profile ipam-account
```

   出力に、IPAM での割り当てが示されます。

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

8. 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"

    }

}
```

9. 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。
10. 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"
    }
}
```

11. 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"

    }

}
```

12. 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"
    }
}
```

13. 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"
            }
        ],
    }
}
```

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。

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 と統合する (p. 5).
  - IPAM を作成する (p. 7).
- 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 と統合する (p. 5) 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。

目次

ステップ 1: AWS CLI 名前付きプロファイルを作成

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 名前付きプロファイルを使用して、1 つの AWS アカウント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 IAM アクセスキー ID とシークレットアクセスキーのコレクションであり、ローカルに保存し、AWS CLI を使用するときに `--profile` オプションを使用して参照します。AWS アカウントの IAM アクセスキーを作成または取得する方法の詳細については、AWS Identity and Access Management ユーザーガイドの IAM ユーザーのアクセスキーの管理を参照してください。

AWS コマンドラインインターフェイスユーザーガイドの名前付きプロファイルを作成に記載されているステップを実行して、このチュートリアルで使用する 3 つの AWS アカウントのそれぞれに対して名前付きプロファイルを 1 つずつ作成します。

- 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。

名前付きプロファイルを作成したら、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口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口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口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 を最上位プール内のプールにプロビジョニングする場合、アドバタイズ可能な IPAM プールにプロビジョンできる最小 IPv6 CIDR は `/48` です。より具体的な CIDR (`/49` など) は許可されません。アドバタイズできない IPAM プールに取り込むことができる最小 CIDR は `/56` です。より具体的な CIDR (`/57` など) は許可されません。パブリックスペースを所有していることを確認できるように、リクエストに CIDR と BYOIP メッセージ、および証明書の署名を含める必要があります。この BYOIP メッセージと証明書署名の取得方法を含めた、BYOIP の前提条件の一覧については 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 (p. 70) を参照してください。

`--cidr-authorization-context` を追加する必要があるのは、BYOIP CIDR を最上位プールにプロビジョンするときのみです。最上位のプール内のリージョンプールについては、`--cidr-authorization-context` 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. 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-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --cidr-authorization-
context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|
SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfDO0NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~Crt-
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSaDcT~tW4C
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --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。BYOIP CIDR がプロビジョンされるまでに最大 1 週間かかることがあります。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 (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-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 を最上位プール内のプールにプロビジョニングするとき、アドバタイズ可能な IPAM プールにプロビジョンできる最小 IPv6 CIDR は `/48` です。より具体的な CIDR (`/49` など) は許可されません。アドバタイズできない IPAM プールに取り込むことができる最小 CIDR は `/56` です。より具体的な CIDR (`/57` など) は許可されません。

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。

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
```

   以下の出力の例は、正しい状態を示しています。

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

ステップ 7: AWS RAM を使用して AWS Organizations でのリソース共有を有効にする

AWS RAM を使用して、リージョンプールからの CIDR を VPC に割り当てたい AWS Organizations メンバーアカウントとリージョンプールを共有します。これを行う前に、AWS Organizations と RAM の統合を有効にする必要があります。

管理アカウントを使用して、AWS RAM ユーザーガイド内にあるAWS Organizations 内でリソース共有を有効にするに記載されているステップを完了します。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。RAM でリソース共有を有効にしたら、このチュートリアルの次のステップに進みます。

ステップ 8: AWS RAM を使用して、リージョンプールを AWS Organizations メンバーアカウントと共有する

AWS RAM を使用して IPAM プールを共有する (p. 19) のプロセスを完了し、リージョンプールを AWS Organizations メンバーアカウントと共有します。

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 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。

> Important
>
> リソース共有を作成する際には、以下を確認してください。
>
> - プリンシパルが、Elastic IP アドレス向けプールから CIDR を割り当てるメンバーアカウントのアカウント ID になっている。
> - AWSRAMPermissionIpamPoolByoipCidrImport 許可をプールに割り当てている。

ステップ 9: 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 10: 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 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"
            }
        ]
    }
}
```

チュートリアル: 既存の 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。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: BYOIP アドレス CIDR を IPAM へ (p. 53) の手順を完了してください。

Important

- このチュートリアルでは、IPAM を作成する (p. 7) 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。

Note

IPAM アカウントは、AWS RAM を介してプールを BYOIP CIDR 所有者と共有し、共有リソースに `AWSRAMPermissionIpamPoolByoipCidrImport` ポリシーを含める必要があります。詳細については、「AWS RAM を使用して IPAM プールを共有する (p. 19)」を参照してください。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`

目次

ステップ 1: AWS CLI 名前付きプロファイルを作成

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 名前付きプロファイルを使用して、1 つの AWS アカウント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 IAM アクセスキー ID とシークレットアクセスキーのコレクションであり、ローカルに保存し、AWS CLI を使用するときに `--profile` オプションを使用して参照します。AWS アカウントの IAM アクセスキーを作成または取得する方法の詳細については、AWS Identity and Access Management ユーザーガイドの IAM ユーザーのアクセスキーの管理を参照してください。

AWS コマンドラインインターフェイスユーザーガイドの名前付きプロファイルを作成に記載されているステップを実行して、このチュートリアルで使用する各 AWS アカウントに対して 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。

名前付きプロファイルを作成したら、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 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 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 --ipam-scope-id ipam-
scope-0087d83896280b594 --description "top-level-pool" --locale us-west-2 --aws-service
 ec2 --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": "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: 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 CIDR 所有者アカウントによって実行する必要があります。

AWS CLI を使用して BYOIP CIDR を IPAM プールに転送するには

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

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

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

ステップ 6: 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 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. 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 --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": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "470889052924"
        }
    ]
}
```

2. 次のコマンドを実行して、BYOIP CIDR の割り当てを解除します。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。`--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 release-ipam-pool-allocation --region us-west-2 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --cidr 130.137.249.0/24 --ipam-pool-allocation-id ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46 --profile ipam-account
```

出力に、IPAM から削除された割り当てが表示されます。

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

3. 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 --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",
        "AwsService": "ec2"
    }
}
```

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。

目次

IPAM のサービスリンクロール

AWS Identity and Access Management (IAM) のサービスリンクロールを使用すると、AWS サービスがユーザーに代わって他の AWS サービスを呼び出すことができるようになります。サービスリンクロールの詳細については、IAM ユーザーガイドのサービスにリンクされたロールの使用を参照してください。

現在、IPAM には、サービスリンクロールが AWSServiceRoleForIPAM の 1 つしかありません。

サービスリンクロールによって付与されるアクセス許可

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 (p. 107)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 組織と統合する場合

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 と統合する (p. 5) する場合、各 AWS 組織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 (p. 6) 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。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。

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、サービスリンク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 (p. 22)」および「IPAM を削除する (p. 29)」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 をモニタリングする。
- 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。

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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

前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 モニタリングできます。

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 (p. 31)」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
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

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。

[Name] (名前)	デフォルト	調整可能
組織あたりの IPAM 管理者	1	なし
リージョンあたりの IPAM	1	いいえ
IPAM あたりのスコープ数	5	はい
スコープあたりのプール数	50	はい
プールごとの CIDR	50	はい
プールの深さ (プール内のプール数)	10	はい

Note

IPAM を使用して、複数の AWS Organizations のIP アドレスを管理することはできません。

Pricing

IPAM が監視するアクティブな IP アドレスに対し、1 時間ごとに課金されます。アクティブな IP アドレスは、EC2 インスタンスや Elastic Network Interface (ENI) などのリソースに割り当てられた IP アドレスとして定義されます。詳細については、IPAM の料金を参照してください。

IPAM のドキュメント履歴

次の表では、IPAM のリリースを説明しています。

特徴	説明	リリース日
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