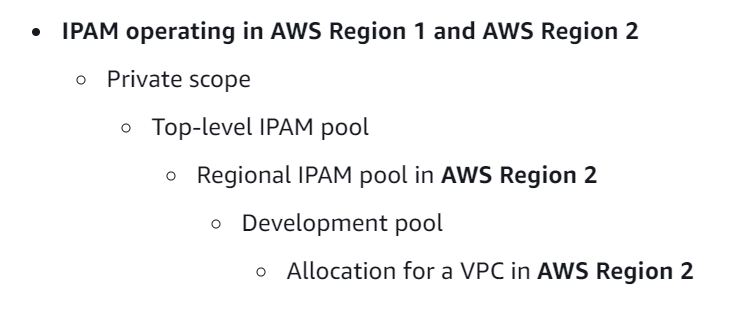
Amazon VPC IP Address Manager ワークショップ

2022/02/04

シニアエバンジェリスト 亀田

IPAMは適応されたサービス用ロールを介して、あらかじめ指定した複数リージョンにおけるVPC/SubnetのIPアドレス使用状況情報を1か所のリージョンに集約します。情報が集約されるリージョンのことをOperating Regionと呼びます。AWS Organizationとの連携により、複数AWSアカウントの情報を1か所に集約することも可能です。



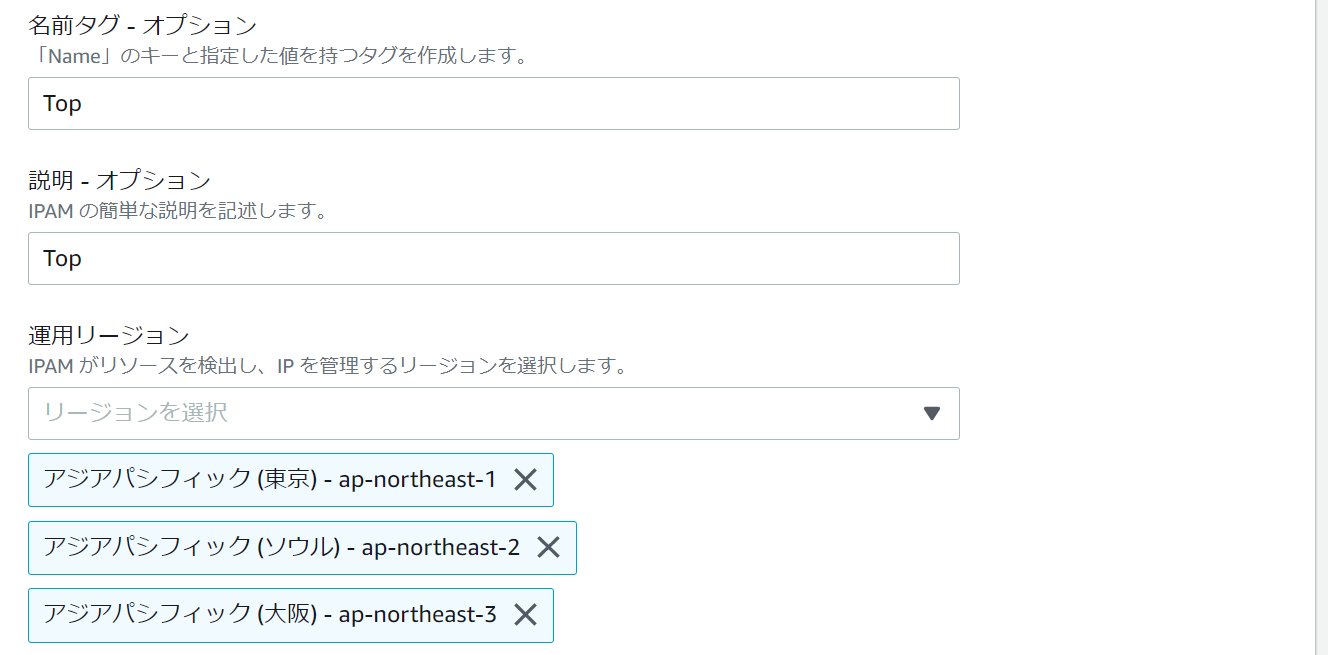
1. 作業を行うOperating Regionを決定し、Amazon VPC IP Address Managerのマネージメントコンソールにアクセスします



1. [IPAMを作成]をおします。複数AWSアカウント、複数リージョンにおけるVPCのIPアドレス使用状況を管理する台帳です。
2. [データレプリケーションを許可]にチェックをつけます

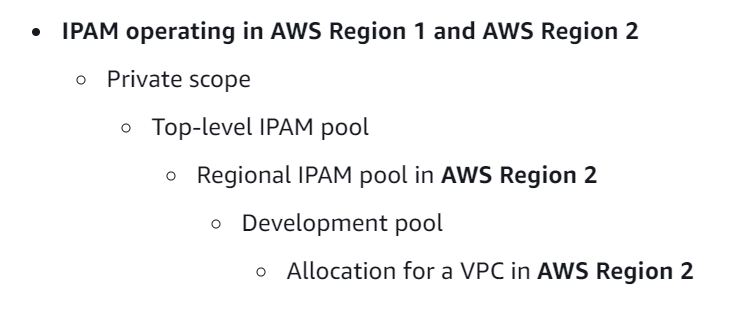


1. [名前]に[Global]と入力し、[運用リージョン]で[すべてのリージョンを選択]にチェックをつけます

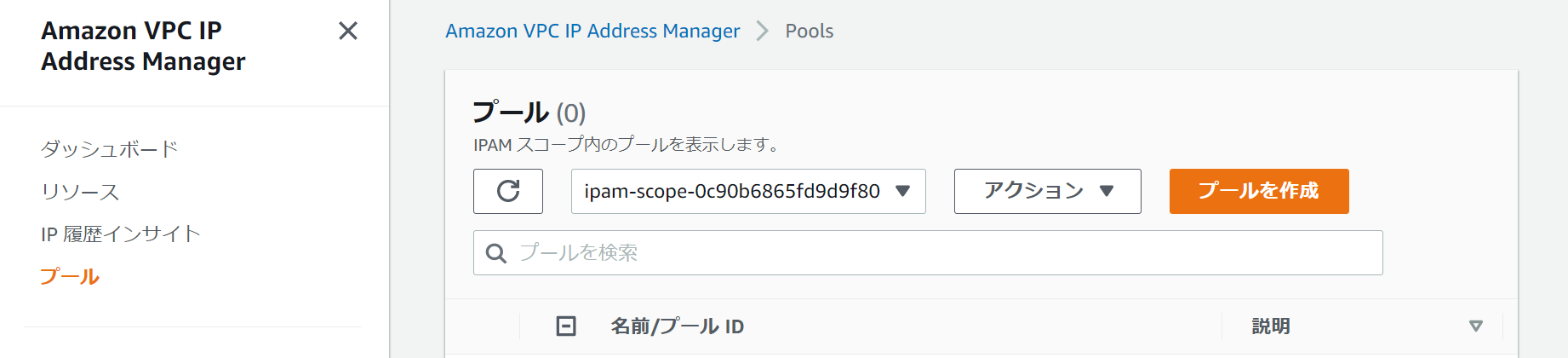


1. [IPAMを作成]ボタンをおします

今までの手順で、Globalな管理台帳が作成されました。ここからIPアドレスの管理プールを3階層作成します。それぞれTopレイヤ（複数リージョン、複数アカウント）、Regionalレイヤ（単一リージョン、単一アカウント）、特定VPCレイヤ（単一VPC）を管理するPoolを作成していきます。



1. 左ペインから[プール]をクリックし、[プールの作成]をクリックします。



1. [名前タグ]にTopと入力します



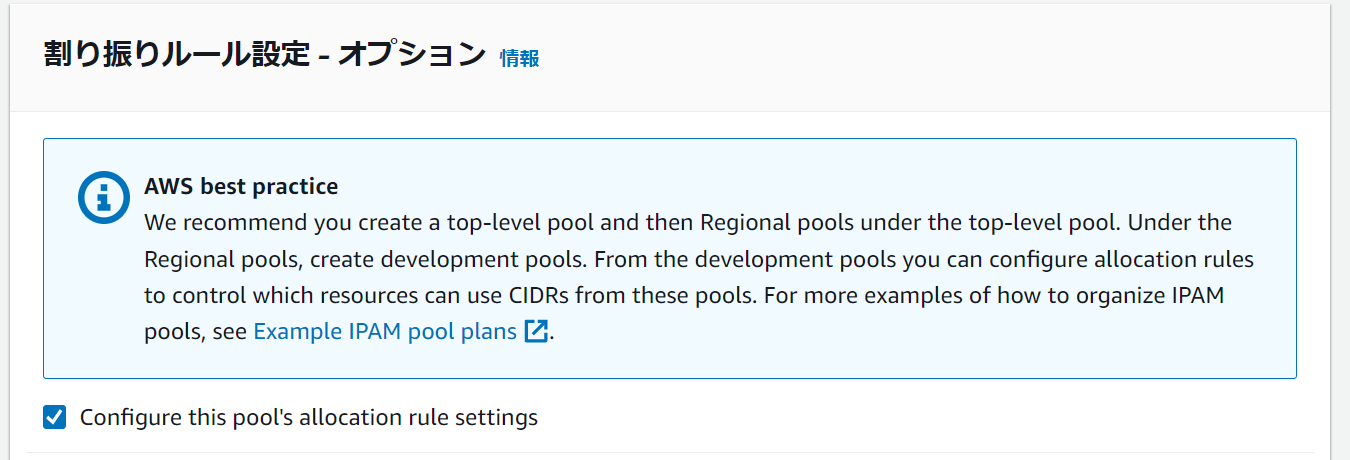
1. 以下のPool階層はデフォルトのまま作業を進めます。後ほど2次プール、3次プールの作成では指定します。



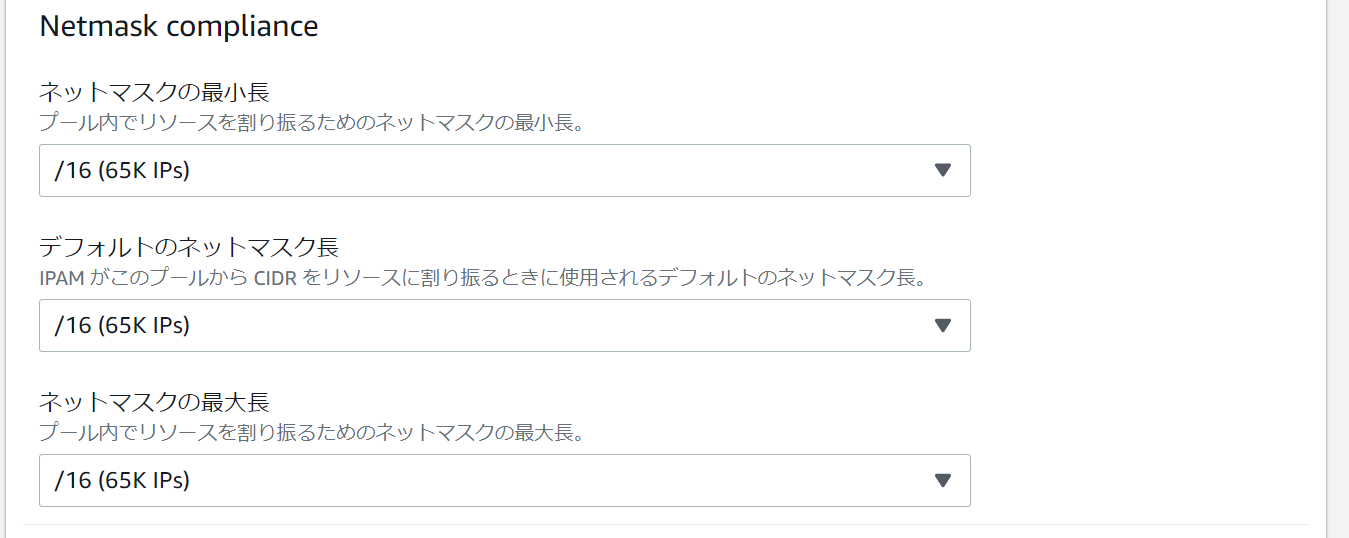
1. [新しいCIDRを追加]をおして、[10.0.0.0/8]を入力します



1. [Configure this pool's allocation rule settings]にチェックをつけます

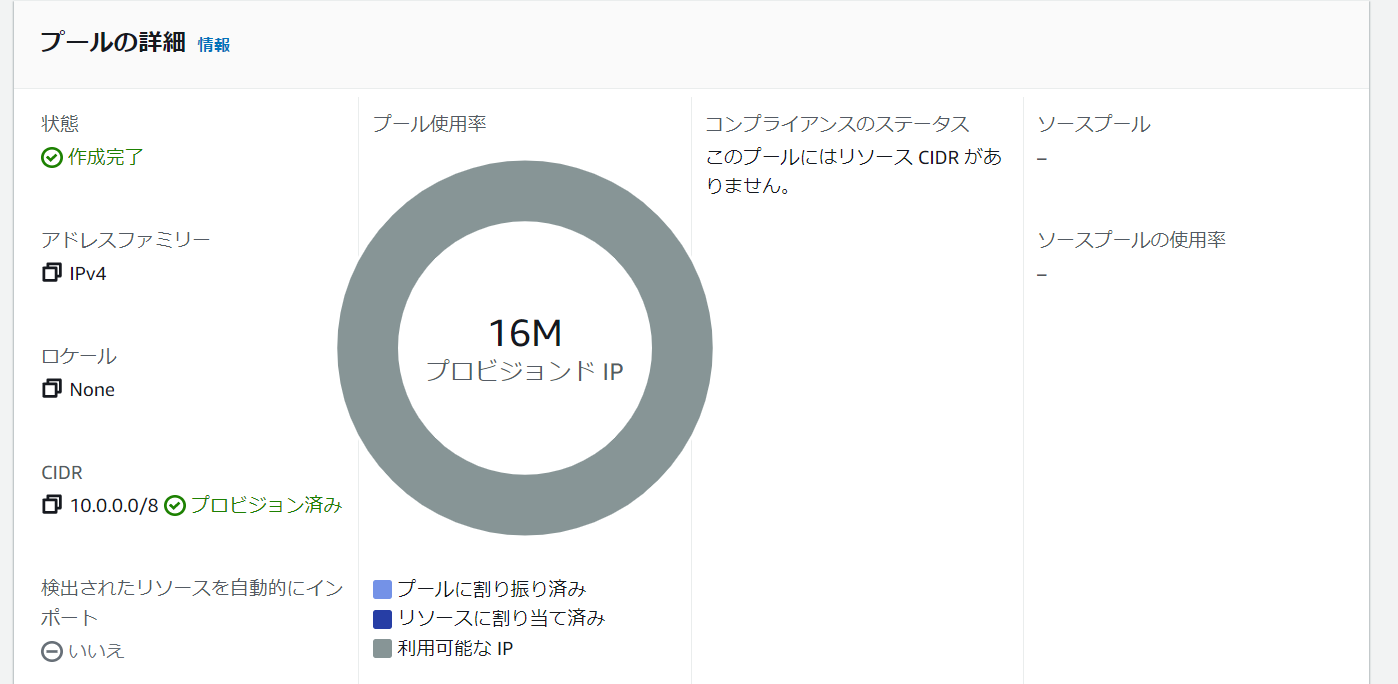


1. 以下のようにNetmask Complianceに全て/16を指定します。これにより、2次プールは/16のアドレス空間のみが作成可能となります。

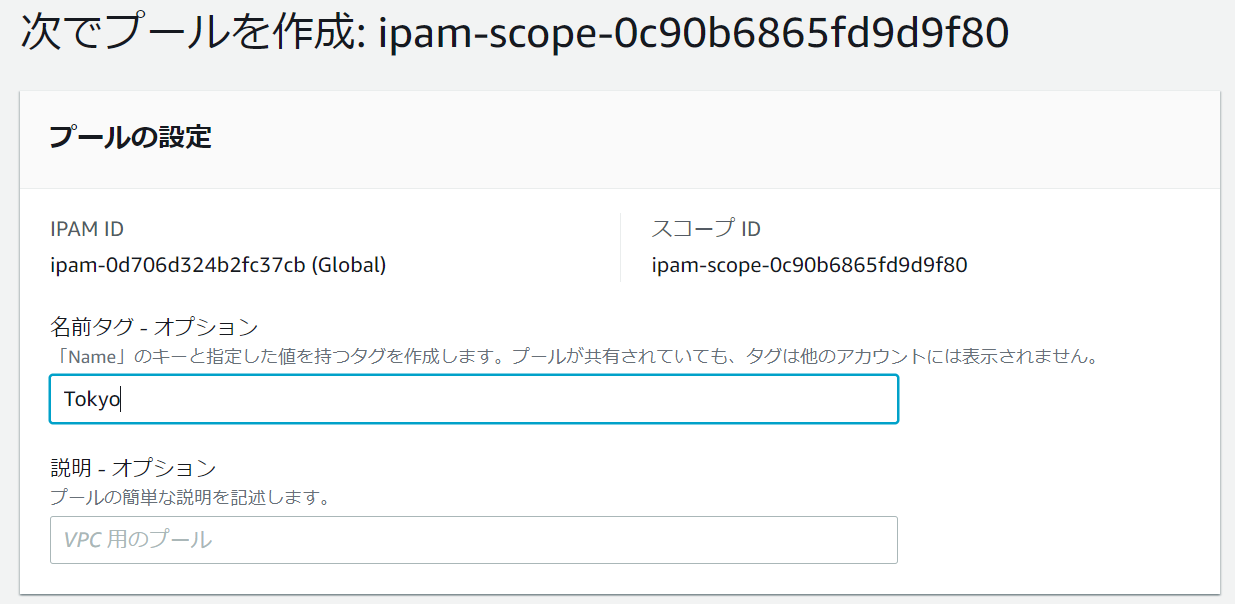


1. [プールの作成]をおします
2. 作成が完了したら、プール詳細画面の[CIDR]タブをクリックします。10.0.0.0/8が管理配下になったことがわかります。（作業完了まで数分間かかりますのでしばらく待ちます）





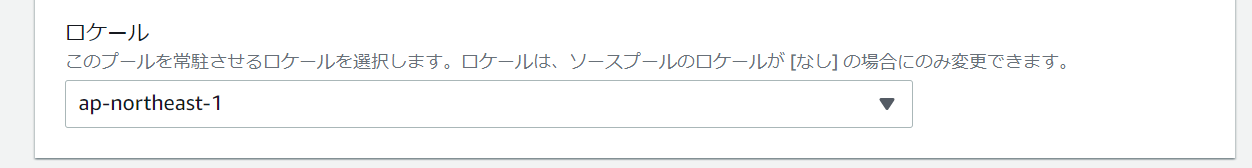
1. 再度[プールの作成]をおして2次プール（Region用）を作成します。**ここで指定するリージョンは、10.0.0.0/8 IPアドレス帯のVPCが存在しないリージョンを選択してください。すでに存在しているVPCIPアドレス帯と10.0.0.0/8が重複する場合、エラーとなります。（10.0.0.0/24 や 10.0.0.0/16 も10.0.0.0/8 の中に含まれているので重複します）**
2. Tokyo等後ほどVPCを作成するリージョンの名前を入力します



1. プール階層で先程作成した[Top]を選択します



1. [ロケール]で後ほどVPCを作成するリージョンを選びます



1. [プロビジョンする CIDR]で[特定のCIDRを追加]をおします



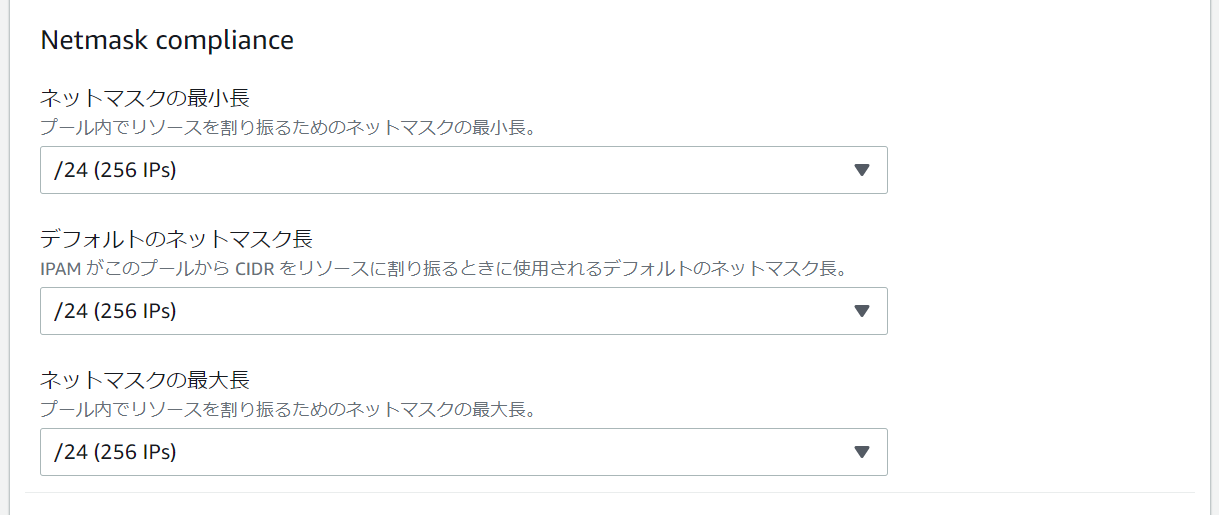
1. [10.0.0.0/16]を入力します



1. [Configure this pool's allocation rule settings]にチェックを付けます
2. [検出されたリソースを自動的にインポート]にチェックを付けます。これにより既存及び新規作成されたVPCのIPアドレス情報がIPAM上で確認できるようになります。



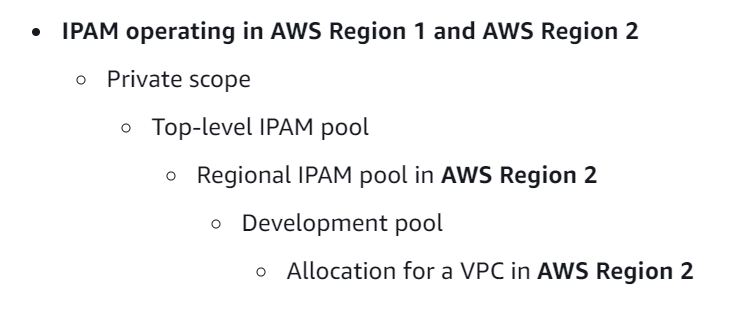
1. [Netmask Compliance]に[/24]を指定します。3次プール（VPC用）に/24を割り振ることが出来るようになります。



1. [プールを作成]をおします
2. 以下の通り2次プールが作成されています



1. ここから個別VPC用の3次プールを作成します。なおこのハンズオンの手順は以下の構造に従っていますが、階層構造は自由です。プロジェクト用プールの下に、個別リージョンごとのプールを作成することも可能です。単一プールの下に複数VPCを割り当てることも可能です。



1. [プールを作成]をおして、名前に[Dev]と入力します



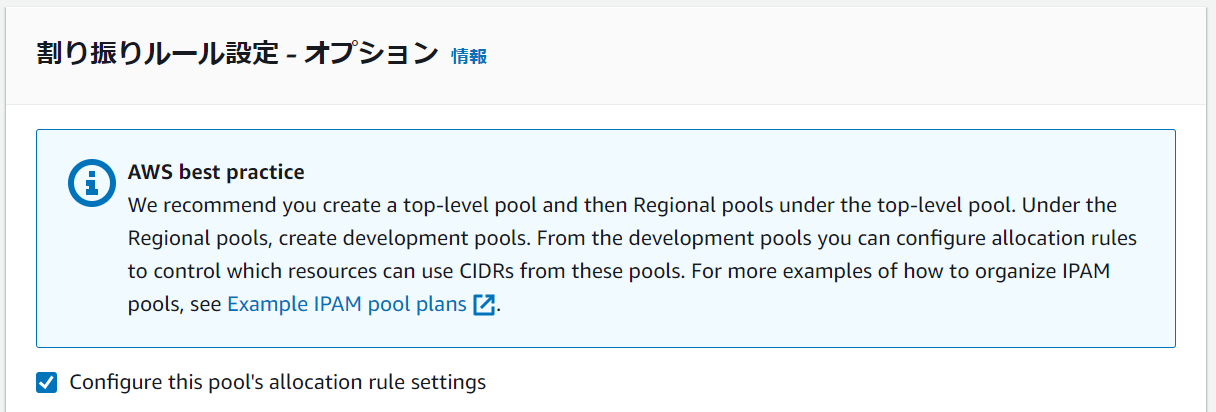
1. 2次プール（Region用）を指定します



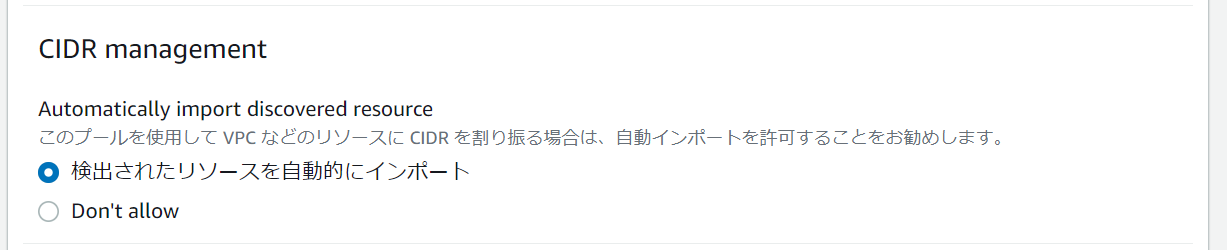
1. [特定のCIDRを追加]をおし、[10.0.0.0/24]を入力します



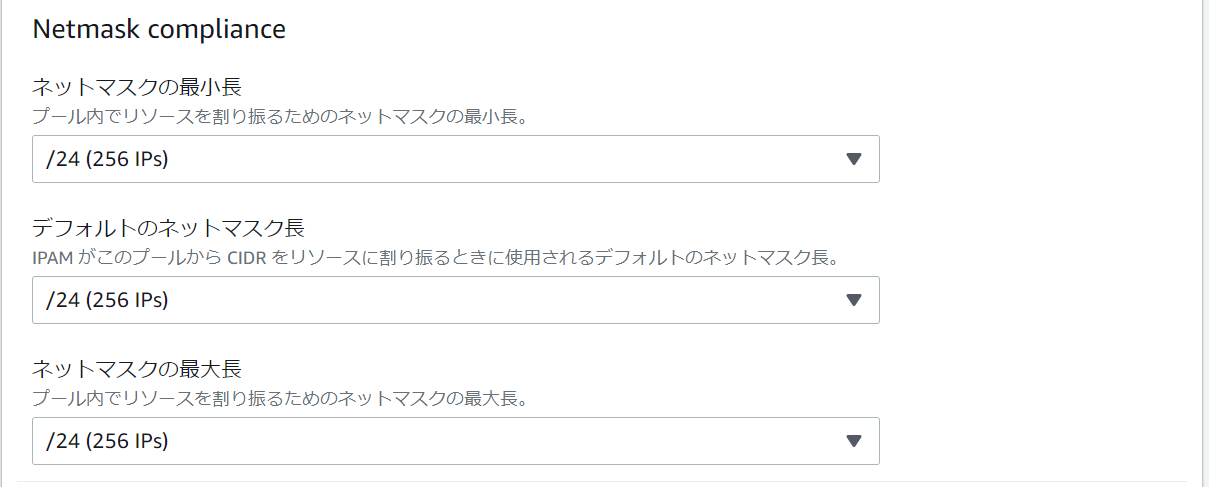
1. [Configure this pool's allocation rule settings]にチェックをつけます



1. [検出されたリソースを自動的にインポート]にチェックをつけます



1. [Netmask Compliance]で[/24]を設定します。これにより、2次プールから3次プールに割り当てられた[/24]CIDRブロックを全て割り当て可能となります。



1. [プールを作成]をおします
2. 以下のように3階層構造となっています。



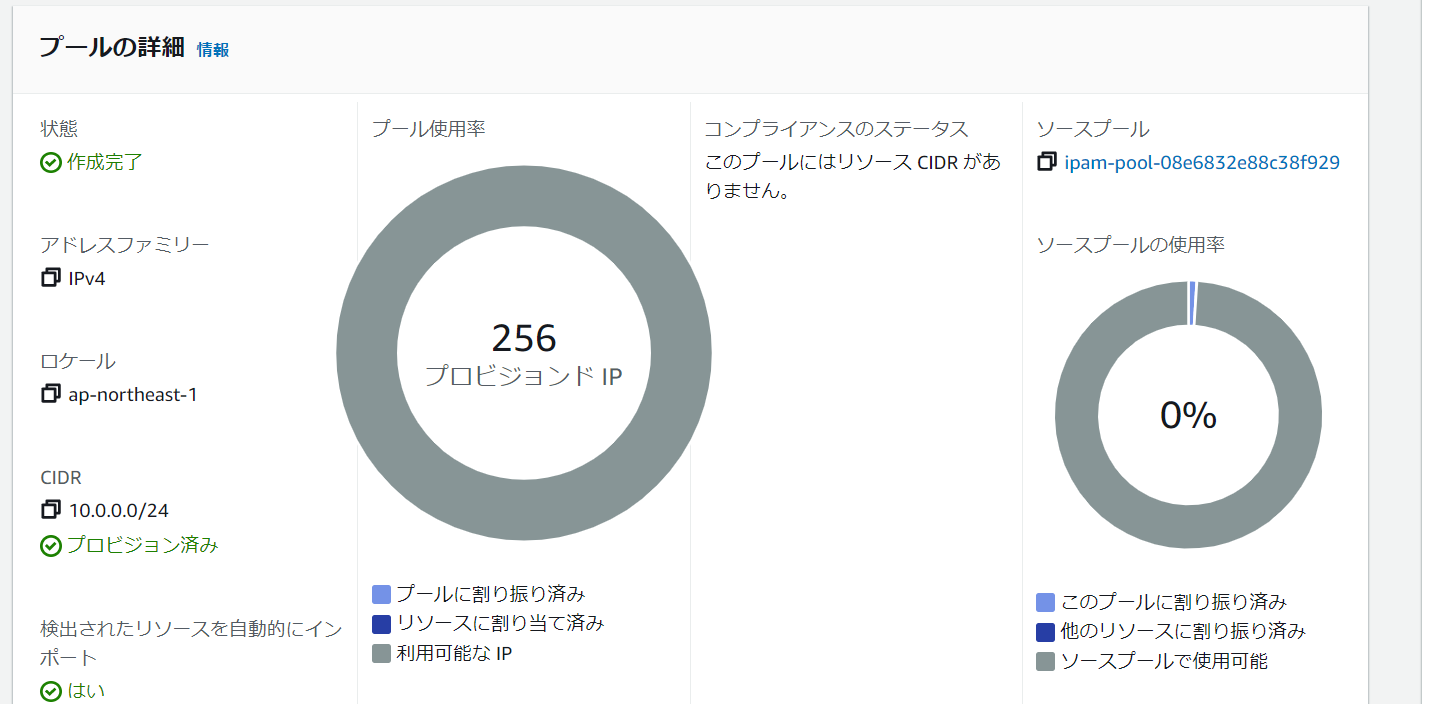
1. Devプールの詳細画面で[CIDR]タブをクリックすると以下のように正しく10.0.0.0/24がプロビジョンされているかを確認します。



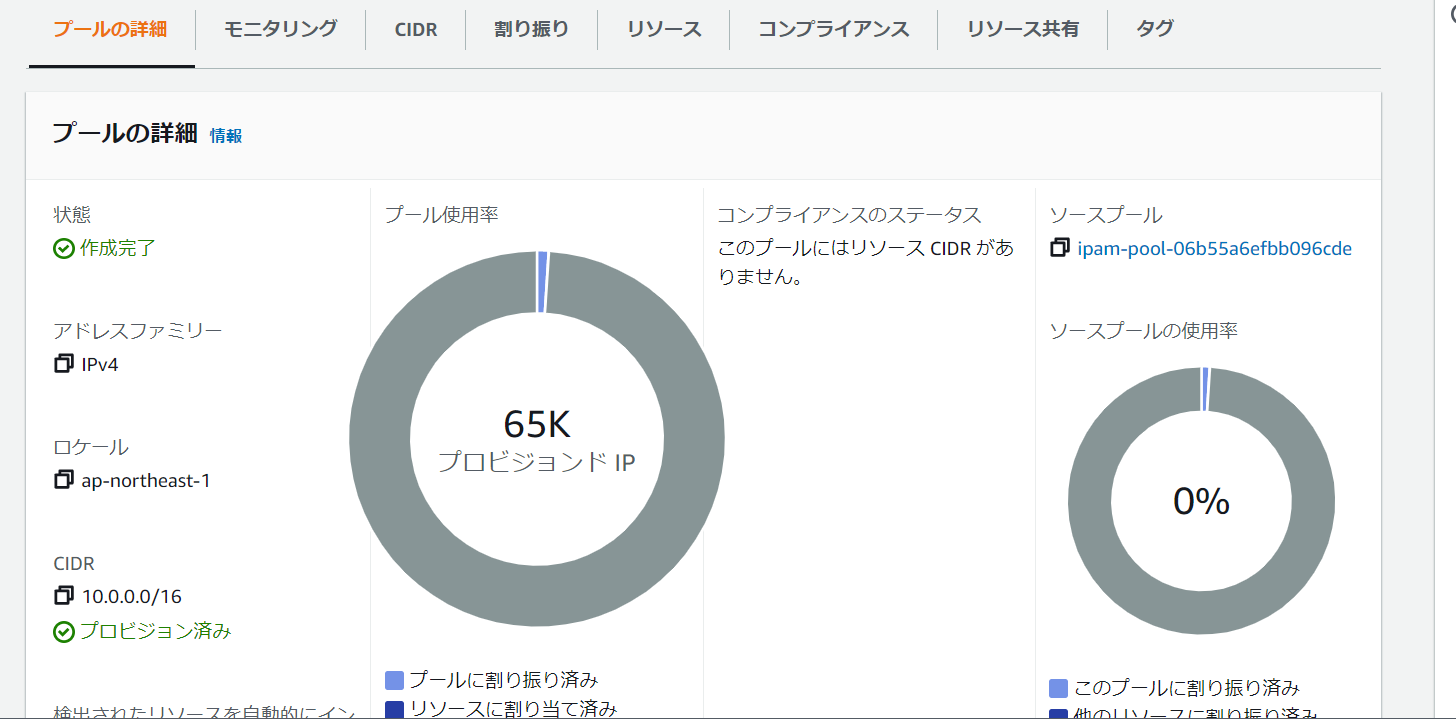
1. [割り振り]タブを確認すると、管理可能なCIDR IPアドレス帯がまだ何も割り振られていないことがわかります。



以下のように詳細画面のトップのグラフでは。/24 が利用可能なIPとして認識されています。



1. 2次プールを見ると、一部のIPがプールに割り振り済みとなっています。

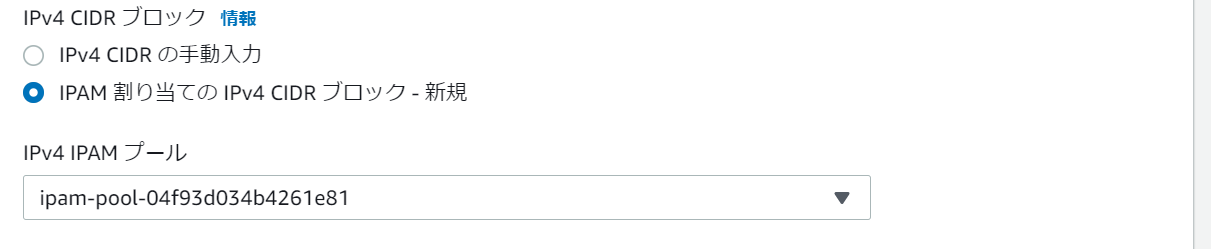




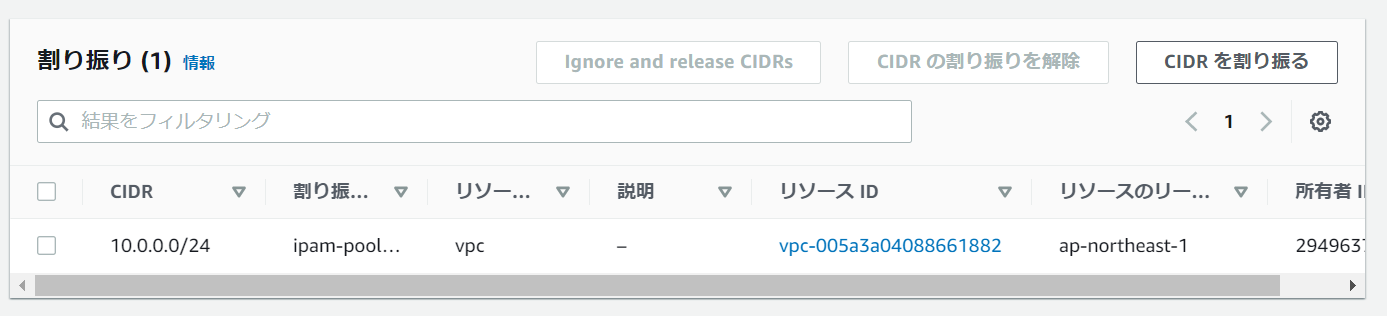
IPAMでは、そのIPアドレスが実際使用されているかどうか(EC2やELB、EIP等が利用しているか)ではなく、そのIPアドレスがVPCに割り当てられているか、下位Poolに割り振っているか、をIPアドレスが利用可能かどうかとして判断していますので注意してさい。2022/02/04現在、IPAMはVPC及びSubnetのIPアドレス割り当て状況の管理に対応していますが、VPC内部のリソース(EC2やELB、EIP等が利用しているか)のIPアドレス利用状況の管理には対応していません。

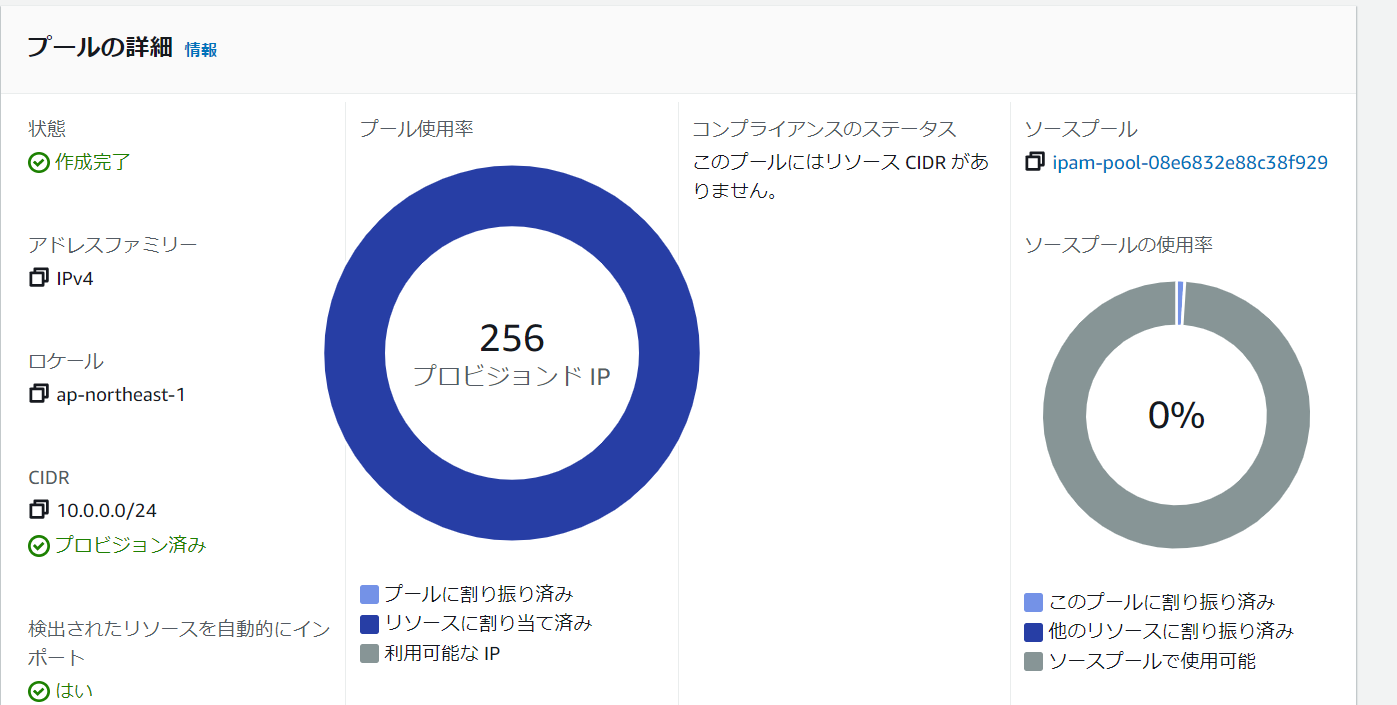
いままでの手順で作成された3次プールに割り当てられたCIDR IPアドレスブロック[10.0.0.0/24] をVPCに割り振り、VPCを作成します。

1. マネージメントコンソールからVPCの画面に移動します。2次プールで作成したリージョンで作業を行います。
2. 左ペインから[VPC]をクリックし、[VPCを作成]をおします
3. 適当な名前をつけます
4. [IPv4 CIDRブロック]で[IPAM 割り当ての IPv4 CIDR ブロック]を選択します



1. [IPv4 IPAM プール] からDev用3次プールを選びます
2. [VPCを作成]をおします
3. VPC作成後しばらく待つと、IPAMマネージメントコンソールのDevプールの詳細画面ですべてのIPアドレスが割り当て済となっていることがわかります。





この割り振りタブから、プロビジョンされているCIDR IPアドレス帯を分割してより小さいCIDR ブロックをVPC以外のリソースに利用目的で割り振りを行うことができます。（Direct Connect Gateway経由のオンプレミスIPアドレスブロック等）

1. しばらく（10-分程度待つと）リソースタブから、このプールが管理しているＩＰアドレスブロックを保有するリソース（今回の手順だとVPC）が確認できるようになります。



1. IPAMマネージメントコンソール左ペインの[リソース]をクリックすると、GlobalのIPアドレス利用状況（初期のIPAM設定時に指定した全リージョン）が一元管理できます。



VPC内部に作成されたSubnetのIPアドレスブロックが管理が可能です。注意：2022/02/04個別プール詳細画面ではSubnetに割り振ったＩＰアドレスブロックの管理が行えません。

お疲れ様でした！

以下を削除してください

・ＶＰＣ

・3次プールの割り振り→ＣＩＤＲ

・3次プール

・2次プールの割り振り→ＣＩＤＲ

・2次プール

・1次プールの割り振り→ＣＩＤＲ

・1次プール

・IPAM