IP-Adress-Manager

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: IP-Adress-Manager

Table of Contents

Was ist IPAM?

Amazon VPC IP-Adressenmanager (IPAM) ist eine VPC-Funktion, die es Ihnen erleichtert, IP-Adressen für Ihre AWS-Workloads zu planen, zu verfolgen und zu überwachen. Sie können IPAM automatisierte Workflows verwenden, um IP-Adressen effizienter zu verwalten.

Sie können den IPAM für Folgendes verwenden:

- Organisieren Sie den IP-Adressraum in Routing- und Sicherheitsdomänen
- Überwachen Sie den verwendeten IP-Adressraum und überwachen Sie Ressourcen, die Speicherplatz gegen Geschäftsregeln verwenden
- Zeigen Sie den Verlauf der IP-Adresszuweisungen in Ihrer Organisation an
- Weisen Sie CIDRs automatisch VPCs mit bestimmten Geschäftsregeln zu
- Fehlerbehebung bei Netzwerk-Verbindungsproblemen
- Aktivieren Sie regionsübergreifende und kontoübergreifende Freigabe Ihrer Bring Your Own IP (BYOIP)-Adressen
- Bereitstellen der von Amazon bereitgestellten zusammenhängenden IPv6-CIDR-Blöcke für Pools zur VPC-Erstellung

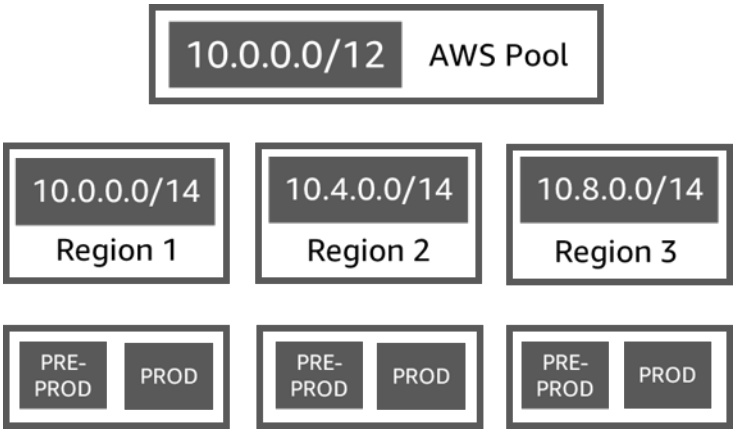
Dieses Handbuch enthält die folgenden Abschnitte:

- Funktionsweise von IPAM: IPAM-Kernkonzepte und Terminologie.
- Erste Schritte mit IPAM: Schritte zum Aktivieren der unternehmensweiten IP-Adressverwaltung mit AWS Organizations, Erstellen eines IPAMs und Planen der IP-Adressnutzung.
- Verwalten des IP-Adressraums in IPAM: Schritte zum Verwalten von IPAM, Bereichen, Pools und Zuweisungen.
- Verfolgung der IP-Adressnutzung in IPAM: Schritte zur Überwachung und Verfolgung der IP-Adressnutzung mit IPAM.
- Tutorials für Amazon VPC IP Address Manager: Detaillierte Tutorials zum Erstellen eines IPAM und von Pools, zum Zuweisen von VPC-CIDRs und zum Einbringen Ihrer eigenen CIDRs für öffentliche IP-Adressen in IPAM.

Funktionsweise von IPAM

In diesem Thema werden die wichtigsten Konzepte vorgestellt, um Ihnen den Einstieg in IPAM zu erleichtern.

Die folgende Abbildung zeigt eine IPAM-Pool-Hierarchie für mehrere AWS-Regionen innerhalb eines IPAM-Pools der obersten Ebene. Jeder AWS-regionale Pool verfügt über zwei IPAM-Entwicklungspools, einen Pool für die Vorproduktion und einen Poolproduktionsressourcen. Weitere Informationen zu IPAM-Konzepten finden Sie in den Beschreibungen unter dem Diagramm.



Um Amazon VPC IP Address Manager zu verwenden, erstellen Sie zuerst ein IPAM.

Wenn Sie ein IPAM erstellen, wählen Sie die AWS-Region aus, in der er erstellt werden soll. Wenn Sie ein IPAM erstellen, erstellt AWS-VPC-IPAM automatisch zwei Bereiche für das IPAM. Die Bereiche sind zusammen mit Pools und Allokationen Schlüsselkomponenten Ihres IPAM.

- Ein Bereich ist der Container auf höchster Ebene innerhalb von IPAM. Ein IPAM enthält zwei Standardbereiche. Jeder Bereich repräsentiert den IP-Bereich für ein einzelnes Netzwerk. Der private Bereich ist für den gesamten privaten Raum gedacht. Der öffentliche Bereich ist für den gesamten öffentlichen Raum bestimmt. Mit Bereichen können Sie IP-Adressen in mehreren nicht verbundenen Netzwerken wiederverwenden, ohne dass sich die IP-Adresse überschneidet oder Konflikte verursachen muss. In einem Bereich erstellen Sie IPAM-Pools.
- Ein Pool ist eine Sammlung von zusammenhängenden IP-Adressbereichen (oder CIDRs). IPAM-Pools ermöglichen es Ihnen, Ihre IP-Adressen entsprechend Ihren Routing- und Sicherheitsanforderungen zu organisieren. Sie können mehrere Pools in einem Pool der obersten Ebene haben. Wenn Sie beispielsweise separate Routing- und Sicherheitsanforderungen für Entwicklungs- und Produktionsanwendungen haben, können Sie für jeden einen Pool erstellen. Innerhalb von IPAM-Pools weisen Sie CIDRs zu AWS-Ressourcen zu.

- In der Zuweisung ist eine CIDR-Zuweisung von einem IPAM-Pool zu einer anderen Ressource oder einem IPAM-Pool. Wenn Sie eine VPC erstellen und einen IPAM-Pool für den CIDR der VPC auswählen, wird das CIDR aus das CIDR zugewiesen, der dem IPAM-Pool zugewiesen wurde. Sie können die Zuweisung mit IPAM überwachen und verwalten.

IPAM kann private IPv4-CIDRs, öffentliche IPv4/IPv6-CIDRs, die Ihnen gehören, und Amazon-eigenen öffentlichen IPv6-Bereich verwalten und überwachen.

Für die ersten Schritte und zum Erstellen eines IPAM, siehe Erste Schritte mit IPAM.

Erste Schritte mit IPAM

Informationen zu Ihren ersten Schritten mit IPAM sind in diesem Abschnitt beschrieben. Sie greifen zunächst auf IPAM zu und entscheiden, ob Sie ein IPAM-Konto delegieren möchten. Am Ende dieses Abschnitts haben Sie ein IPAM erstellt, mehrere Pools von IP-Adressen erstellt und einer VPC ein CIDR in einem Pool zugewiesen.

Inhalt

Zugriff auf IPAM

Wie bei anderen AWS-Services können Sie die folgenden Methoden verwenden, um Ihr IPAM zu erstellen, auf sie zuzugreifen und sie zu verwalten:

- AWS-Managementkonsole: Bietet eine Webschnittstelle für die Erstellung und Verwaltung Ihres IPAM. Weitere Informationen finden Sie unter https://console.aws.amazon.com/ipam/.
- AWS-Befehlszeilenschnittstelle (AWS-CLI): Stellt Befehle für eine breite Palette von AWS-Services bereit, einschließlich Amazon VPC. Die AWS-CLI wird unter Windows, macOS und Linux unterstützt. Um die AWS-CLI zu erhalten, siehe AWS Command Line Interface.
- AWS-SDKs: Geben Sie sprachspezifische APIs an. Die AWS-SDKs kümmern sich um viele der Verbindungsdetails, wie z. B. das Berechnen von Signaturen, die Verarbeitung von Anforderungswiederholungen und die Behandlung von Fehlern. Weitere Informationen finden Sie unter AWS-SDKs.
- Query API (Abfrage-API): bietet API-Aktionen auf niedriger Ebene, die Sie mithilfe von HTTPS-Anforderungen abrufen können. Die Verwendung der Abfrage-API ist die direkteste Möglichkeit für den Zugriff auf IPAM. Allerdings müssen dann viele technische Abläufe, wie beispielsweise das Erzeugen des Hashwerts zum Signieren der Anforderung und zur Fehlerbehandlung, in der Anwendung durchgeführt werden. Weitere Informationen finden Sie unter Amazon-IPAM-Aktionen in der Referenz zu Amazon EC2 API.

Dieser Leitfaden konzentriert sich hauptsächlich auf die Verwendung der AWS-Managementkonsole für die Erstellung von IPAM, den Zugriff darauf und deren Verwaltung. In jeder Beschreibung, wie Sie einen Prozess in der Konsole abschließen, fügen wir Links zur AWS-CLI-Dokumentation, die Ihnen zeigt, wie Sie die AWS-CLI verwenden können.

Wenn Sie zum ersten Mal IPAM verwenden, sollten Sie zum ersten Mal Funktionsweise von IPAM überprüfen, um mehr über die Rolle von IPAM in Amazon VPC zu erfahren und dann mit den Anweisungen in Konfigurieren Sie Berechtigungen für Ihr IPAM fortfahren.

Konfigurieren Sie Berechtigungen für Ihr IPAM

Bevor Sie mit der Verwendung von IPAM beginnen, müssen Sie eine der Optionen in diesem Abschnitt auswählen, damit IPAM CIDRs überwachen kann, die mit EC2-Netzwerkressourcen und Speicher-Metriken verknüpft sind:

- Informationen zum Aktivieren von IPAM für die Integration mit AWS Organizations, damit der Amazon VPC-IPAM-Service Netzwerkressourcen verwalten und überwachen kann, die von allen Mitgliedskonten der AWS Organizations erstellt wurden, finden Sie unter Integrieren von IPAM mit Konten in einer - AWS Organisation.
- Informationen AWS Organizationszur Integration von IPAM mit Konten außerhalb Ihrer Organisation finden Sie unter Integrieren von IPAM mit Konten außerhalb Ihrer Organisation.
- Um ein einzelnes AWS-Konto mit IPAM zu verwenden und den Amazon-VPC-IPAM-Service zu aktivieren, um die Netzwerkressourcen zu verwalten und zu überwachen, die Sie mit dem einzelnen Konto erstellen, siehe Verwenden Sie IPAM mit einem einzigen Konto.

Wenn Sie keine dieser Optionen auswählen, können Sie dennoch IPAM-Ressourcen wie Pools erstellen, aber Sie werden keine Metriken in Ihrem Dashboard sehen und Sie können den Status von Ressourcen nicht überwachen.

Inhalt

Integrieren von IPAM mit Konten in einer - AWS Organisation

Optional können Sie die Schritte in diesem Abschnitt ausführen, um IPAM in AWS Organizations zu integrieren und ein Mitgliedskonto als IPAM-Konto zu delegieren.

Das IPAM-Konto ist dafür verantwortlich, ein IPAM zu erstellen und es zum Verwalten und Überwachen der IP-Adressnutzung zu verwenden.

Die Integration von IPAM in AWS Organizations und die Delegierung eines IPAM-Administrators hat die folgenden Vorteile:

- Freigeben Ihrer IPAM-Pools für Ihre Organisation: Wenn Sie ein IPAM-Konto delegieren, ermöglicht IPAM anderen Mitgliedskonten von AWS Organizations in der Organisation, CIDRs aus IPAM-Pools zuzuweisen, die mit AWS Resource Access Manager (RAM) freigegeben werden. Weitere Informationen zur Einstellung von Organizations finden Sie unter Was ist AWS Organizations? im Benutzerhandbuch zu AWS Organizations.
- Überwachen der IP-Adressnutzung in Ihrer Organisation: Wenn Sie ein IPAM-Konto delegieren, erteilen Sie IPAM die Berechtigung, die IP-Nutzung über alle Ihre Konten hinweg zu überwachen. Daher importiert IPAM automatisch CIDRs, die von vorhandenen VPCs über andere Mitgliedskonten von AWS Organizations hinweg verwendet werden, in IPAM.

Wenn Sie ein Mitgliedskonto von AWS Organizations nicht als IPAM-Konto delegieren, überwacht IPAM Ressourcen nur in dem AWS Konto, das Sie zum Erstellen des IPAM verwenden.

Important

- Sie müssen die Integration mit AWS Organizations aktivieren, indem Sie IPAM in der - AWS Managementkonsole oder den AWS CLI-Befehl enable-ipam-organization-admin-account verwenden. Dadurch wird sichergestellt, dass die `AWSServiceRoleForIPAM`-serviceverknüpfte Rolle erstellt wird. Wenn Sie den vertrauenswürdigen Zugriff mit AWS Organizations über die AWS Organizations-Konsole oder den register-delegated-administrator AWS CLI-Befehl aktivieren, wird die `AWSServiceRoleForIPAM` serviceverknüpfte Rolle nicht erstellt und Sie können keine Ressourcen innerhalb Ihrer Organisation verwalten oder überwachen.

Note

Bei der Integration mit AWS Organizations:

- IPAM belastet Sie für jede aktive IP-Adresse, die es in den Mitgliedskonten Ihrer Organisation überwacht. Weitere Informationen zu Preisen finden Sie unter IPAM-Preise.
- Sie müssen ein Konto in AWS Organizations und ein Verwaltungskonto mit einem oder mehreren Mitgliedskonten eingerichtet haben. Weitere Informationen zu den verschiedenen Kontotypen finden Sie unter Terminologie und Konzepte im Benutzerhandbuch zu AWS Organizations. Weitere Informationen zum Einrichten einer Organisation finden Sie unter Erste Schritte mit AWS -Organizations.
- Das IPAM-Konto muss ein Mitgliedskonto von AWS Organizations sein. Sie können das AWS -Organizations-Verwaltungskonto nicht als IPAM-Konto verwenden.
- Das IPAM-Konto muss eine IAM-Rolle verwenden, der eine IAM-Richtlinie beigefügt ist, welche die Aktion `iam:CreateServiceLinkedRole` erlaubt. Wenn Sie das IPAM erstellen, erstellen Sie automatisch die AWSServiceRoleForIPAM serviceverknüpfte Rolle.
- Der dem AWS Organizations-Verwaltungskonto zugeordnete Benutzer muss eine IAM-Rolle verwenden, an die die folgenden IAM-Richtlinienaktionen angehängt sind:
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`
  - `iam:CreateServiceLinkedRole`

  Weitere Informationen zum Erstellen einer IAM-Rolle finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer im IAM-Benutzerhandbuch.
- Der Benutzer, der dem AWS Organizations-Verwaltungskonto zugeordnet ist, kann eine IAM-Rolle verwenden, an die die folgenden IAM-Richtlinienaktionen angehängt sind, um Ihre aktuellen delegierten AWS Orgs-Administratoren aufzulisten: `organizations:ListDelegatedAdministrators`

AWS Management Console

So wählen Sie ein IPAM-Konto aus

1. Öffnen Sie mit dem Verwaltungskonto von AWS Organizations die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie in der - AWS Managementkonsole die AWS Region aus, in der Sie mit IPAM arbeiten möchten.
3. Klicken Sie im Navigationsbereich auf Organization settings (Organisationseinstellungen).
4. Die Option Delegieren ist nur verfügbar, wenn Sie sich bei der Konsole als Verwaltungskonto von AWS Organizations angemeldet haben. Wählen Sie Delegate (Delegieren).
5. Geben Sie die AWS Konto-ID für ein IPAM-Konto ein. Der IPAM-Administrator muss ein Mitgliedskonto von AWS Organizations sein.
6. Wählen Sie Änderungen speichern aus.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

- Um ein IPAM-Administratorkonto mit zu delegieren AWS CLI, verwenden Sie den folgenden Befehl: enable-ipam-organization-admin-account

Wenn Sie ein Mitgliedskonto für Organizations als IPAM-Konto delegieren, erstellt IPAM automatisch eine dienstgebundene IAM-Rolle in allen Mitgliedskonten in Ihrer Organisation. IPAM überwacht die Verwendung der IP-Adresse in diesen Konten, indem es die dienstgebundene IAM-Rolle in jedem Mitgliedskonto übernimmt, die Ressourcen und ihre CIDRs erkennt und sie in IPAM integriert. Die Ressourcen in allen Mitgliedskonten können von IPAM unabhängig von ihrer Organisationseinheit gefunden werden. Wenn es beispielsweise Mitgliedskonten gibt, die eine VPC erstellt haben, sehen Sie die VPC und ihr CIDR im Abschnitt Ressourcen der IPAM-Konsole.

> **Important**
>
> Die Rolle des AWS Organizations Verwaltungskontos, das den IPAM-Administrator delegiert hat, ist jetzt abgeschlossen. Um IPAM weiterhin verwenden zu können, muss sich das IPAM-Administratorkonto bei Amazon VPC IPAM anmelden und ein IPAM erstellen.

Integrieren von IPAM mit Konten außerhalb Ihrer Organisation

In diesem Abschnitt wird beschrieben, wie Sie Ihr IPAM mit AWS-Konten außerhalb Ihrer Organisation integrieren. Um die Schritte in diesem Abschnitt auszuführen, müssen Sie die Schritte in Integrieren von IPAM mit Konten in einer - AWS Organisation bereits ausgeführt und ein IPAM-Konto delegiert haben.

Durch die Integration von IPAM mit AWS-Konten außerhalb Ihrer Organisation können Sie Folgendes tun:

- Verwalten Sie IP-Adressen außerhalb Ihrer Organisation von einem einzigen IPAM-Konto aus.
- Geben Sie IPAM-Pools mit Services von Drittanbietern, die von anderen AWS-Konten in andere AWS Organizations gehostet werden, frei.

Nachdem Sie IPAM mit AWS-Konten außerhalb Ihrer Organisation integriert haben, können Sie einen IPAM-Pool direkt für die gewünschten Konten anderer Organisationen freigeben.

Inhalt

Überlegungen und Einschränkungen

Dieser Abschnitt enthält Überlegungen und Einschränkungen für die Integration von IPAM mit Konten außerhalb Ihrer Organisation:

- Wenn Sie eine Ressourcenerkennung für ein anderes Konto freigeben, werden nur die IP-Adresse und Daten zur Überwachung des Kontostatus ausgetauscht. Sie können diese Daten vor der Freigabe mit den CLI-Befehlen get-ipam-discovered-resource-cidrs und get-ipam-discovered-accounts oder den GetIpamDiscoveredResourceCidrs- und GetIpamDiscoveredAccounts-APIs

anzeigen. Bei Ressourcenergebnissen, die Ressourcen in einer Organisation überwachen, werden keine Organisationsdaten (z. B. die Namen von Organisationseinheiten in Ihrer Organisation) freigegeben.

- Wenn Sie eine Ressourcenerkennung erstellen, überwacht die Ressourcenerkennung alle sichtbaren Ressourcen im Besitzerkonto. Wenn es sich bei dem Besitzerkonto um ein AWS-Servicekonto eines Drittanbieters handelt, das Ressourcen für mehrere seiner eigenen Kunden erstellt, werden diese Ressourcen bei der Ressourcenerkennung erkannt. Wenn das AWS-Servicekonto des Drittanbieters die Ressourcenerkennung für ein AWS-Endbenutzerkonto freigibt, hat der Endbenutzer Einblick in die Ressourcen der anderen Kunden des AWS-Drittanbieterservices. Aus diesem Grund sollte der AWS-Drittanbieterservice beim Erstellen und Freigeben von Ressourcenergebnissen Vorsicht walten lassen oder für jeden Kunden ein eigenes AWS-Konto verwenden.

Prozessübersicht

In diesem Abschnitt wird erklärt, wie Sie Ihr IPAM mit AWS-Konten außerhalb Ihrer Organisation integrieren. Es bezieht sich auf Themen, die in anderen Abschnitten dieses Handbuchs behandelt werden. Halten Sie diese Seite sichtbar und öffnen Sie die unten verlinkten Themen in einem neuen Fenster, damit Sie zur Anleitung auf diese Seite zurückkehren können.

Wenn Sie IPAM mit AWS-Konten außerhalb Ihrer Organisation integrieren, sind 4 AWS-Konten an dem Prozess beteiligt:

- Primärer Organisationsbesitzer – Das AWS Organizations-Verwaltungskonto für Organisation 1.
- IPAM-Konto der primären Organisation – Das delegierte IPAM-Administratorkonto für Organisation 1.
- Sekundärer Organisationsbesitzer – Das AWS Organizations-Verwaltungskonto für Organisation 2.
- Administratorkonto der sekundären Organisation – Das delegierte IPAM-Administratorkonto für Organisation 2.

Schritte

1. Der primäre Organisationsbesitzer delegiert ein Mitglied seiner Organisation als IPAM-Konto der primären Organisation (siehe Integrieren von IPAM mit Konten in einer - AWS Organisation).
2. Das IPAM-Konto der primären Organisation erstellt ein IPAM (siehe Erstellen eines IPAM).

3. Der sekundäre Organisationsbesitzer delegiert ein Mitglied seiner Organisation als sekundäres Organisations-Administratorkonto (siehe Integrieren von IPAM mit Konten in einer - AWS Organisation).
4. Das Administratorkonto der sekundären Organisation erstellt eine Ressourcenerkennung und gibt diese für das IPAM-Konto der primären Organisation unter Verwendung von AWS RAM (siehe Erstellen einer Ressourcenerkennung und Freigabe einer Ressourcenerkennung) frei. Die Ressourcenerkennung muss in derselben Heimatregion wie das IPAM der primären Organisation erstellt werden.
5. Das IPAM-Konto der primären Organisation akzeptiert die Einladung zur Ressourcenfreigabe mithilfe von AWS RAM (siehe Annehmen und Ablehnen von Einladungen zur Ressourcenfreigabe im AWS RAM-Benutzerhandbuch).
6. Das IPAM-Konto der primären Organisation ordnet die Ressourcenerkennung ihrem IPAM zu (siehe Zuordnung einer Ressourcenerkennung zu einem IPAM).
7. Das IPAM-Konto der primären Organisation kann jetzt IPAM-Ressourcen überwachen und/oder verwalten, die von den Konten in der sekundären Organisation erstellt wurden.
8. (Optional) Das IPAM-Konto der primären Organisation gibt IPAM-Pools für Mitgliedskonten in der sekundären Organisation frei (siehe Teilen Sie einen IPAM-Pool mit AWS RAM).
9. (Optional) Wenn das IPAM-Konto der primären Organisation die Erkennung von Ressourcen in der sekundären Organisation beenden möchte, kann es die Erkennung von Ressourcen vom IPAM-Konto trennen (siehe Aufhebung der Zuordnung einer Ressourcenerkennung).
10. (Optional) Wenn das Administratorkonto der sekundären Organisation nicht mehr am IPAM der primären Organisation teilnehmen möchte, kann es die gemeinsame Ressourcenerkennung rückgängig machen (siehe Aktualisieren einer Ressourcenfreigabe in AWS RAM im AWS RAM-Benutzerhandbuch) oder die Ressourcenerkennung löschen (siehe Löschen einer Ressourcenerkennung).

Verwenden Sie IPAM mit einem einzigen Konto

Wenn Sie sich dazu entscheiden, nicht zu Integrieren von IPAM mit Konten in einer - AWS Organisation, können Sie IPAM mit einem einzigen AWS-Konto verwenden.

Wenn Sie im nächsten Abschnitt ein IPAM erstellen, wird automatisch eine serviceverknüpfte Rolle für den Amazon-VPC-IPAM-Service in AWS Identity and Access Management erstellt. IPAM verwendet die serviceverknüpfte Rolle, um Metriken für CIDRs, die mit EC2-Netzwerkressourcen

verknüpft sind, zu überwachen und zu speichern. Weitere Informationen zur serviceverknüpften Rolle und deren Verwendung durch IPAM finden Sie unter Serviceverknüpfte Rollen für IPAM.

> **Important**
>
> Wenn Sie IPAM mit einem einzigen AWS-Konto verwenden, müssen Sie sicherstellen, dass das AWS-Konto, mit dem Sie das IPAM erstellen, eine mit einer Richtlinie verknüpften IAM-Rolle verwendet, welche die `iam:CreateServiceLinkedRole`-Aktion zulässt. Wenn Sie ein IPAM erstellen, erstellen Sie automatisch die serviceverknüpfte Rolle AWSServiceRoleForIPAM. Informationen zum Verwalten von IAM-Richtlinien finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

Sobald das einzelne AWS-Konto die Berechtigung hat, die mit dem IPAM-Service verknüpfte Rolle zu erstellen, gehen Sie zu Erstellen eines IPAM.

Erstellen eines IPAM

Um Ihre IPAM zu erstellen, führen Sie die Schritte in diesem Abschnitt aus. Wenn Sie einen IPAM-Administrator delegiert haben, sollten diese Schritte vom IPAM-Konto ausgeführt werden.

> **Important**
>
> Wenn Sie ein IPAM erstellen, werden Sie aufgefordert, IPAM zu erlauben, Daten von Quellkonten in ein IPAM-Delegiertenkonto zu replizieren. Um IPAM in AWS Organizations zu integrieren, benötigt IPAM Ihre Erlaubnis, Ressourcen- und IP-Nutzungsdetails kontoübergreifend (von Mitgliedskonten bis zum delegierten IPAM-Mitgliedskonto) und AWS-Regionen (von Betriebsregionen bis zur Heimatregion Ihres IPAMs) zu replizieren. Für IPAM-Benutzer mit einem Konto benötigt IPAM Ihre Berechtigung, Ressourcen- und IP-Nutzungsdetails in den Betriebsregionen in die Heimatregion Ihres IPAM zu replizieren.

Wenn Sie das IPAM erstellen, wählen Sie die AWS-Regionen, in denen das IPAM IP-Adress-CIDRs verwalten darf. Diese AWS-Regionen werden operating Regions (Betriebsregionen) genannt. IPAM entdeckt und überwacht Ressourcen nur in AWS-Regionen, die Sie als Betriebsregionen auswählen. IPAM speichert keine Daten außerhalb der von Ihnen ausgewählten Betriebsregionen.

Die folgende Beispielhierarchie zeigt, wie die AWS-Regionen, die Sie beim Erstellen des IPAM zuweisen, sich auf die Regionen auswirken, die für Pools verfügbar sind, die Sie später erstellen.

- IPAM arbeitet in AWS-Region 1 und AWS-Region 2
  - Privater Bereich
    - IPAM-Pool der obersten Ebene
      - Regionaler IPAM-Pool in AWS-Region 2
        - Entwicklungs-Pool
          - Zuteilung für eine VPC in AWS-Region 2

Sie können nur ein IPAM erstellen. Weitere Informationen zum Erhöhen von Kontingenten im Zusammenhang mit IPAM finden Sie unter Kontingente für Ihr IPAM.

AWS Management Console

Erstellen eines IPAM

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie in der AWS-Managementkonsole die AWS-Region, in der Sie das IPAM erstellen möchten. Erstellen Sie den IPAM in Ihrer Hauptbetriebsregion.
3. Wählen Sie auf der Service-Website Create IPAM (Eine IPAM erstellen).
4. Wählen Sie Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Replizieren von VPC aus Quellkonten in das Replizieren von Daten aus Quellkonten in das IPAM-Delegate-Konto erlauben) aus. Wenn Sie diese Option nicht wählen, können Sie kein IPAM erstellen.
5. Wählen Sie eine IPAM-Stufe. Weitere Informationen zu den in den einzelnen Kontingenten verfügbaren Features und den Kosten der Kontingente finden Sie unter Preise für Amazon VPC auf der Registerkarte „IPAM“.
6. Wählen Sie unter Operating regions (Betriebsregionen) die AWS-Regionen aus, in denen dieses IPAM Ressourcen verwalten und erkennen kann. Die AWS-Region, in der Sie Ihr IPAM erstellen, wird standardmäßig als eine der Betriebsregionen ausgewählt. Wenn Sie beispielsweise dieses IPAM in AWS-Region `us-east-1` erstellen, aber später regionale IPAM-Pools erstellen möchten, die CIDRs für VPCs in `us-west-2` bereitstellen, wählen Sie hier `us-west-2` aus. Wenn Sie eine Betriebsregion vergessen haben, können Sie zu einem späteren Zeitpunkt zurückkehren und Ihre IPAM-Einstellungen bearbeiten.

> **Note**
>
> Wenn Sie einen IPAM im Rahmen des kostenlosen Kontingents erstellen, können Sie mehrere Betriebsregionen für Ihren IPAM auswählen. Einblicke in öffentliche IPs ist jedoch das einzige IPAM-Feature, das in allen Betriebsregionen verfügbar sein wird. Sie können andere Features des kostenlosen Kontingents, wie BYOIP, nicht in allen Betriebsregionen des IPAM verwenden. Sie können sie nur in der Heimatregion des IPAM verwenden. Um alle IPAM-Features in allen Betriebsregionen nutzen zu können, erstellen Sie einen IPAM in der erweiterten Stufe.

7. Wählen Sie Create IPAM (IPAM erstellen) aus.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Erstellen, Ändern und Anzeigen von Details zu Ihrem IPAM:

1. Erstellen Sie das IPAM: create-ipam
2. Zeigen Sie das von Ihnen erstellte IPAM an: describe-ipams
3. Zeigen Sie die Bereiche an, die automatisch erstellt werden: describe-ipam-Scopes
4. Ändern Sie ein vorhandenes IPAM: modify-ipam

Wenn Sie diese Schritte ausgeführt haben, hat IPAM Folgendes ausgeführt:

- Haben Sie Ihr IPAM erstellt. Sie können das IPAM und die aktuell ausgewählten Betriebsregionen anzeigen, indem Sie im linken Navigationsbereich der Konsole IPAMs auswählen.
- Einen privaten und einen öffentlichen Bereich erstellt. Sie können die Bereiche sehen, indem Sie Scopes (Bereiche) im Navigationsbereich auswählen. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.

Planen der Bereitstellung von IP-Adressen

Führen Sie die Schritte in diesem Abschnitt aus, um die Bereitstellung von IP-Adressen mithilfe von IPAM-Pools zu planen. Wenn Sie ein IPAM-Konto konfiguriert haben, sollten diese Schritte von diesem Konto ausgeführt werden. Der Poolerstellungsprozess unterscheidet sich für Pools im öffentlichen und privaten Bereich. Dieser Abschnitt enthält Schritte zur Einrichtung eines regionalen Pools im privaten Bereich. Tutorials zu BYOIP und BYOASN finden Sie unter. Tutorials

Important

Um IPAM-Pools AWS kontenübergreifend zu verwenden, müssen Sie IPAM in AWS Organizations integrieren, da sonst einige Funktionen möglicherweise nicht richtig funktionieren. Weitere Informationen finden Sie unter Integrieren von IPAM mit Konten in einer - AWS Organisation.

In IPAM ist ein Pool eine Sammlung zusammenhängender IP-Adressbereiche (oder CIDRs). Pools ermöglichen es Ihnen, Ihre IP-Adressen entsprechend Ihren Routing- und Sicherheitsanforderungen zu organisieren. Sie können Pools für AWS Regionen außerhalb Ihrer IPAM-Region erstellen. Wenn Sie beispielsweise separate Routing- und Sicherheitsanforderungen für Entwicklungs- und Produktionsanwendungen haben, können Sie für jeden einen Pool erstellen.

Im ersten Schritt in diesem Abschnitt erstellen Sie einen Pool auf oberster Ebene. Anschließend erstellen Sie einen regionalen Pool innerhalb des Pools der obersten Ebene. Innerhalb des Regionalpools können Sie nach Bedarf zusätzliche Pools erstellen, z. B. Pools für Produktions- und Entwicklungsumgebung. Standardmäßig können Sie Pools bis zu einer Tiefe von 10 erstellen. Weitere Informationen zu IPAM-Kontigenten finden Sie unter Kontingente für Ihr IPAM.

Note

Die Ausdrücke provision (Bereitstellung) und allocate (zuweisen) werden in diesem Benutzerhandbuch und in der IPAM-Konsole verwendet. Provision (Bereitstellen) wird verwendet, wenn Sie einem IPAM-Pool einen CIDR hinzufügen. Allocate (Zuweisen) wird verwendet, wenn Sie ein CIDR aus einem IPAM-Pool mit einer Ressource verknüpfen.

Im Folgenden sehen Sie eine Beispielhierarchie der Poolstruktur, die Sie erstellen, indem Sie die Schritte in diesem Abschnitt ausführen:

- IPAM ist in AWS Region 1 und AWS Region 2 tätig
  - Privater Bereich
    - Pool auf oberster Ebene
      - Regionaler Pool in AWS Region 1
        - Entwicklungs-Pool
          - Zuteilung für eine VPC

Diese Struktur dient als Beispiel dafür, wie Sie IPAM verwenden möchten, aber Sie können IPAM verwenden, um den Anforderungen Ihrer Organisation gerecht zu werden. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden zum Amazon VPC IP Address Manager.

Wenn Sie einen einzelnen IPAM-Pool erstellen, führen Sie die Schritte in Erstellen eines IPv4-Pools der obersten Ebene aus und fahren Sie dann mit Zuweisen von CIDRs fort.

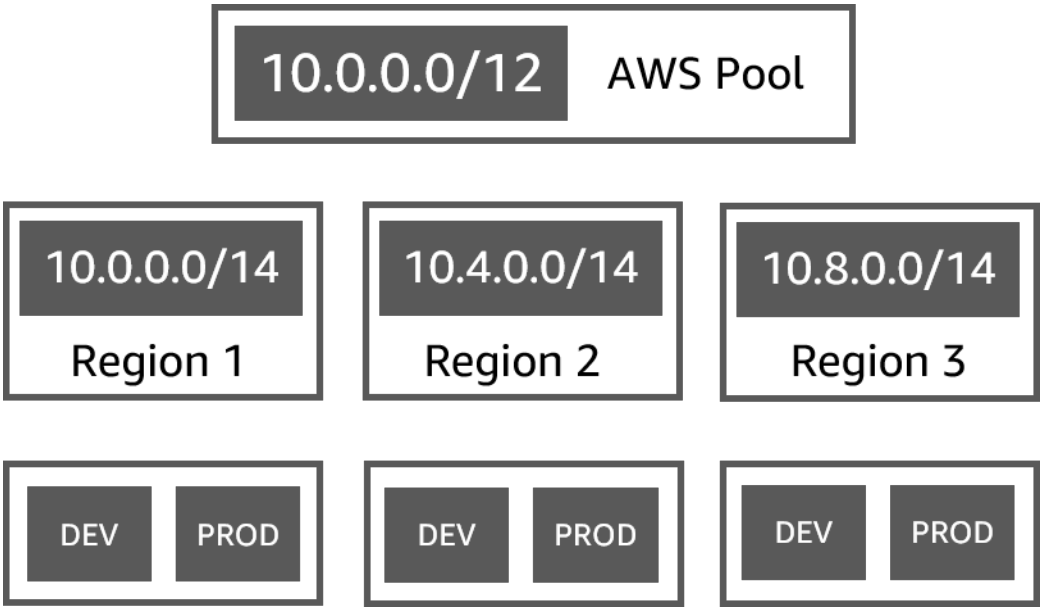
Inhalt

Beispiel für IPAM-Poolpläne

Sie können IPAM verwenden, um die Anforderungen Ihrer Organisation zu erfüllen. Dieser Abschnitt enthält Beispiele dafür, wie Sie Ihre IP-Adressen organisieren.

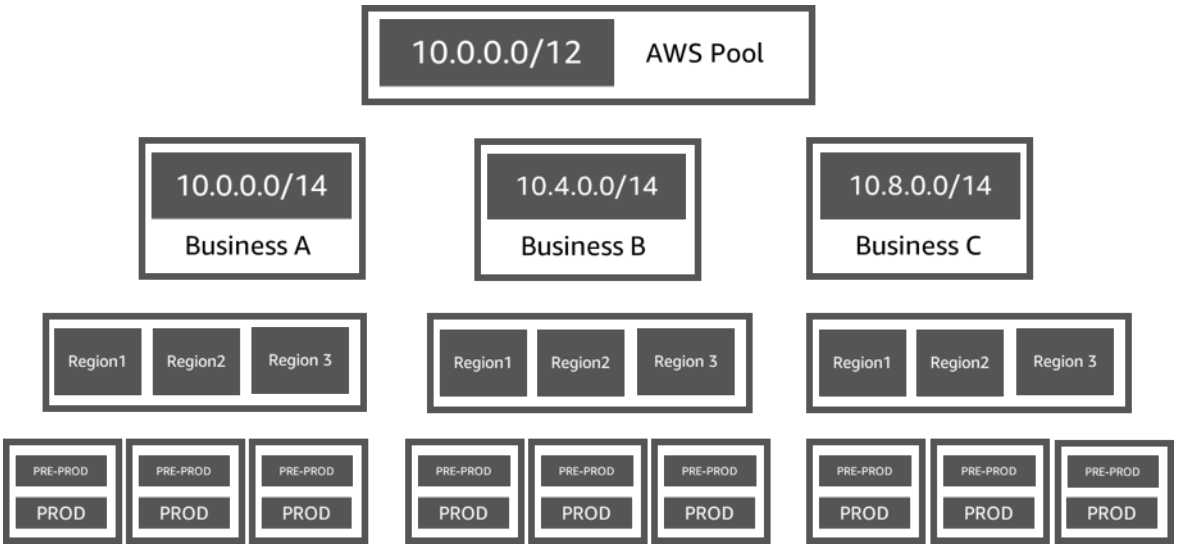
IPv4-Pools in mehreren AWS-Regionen

Das folgende Beispiel zeigt eine IPAM-Pool-Hierarchie für mehrere AWS-Regionen in einem Pool der obersten Ebene. Jeder AWS-regionale Pool verfügt über zwei IPAM-Entwicklungspools, einen Pool für Entwicklungsressourcen und einen Pool für Produktionsressourcen.



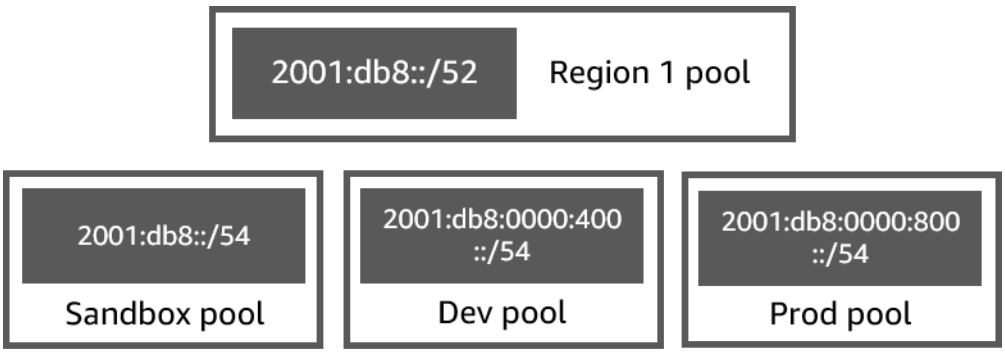
IPv4-Pools für mehrere Geschäftsbereiche

Das folgende Beispiel zeigt eine IPAM-Pool-Hierarchie für mehrere Geschäftsbereiche innerhalb eines Pools der obersten Ebene. Jeder Pool für jeden Geschäftsbereich enthält drei regionale AWS-Pools. Jeder regionale Pool verfügt über zwei IPAM-Entwicklungspools, einen Pool für Vorproduktionsressourcen und einen Pool für Produktionsressourcen.



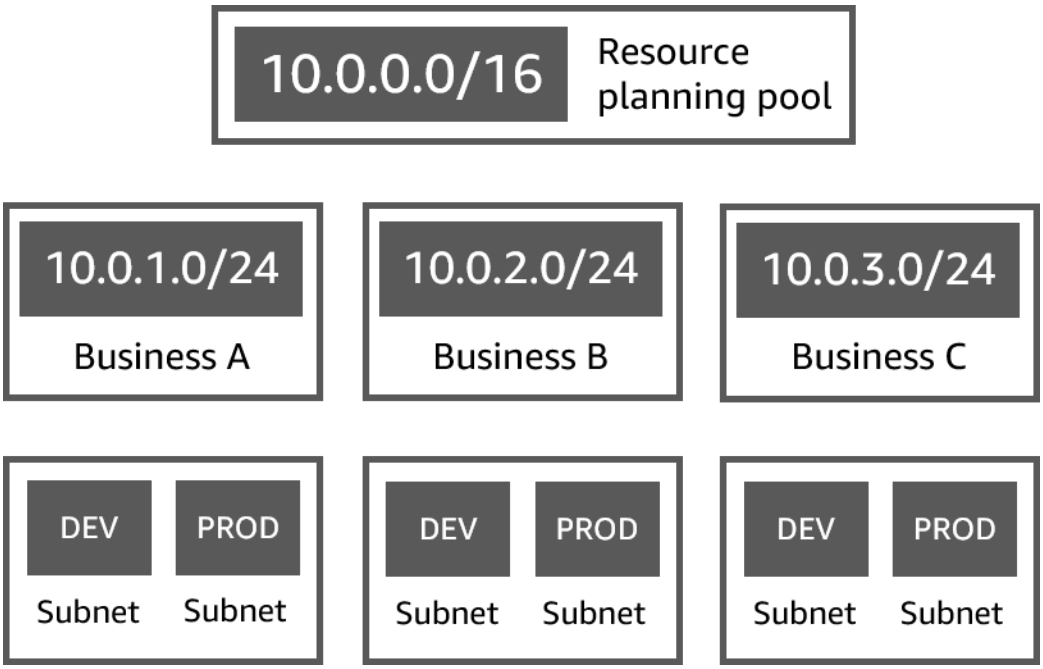
IPv6-Pools in einer AWS-Region

Das folgende Beispiel zeigt eine IPAM-IPv6-Poolhierarchie für mehrere Geschäftsbereiche innerhalb eines regionalen Pools. Jeder regionale Pool verfügt über drei IPAM-Pools: einen Pool für Sandbox-Ressourcen, einen Pool für Entwicklungsressourcen und einen Pool für Produktionsressourcen.



Subnetzpools für mehrere Geschäftsbereiche

Das folgende Beispiel zeigt eine Poolhierarchie für mehrere Geschäftsbereiche und Dev/Prod-Subnetzpools. Weitere Informationen zur Planung des IP-Adressraums in Subnetzen mithilfe von IPAM finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.



Erstellen von IPv4-Pools

Führen Sie die Schritte in diesem Abschnitt aus, um eine IPv4-IPAM-Poolhierarchie zu erstellen.

Das folgende Beispiel zeigt die Hierarchie der Poolstruktur, die Sie mit den Anweisungen in diesem Leitfaden erstellen können. In diesem Abschnitt erstellen Sie eine IPv4-IPAM-Poolhierarchie:

- IPAM operiert in AWS-Region 1 und AWS-Region 2
  - Privater Bereich

- Top-level Pool (10.0.0.0/8)
  - Regionaler Pool in AWS-Region 2 (10.0.0.0/16)
    - Entwicklungspool (10.0.0.0/24)
      - Zuweisung für eine VPC (10.0.0.0/25)

Im obigen Beispiel sind die verwendeten CIDRs nur Beispiele. Sie veranschaulichen, dass jeder Pool innerhalb des Pools der obersten Ebene mit einem Teil des CIDR der obersten Ebene bereitgestellt wird.

Inhalt

Erstellen eines IPv4-Pools der obersten Ebene

Führen Sie die Schritte in diesem Abschnitt aus, um einen IPv4-IPAM-Pool der obersten Ebene zu erstellen. Wenn Sie den Pool erstellen, stellen Sie ein CIDR bereit, das der Pool verwenden kann. Anschließend weisen Sie diesen Bereich einer Zuordnung zu. Eine Zuordnung ist eine CIDR-Zuweisung von einem IPAM-Pool zu einem anderen IPAM-Pool oder zu einer Ressource.

Das folgende Beispiel zeigt die Hierarchie der Poolstruktur, die Sie mit den Anweisungen in diesem Leitfaden erstellen können. In diesem Schritt erstellen Sie den IPAM-Pool der obersten Ebene:

- IPAM operiert in AWS-Region 1 und AWS-Region 2
  - Privater Bereich
    - Top-level Pool (10.0.0.0/8)
      - Regionaler Pool in AWS-Region 1 (10.0.0.0/16)
        - Entwicklungspool für Nicht-Produktions-VPCs (10.0.0.0/24)
          - Zuweisung für eine VPC (10.0.0.0/25)

Im obigen Beispiel sind die verwendeten CIDRs nur Beispiele. Sie veranschaulichen, dass jeder Pool innerhalb des Pools der obersten Ebene mit einem Teil des CIDR der obersten Ebene bereitgestellt wird.

Wenn Sie einen IPAM-Pool erstellen, können Sie Regeln für die Zuweisungen konfigurieren, die im IPAM-Pool vorgenommen werden.

Mit Zuweisungsregeln können Sie Folgendes konfigurieren:

- Ob IPAM CIDRs automatisch in den IPAM-Pool importieren soll, wenn es sie im CIDR-Bereich dieses Pools findet
- Die erforderliche Netzmaskenlänge für Zuweisungen innerhalb des Pools
- Die erforderlichen Tags für Ressourcen im Pool
- Das erforderliche Gebietsschema für Ressourcen innerhalb des Pools. Das Gebietsschemas ist die AWS-Region, in der ein IPAM-Pool für Zuweisungen verfügbar ist.

Zuweisungsregeln legen fest, ob Ressourcen konform oder nicht konform sind. Weitere Informationen zur Compliance finden Sie unter Überwachen Sie die CIDR-Nutzung nach Ressourcen.

> **Important**
>
> Es gibt eine zusätzliche implizite Regel, die in den Zuweisungsregeln nicht angezeigt wird. Wenn sich die Ressource in einem IPAM-Pool befindet, bei dem es sich um eine gemeinsam genutzte Ressource im AWS Resource Access Manager (RAM) handelt, muss der Ressourcenbesitzer als Prinzipal im AWS-RAM konfiguriert werden. Weitere Informationen zum Freigeben von Pools mit RAM finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM.

Im folgenden Beispiel wird gezeigt, wie Sie mit Zuteilungsregeln den Zugriff auf einen IPAM-Pool steuern können:

Example

Wenn Sie Ihre Pools basierend auf Routing- und Sicherheitsanforderungen erstellen, möchten Sie möglicherweise nur bestimmten Ressourcen erlauben, einen Pool zu verwenden. In solchen Fällen können Sie eine Allokationsregel festlegen, die besagt, dass jede Ressource, die ein CIDR aus diesem Pool wünscht, ein Tag haben muss, das den Anforderungen für das Zuordnungsregeltag entspricht. Sie können beispielsweise eine Zuweisungsregel festlegen, die angibt, dass nur VPCs mit dem Tag prod CIDRs aus einem IPAM-Pool holen können. Sie könnten auch eine Regel festlegen, die besagt, dass CIDRs, die aus diesem Pool zugewiesen werden, nicht größer als /24 sein können. In diesem Fall könnte eine Ressource weiterhin mit einem CIDR von mehr als /24 aus diesem Pool

erstellt werden, wenn der Speicherplatz verfügbar ist, aber da dies gegen eine Zuweisungsregel im Pool verstößt, markiert IPAM diese Ressource als nicht konform.

> **Important**
>
> In diesem Thema wird beschrieben, wie Sie einen IPv4-Pool der obersten Ebene mit einem von AWS bereitgestellten IP-Adressbereich erstellen. Wenn Sie Ihre eigenen IPv4-IP-Adressbereiche in AWS (BYOIP) einbringen möchten, müssen einige Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Tutorial: Mitbringen eigener IP-Adressen in IPAM.

AWS Management Console

So erstellen Sie einen Pool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie Pool erstellen.
4. Wählen Sie unter IPAM-Bereich den privaten Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.

   Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Pools im privaten Bereich müssen IPv4-Pools sein. Pools im öffentlichen Bereich können IPv4- oder IPv6-Pools sein. Der öffentliche Bereich ist für den gesamten öffentlichen Raum bestimmt.
5. (Optional) Fügen Sie Name tag (Namenstag) für den Pool und eine Beschreibung für den Pool ein.
6. Wählen Sie unter Quelle die Option IPAM-Bereich aus.
7. Wählen Sie unter Adressfamilie IPv4 aus.
8. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
9. Wählen Sie für das Locale (Gebietsschema) None (Keine) aus. Sie legen das Gebietsschema im Regionalpool fest.

Das Gebietsschema AWS-Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden.

10. (Optional) Sie können einen Pool ohne CIDR erstellen, aber Sie können den Pool erst für Zuweisungen verwenden, wenn Sie ein CIDR dafür bereitgestellt haben. Um ein CIDR bereitzustellen, wählen Sie Neues CIDR hinzufügen. Geben Sie ein IPv4-CIDR ein, das für den Pool bereitgestellt werden soll. Wenn Sie Ihre eigenen IPv4- oder IPv6-IP-Adressbereiche in AWS einbringen möchten, müssen einige Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Tutorial: Mitbringen eigener IP-Adressen in IPAM.
11. Wählen Sie optionale Zuordnungsregeln für diesen Pool aus:

    - Automatically import discovered resources (Entdeckte Ressourcen automatisch importieren): Diese Option ist nicht verfügbar, wenn Locale (Gebietsschema) auf None (Keine) gesetzt wird. Wenn diese Option ausgewählt ist, sucht IPAM kontinuierlich nach Ressourcen im CIDR-Bereich dieses Pools und importiert diese automatisch als Zuweisungen in Ihr IPAM. Beachten Sie Folgendes:
        - Die CIDRs, die für diese Ressourcen zugewiesen werden, dürfen nicht bereits anderen Ressourcen zugeordnet sein, damit der Import erfolgreich ist.
        - IPAM importiert ein CIDR unabhängig von seiner Compliance der Zuordnungsregeln des Pools, sodass eine Ressource importiert und anschließend als nicht konform gekennzeichnet wird.
        - Wenn IPAM mehrere sich überlappende CIDRs entdeckt, importiert IPAM nur das größte CIDR.
        - Wenn IPAM mehrere CIDRs mit übereinstimmenden CIDRs entdeckt, importiert IPAM zufällig nur einen von ihnen.

    > ⚠ Warning
    >
    > - Nachdem Sie ein IPAM erstellt haben, wählen Sie beim Erstellen einer VPC die IPAM-zugewiesene CIDR-Blockoption. Wenn Sie dies nicht tun, kann sich das für Ihre VPC gewählte CIDR mit einer IPAM-CIDR-Zuordnung überschneiden.

- Wenn Sie bereits eine VPC in einem IPAM-Pool zugewiesen haben, kann eine VPC mit einem überlappenden CIDR nicht automatisch importiert werden. Wenn z. B. eine VPC mit 10.0.0.0/26 CIDR in einem IPAM-Pool ist, kann eine VPC mit 10.0.0.0/23 CIDR (die 10.0.0.0/26 CIDR abdecken würde) nicht importiert werden.
- Es dauert einige Zeit, bis bestehende VPC-CIDR-Zuordnung automatisch in IPAM importiert werden.

- Minimum netmask lenght (Minimale Netzmaskenlänge): Die minimale Netzmaskenlänge, die erforderlich ist, damit CIDR-Zuweisungen in diesem IPAM-Pool konform sind, und der CIDR-Block der größten Größe, der aus dem Pool zugewiesen werden kann. Die minimale Netzmaskenlänge muss kleiner als die maximale Netzmaskenlänge sein. Mögliche Netzmaskenlängen für IPv4-Adressen sind 0 - 32. Mögliche Netzmaskenlängen für IPv6-Adressen sind 0 - 128.
- Default netmask lenght (Standardlänge für Netzmasken): Eine standardmäßige Netzmaskenlänge für Zuweisungen, die diesem Pool hinzugefügt wurden. Wenn die CIDR, die diesem Pool bereitgestellt wird, beispielsweise **`10.0.0.0/8`** ist und Sie hier **`16`** eingeben, wird für alle neuen Zuweisungen in diesem Pool standardmäßig eine Netzmaskenlänge von /16 verwendet.
- Maximum netmask lenght (Maximale Netzmaskellänge): Die maximale Netzmaskenlänge, die für CIDR-Zuweisungen in diesem Pool erforderlich ist. Dieser Wert gibt den CIDR-Block der kleinsten Größe vor, der aus dem Pool zugewiesen werden kann.
- Tagging (Markierung): Die Tags, die benötigt werden, damit Ressourcen Speicherplatz aus dem Pool zuweisen können. Wenn die Ressourcen ihre Tags geändert haben, nachdem sie Speicherplatz zugewiesen haben oder wenn die Zuordnungskennzeichnungsregeln im Pool geändert werden, wird die Ressource möglicherweise als nicht konform gekennzeichnet.
- Locale (Gebietsschema): Das Gebietsschema, das für Ressourcen benötigt wird, die CIDRs aus diesem Pool verwenden. Automatisch importierte Ressourcen, die dieses Gebietsschema nicht haben, werden als nicht konform gekennzeichnet. Ressourcen, die nicht automatisch in den Pool importiert werden, dürfen keinen Speicherplatz aus dem Pool zuweisen, es sei denn, sie befinden sich in diesem Gebietsschema.

12. (Optional) Wählen Sie Tags für den Pool.
13. Wählen Sie Pool erstellen.
14. Siehe Erstellen eines regionalen IPv4-Pools.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Erstellen oder Bearbeiten eines Pools der obersten Ebene in Ihrem IPAM:

1. Erstellen eines Pools: create-ipam-pool.
2. Bearbeiten Sie den Pool, nachdem Sie ihn erstellt haben, um die Zuordnungsregeln zu ändern: modify-ipam-pool.

Erstellen eines regionalen IPv4-Pools

Führen Sie die Schritte in diesem Abschnitt aus, um einen regionalen Pool in Ihrem Pool der obersten Ebene zu erstellen. Wenn Sie nur einen Pool der obersten Ebene und keine zusätzlichen Regional- und Entwicklungspools benötigen, fahren Sie mit Zuweisen von CIDRs fort.

> **Note**
>
> Der Poolerstellungsprozess unterscheidet sich für Pools im öffentlichen und privaten Bereich. Dieser Abschnitt enthält Schritte zur Einrichtung eines regionalen Pools im privaten Bereich. Tutorials zu BYOIP und BYOASN finden Sie unter. Tutorials

Das folgende Beispiel zeigt die Hierarchie der Poolstruktur, die Sie erstellen, indem Sie die Anweisungen in diesem Handbuch befolgen. In diesem Schritt erstellen Sie den regionalen IPAM-Pool:

- IPAM arbeitet in Region 1 und Region 2 AWS AWS
  - Privater Bereich
    - Top-level Pool (10.0.0.0/8)
      - Regionalpool in AWS Region 1 (10.0.0.0/16)
        - Entwicklungspool für Nicht-Produktions-VPCs (10.0.0.0/24)
          - Zuweisung für eine VPC (10.0.0.0/25)

Im obigen Beispiel sind die verwendeten CIDRs nur Beispiele. Sie veranschaulichen, dass jeder Pool innerhalb des Pools der obersten Ebene mit einem Teil des CIDR der obersten Ebene bereitgestellt wird.

AWS Management Console

Erstellen eines regionalen Pools im Pool der obersten Ebene

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie Pool erstellen.
4. Wählen Sie unter IPAM-Bereich denselben Bereich aus, den Sie beim Erstellen der Pools der obersten Ebene verwendet haben. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
5. (Optional) Fügen Sie Name tag (Namenstag) für den Pool und eine Beschreibung für den Pool ein.
6. Wählen Sie unter Quelle die Option IPAM-Pool aus. Wählen Sie den Pool der obersten Ebene aus, den Sie im vorherigen Abschnitt erstellt haben.
7. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
8. Wählen Sie das Gebietsschema für den Pool aus. Die Auswahl eines Gebietsschemas stellt sicher, dass es keine regionsübergreifenden Abhängigkeiten zwischen Ihrem Pool und den daraus zugewiesenen Ressourcen gibt. Die verfügbaren Optionen stammen aus den Betriebsregionen, die Sie beim Erstellen Ihres IPAM ausgewählt haben.

   Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden.

> **Note**
>
> Wenn Sie einen Pool im kostenlosen Kontingent erstellen, können Sie nur das Gebietsschema wählen, das der Heimatregion Ihres IPAM entspricht. Um alle IPAM-Feature gebietsschemaübergreifend nutzen zu können, führen Sie ein Upgrade auf das erweiterte Kontingent durch.

9. (Optional) Wählen Sie ein CIDR aus, das für den Pool bereitgestellt werden soll. Sie können einen Pool ohne CIDR erstellen, aber Sie können den Pool erst für Zuweisungen verwenden, wenn Sie ein CIDR dafür bereitgestellt haben. Sie können einem Pool jederzeit CIDRs hinzufügen, indem Sie den Pool bearbeiten.
10. Sie haben hier dieselben Zuweisungsregeloptionen wie beim Erstellen des Pools der obersten Ebene. Für eine Erläuterung der Optionen, die beim Erstellen von Pools verfügbar sind, siehe Erstellen eines IPv4-Pools der obersten Ebene. Die Zuordnungsregeln für den Regionalpool werden nicht vom Pool der obersten Ebene geerbt. Wenn Sie hier keine Regeln anwenden, werden keine Zuteilungsregeln für den Pool festgelegt.
11. (Optional) Wählen Sie Tags für den Pool.
12. Wenn Sie mit der Konfiguration Ihres Pools fertig sind, wählen Sie Create pool (Pool erstellen) aus.
13. Siehe Erstellen eines IPv4-Entwicklungspool.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI Befehle, um einen regionalen Pool in Ihrem IPAM zu erstellen:

1. Rufen Sie die ID des Bereichs ab, in dem Sie den Pool erstellen möchten: describe-ipam-scopes
2. Rufen Sie die ID des Pools ab, in dem Sie den Pool erstellen möchten: describe-ipam-pools
3. Erstellen Sie den Pool: create-ipam-pool
4. Sehen Sie sich den neuen Pool an: describe-ipam-pools

Wiederholen Sie diese Schritte, um nach Bedarf zusätzliche Pools innerhalb des Pools der obersten Ebene zu erstellen.

Erstellen eines IPv4-Entwicklungspool

Führen Sie die Schritten in diesem Abschnitt aus, um einen Entwicklungspool in Ihrem Regionalpool zu erstellen. Wenn Sie nur einen Top-Level- und Regionalpool benötigen und keine Entwicklungspools benötigen, fahren Sie mit Zuweisen von CIDRs fort.

Das folgende Beispiel zeigt die Hierarchie der Poolstruktur, die Sie mit den Anweisungen in diesem Leitfaden erstellen können. In diesem Schritt erstellen Sie einen IPAM-Entwicklungspool:

- IPAM operiert in AWS-Region 1 und AWS-Region 2
  - Privater Bereich
    - Top-level Pool (10.0.0.0/8)
      - Regionaler Pool in AWS-Region 1 (10.0.0.0/16)
        - Entwicklungspool für Nicht-Produktions-VPCs (10.0.0.0/24)
          - Zuweisung für eine VPC (10.0.1.0/25)

Im obigen Beispiel sind die verwendeten CIDRs nur Beispiele. Sie veranschaulichen, dass jeder Pool innerhalb des Pools der obersten Ebene mit einem Teil des CIDR der obersten Ebene bereitgestellt wird.

AWS Management Console

So erstellen Sie einen Entwicklungspool in einem Regionalpool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie Pool erstellen.
4. Wählen Sie unter IPAM-Bereich denselben Bereich aus, den Sie beim Erstellen der Pools der obersten Ebene und der regionalen Pools verwendet haben. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
5. (Optional) Fügen Sie Name tag (Namenstag) für den Pool und eine Beschreibung für den Pool ein.
6. Wählen Sie unter Quelle die Option IPAM-Pool aus. Wählen Sie dann den regionalen Pool aus.

7. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
8. (Optional) Wählen Sie ein CIDR aus, das für den Pool bereitgestellt werden soll. Sie können nur ein CIDR bereitstellen, das für den Pool der obersten Ebene bereitgestellt wurde. Sie können einen Pool ohne CIDR erstellen, aber Sie können den Pool erst für Zuweisungen verwenden, wenn Sie ein CIDR dafür bereitgestellt haben. Sie können einem Pool jederzeit CIDRs hinzufügen, indem Sie den Pool bearbeiten.
9. Sie haben hier die gleichen Zuweisungsregeloptionen wie beim Erstellen des obersten und regionalen Pools. Für eine Erläuterung der Optionen, die beim Erstellen von Pools verfügbar sind, siehe Erstellen eines IPv4-Pools der obersten Ebene. Die Zuordnungsregeln für den Pool werden nicht von dem darüber liegenden Pool in der Hierarchie geerbt. Wenn Sie hier keine Regeln anwenden, werden keine Zuteilungsregeln für den Pool festgelegt.
10. (Optional) Wählen Sie Tags für den Pool.
11. Wenn Sie mit der Konfiguration Ihres Pools fertig sind, wählen Sie Create pool (Pool erstellen) aus.
12. Siehe Zuweisen von CIDRs.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Erstellen eines regionalen Pools in Ihrem IPAM:

1. Rufen Sie die ID des Bereichs ab, in dem Sie den Pool erstellen möchten: describe-ipam-scopes
2. Rufen Sie die ID des Pools ab, in dem Sie den Pool erstellen möchten: describe-ipam-pools
3. Erstellen Sie den Pool: create-ipam-pool
4. Sehen Sie sich den neuen Pool an: describe-ipam-pools

Wiederholen Sie diese Schritte, um nach Bedarf zusätzliche Entwicklungspools im Regionalpool zu erstellen.

Erstellen von IPv6-Pools

Führen Sie die Schritte in diesem Abschnitt aus, um eine IPv6-IPAM-Poolhierarchie zu erstellen. Wenn Sie den Pool erstellen, können Sie ein CIDR für die Verwendung durch den Pool bereitstellen. Der Pool weist den Zuordnungen innerhalb des Pools Speicherplatz innerhalb dieses CIDR zu. In der Zuweisung ist eine CIDR-Zuweisung von einem IPAM-Pool zu einer anderen Ressource oder einem IPAM-Pool.

Das folgende Beispiel zeigt die Hierarchie der Poolstruktur, die Sie mit den Anweisungen in diesem Leitfaden erstellen können. In diesem Abschnitt erstellen Sie eine IPv6-IPAM-Poolhierarchie:

- IPAM operiert in AWS-Region 1 und AWS-Region 2
  - Öffentlicher Bereich
    - Regionaler Pool in AWS-Region 1 (2001:db8::/52)
      - Entwicklungspool (2001:db8::/54)
        - Zuweisung für eine VPC (2001:db8::/56)

Inhalt

Erstellen eines regionalen IPv6-Pools

Führen Sie die Schritte in diesem Abschnitt aus, um einen regionalen IPv6-IPAM-Pool zu erstellen. Wenn Sie einen von Amazon bereitgestellten IPv6-CIDR-Block für einen Pool bereitstellen, muss er für einen Pool mit ausgewähltem Gebietsschema (AWS-Region) bereitgestellt werden. Wenn Sie den Pool erstellen, können Sie ein CIDR für den Pool zur Verwendung bereitstellen oder es später hinzufügen. Anschließend weisen Sie diesen Bereich einer Zuweisung zu. Eine Zuordnung ist eine CIDR-Zuweisung von einem IPAM-Pool zu einem anderen IPAM-Pool oder zu einer Ressource.

Das folgende Beispiel zeigt die Hierarchie der Poolstruktur, die Sie mit den Anweisungen in diesem Leitfaden erstellen können. In diesem Schritt erstellen Sie den regionalen IPv6-IPAM-Pool:

- IPAM operiert in AWS-Region 1 und AWS-Region 2

- Öffentlicher Bereich
  - Regionaler Pool in AWS-Region 1 (2001:db8::/52)
    - Entwicklungspool (2001:db8::/54)
      - Zuweisung für eine VPC (2001:db8::/56)

Im obigen Beispiel sind die verwendeten CIDRs nur Beispiele. Diese veranschaulichen, dass jeder Pool innerhalb des regionalen IPv6-Pools mit einem Teil des regionalen IPv6-CIDR bereitgestellt wird.

Wenn Sie einen IPAM-Pool erstellen, können Sie Regeln für die Zuweisungen konfigurieren, die im IPAM-Pool vorgenommen werden.

Mit Zuweisungsregeln können Sie Folgendes konfigurieren:

- Die erforderliche Netzmaskenlänge für Zuweisungen innerhalb des Pools
- Die erforderlichen Tags für Ressourcen im Pool
- Das erforderliche Gebietsschema für Ressourcen innerhalb des Pools. Das Gebietsschemas ist die AWS-Region, in der ein IPAM-Pool für Zuweisungen verfügbar ist.

Zuweisungsregeln legen fest, ob Ressourcen konform oder nicht konform sind. Weitere Informationen zur Compliance finden Sie unter Überwachen Sie die CIDR-Nutzung nach Ressourcen.

> **Important**
>
> Es gibt eine zusätzliche implizite Regel, die in den Zuweisungsregeln nicht angezeigt wird. Wenn sich die Ressource in einem IPAM-Pool befindet, bei dem es sich um eine gemeinsam genutzte Ressource im AWS Resource Access Manager (RAM) handelt, muss der Ressourcenbesitzer als Prinzipal im AWS-RAM konfiguriert werden. Weitere Informationen zum Freigeben von Pools mit RAM finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM.

Im folgenden Beispiel wird gezeigt, wie Sie mit Zuteilungsregeln den Zugriff auf einen IPAM-Pool steuern können:

Example

Wenn Sie Ihre Pools basierend auf Routing- und Sicherheitsanforderungen erstellen, möchten Sie möglicherweise nur bestimmten Ressourcen erlauben, einen Pool zu verwenden. In solchen Fällen können Sie eine Allokationsregel festlegen, die besagt, dass jede Ressource, die ein CIDR aus diesem Pool wünscht, ein Tag haben muss, das den Anforderungen für das Zuordnungsregeltag entspricht. Sie können beispielsweise eine Zuweisungsregel festlegen, die angibt, dass nur VPCs mit dem Tag prod CIDRs aus einem IPAM-Pool holen können.

> **Important**
>
> In diesem Thema wird beschrieben, wie Sie einen regionalen IPv6-Pool mit einem von AWS bereitgestellten IP-Adressbereich erstellen. Wenn Sie Ihre eigenen IPv4- oder IPv6-IP-Adressbereiche in AWS (BYOIP) einbringen möchten, müssen einige Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Tutorial: Mitbringen eigener IP-Adressen in IPAM.

AWS Management Console

So erstellen Sie einen Pool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie Pool erstellen.
4. Wählen Sie unter IPAM-Bereich den öffentlichen Bereich aus. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.

   Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Pools im privaten Bereich müssen IPv4-Pools sein. Pools im öffentlichen Bereich können IPv4- oder IPv6-Pools sein. Der öffentliche Bereich ist für alle Bereiche gedacht, die von AWS im Internet beworben werden können oder derzeit beworben werden.
5. (Optional) Fügen Sie Name tag (Namenstag) für den Pool und eine Beschreibung für den Pool ein.
6. Wählen Sie unter Quelle die Option IPAM-Bereich aus.
7. Wählen Sie für Adressfamilie die Option IPv6 aus. Die Umschaltfläche Zulassen, dass CIDRs in diesem Pool öffentlich beworben werden können wird angezeigt. Standardmäßig

können alle CIDRs in diesem Pool öffentlich beworben werden. Sie können diese Option nicht aktivieren oder deaktivieren.

8. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
9. Wählen Sie das Gebietsschema für den Pool aus. Wenn Sie einen von Amazon bereitgestellten IPv6-CIDR-Block für einen Pool bereitstellen, muss er für einen Pool mit ausgewähltem Gebietsschema (AWS-Region) bereitgestellt werden. Die Auswahl eines Gebietsschemas stellt sicher, dass es keine regionsübergreifenden Abhängigkeiten zwischen Ihrem Pool und den daraus zugewiesenen Ressourcen gibt. Die verfügbaren Optionen stammen aus den Betriebsregionen, die Sie bei der Erstellung des IPAM ausgewählt haben. Sie können jederzeit weitere Betriebsregionen hinzufügen.

   Das Gebietsschema AWS-Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden.

   > **Note**
   >
   > Wenn Sie einen Pool im kostenlosen Kontingent erstellen, können Sie nur das Gebietsschema wählen, das der Heimatregion Ihres IPAM entspricht. Um alle IPAM-Feature gebietsschemaübergreifend nutzen zu können, führen Sie ein Upgrade auf das erweiterte Kontingent durch.

10. Wählen Sie unter Dienst EC2 (EIP/VPC) aus. Der von Ihnen gewählte Service bestimmt den AWS-Service, bei dem die CIDR beworben werden kann. Derzeit ist die einzige Option EC2 (EIP/VPC), was bedeutet, dass die aus diesem Pool zugewiesenen CIDRs für den Amazon-EC2-Service (für elastische IP-Adressen) und den Amazon-VPC-Service (für CIDRs, die mit VPCs verknüpft sind) beworben werden können.
11. Wählen Sie unter der Option Öffentliche IP-Quelle die Option Im Eigentum von Amazon aus, damit AWS einen IPv6-Adressbereich für diesen Pool bereitstellt. Wie oben auf dieser Seite erwähnt, behandelt dieses Thema das Erstellen eines regionalen IPv6-Pools mit einem

von AWS bereitgestellten IP-Adressbereich. Wenn Sie Ihre eigenen IPv4- oder IPv6-IP-Adressbereiche in AWS (BYOIP) einbringen möchten, müssen einige Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Tutorial: Mitbringen eigener IP-Adressen in IPAM.

12. Für Pools im öffentlichen Bereich, die die öffentliche IP-Quelle BYOIP nutzen, können Sie über die Option Öffentliche Ankündigung für CIDRs in diesem Pool zulassen festlegen, ob AWS die CIDRs in diesem Pool öffentlich ankündigen darf. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie diese Option, wenn AWS CIDRs in diesem Pool nicht öffentlich ankündigen dürfen soll.
13. (Optional) Sie können einen Pool ohne CIDR erstellen, aber Sie können den Pool erst für Zuordnungen verwenden, wenn Sie ein CIDR dafür bereitgestellt haben. Um ein CIDR bereitzustellen, wählen Sie Amazon-eigenes CIDR hinzufügen und wählen Sie die Netzmaskengröße zwischen /40 und /52 für den CIDR aus.

> **Note**
>
> Beachten Sie Folgendes:
>
> - Standardmäßig können Sie dem regionalen Pool einen von Amazon bereitgestellten IPv6-CIDR-Block hinzufügen. Informationen zum Erhöhen des Standardlimits finden Sie unter Kontingente für Ihr IPAM.
> - Wenn Sie im Dropdown-Menü eine Netzmaskenlänge auswählen, sehen Sie die Netzmaskenlänge sowie die Anzahl der /56-CIDRs, die die Netzmaske darstellt.

14. Wählen Sie optionale Zuordnungsregeln für diesen Pool aus:

- Minimum netmask lenght (Minimale Netzmaskenlänge): Die minimale Netzmaskenlänge, die erforderlich ist, damit CIDR-Zuweisungen in diesem IPAM-Pool konform sind, und der CIDR-Block der größten Größe, der aus dem Pool zugewiesen werden kann. Die minimale Netzmaskenlänge muss kleiner als die maximale Netzmaskenlänge sein. Mögliche Netzmaskenlängen für IPv6-Adressen sind 0 - 128.
- Default netmask lenght (Standardlänge für Netzmasken): Eine standardmäßige Netzmaskenlänge für Zuweisungen, die diesem Pool hinzugefügt wurden. Wenn die CIDR, die diesem Pool bereitgestellt wird, beispielsweise `2001:db8::/52` ist und Sie hier 56 eingeben, wird für alle neuen Zuweisungen in diesem Pool standardmäßig eine Netzmaskenlänge von /56 verwendet.

- Maximum netmask lenght (Maximale Netzmaskellänge): Die maximale Netzmaskenlänge, die für CIDR-Zuweisungen in diesem Pool erforderlich ist. Dieser Wert gibt den CIDR-Block der kleinsten Größe vor, der aus dem Pool zugewiesen werden kann. Wenn Sie hier beispielsweise /56 eingeben, ist die kleinste Netzmaskenlänge, die CIDRs aus diesem Pool zugewiesen werden kann, /56.
- Tagging (Markierung): Die Tags, die benötigt werden, damit Ressourcen Speicherplatz aus dem Pool zuweisen können. Wenn die Ressourcen ihre Tags geändert haben, nachdem sie Speicherplatz zugewiesen haben oder wenn die Zuordnungskennzeichnungsregeln im Pool geändert werden, wird die Ressource möglicherweise als nicht konform gekennzeichnet.
- Locale (Gebietsschema): Das Gebietsschema, das für Ressourcen benötigt wird, die CIDRs aus diesem Pool verwenden. Automatisch importierte Ressourcen, die dieses Gebietsschema nicht haben, werden als nicht konform gekennzeichnet. Ressourcen, die nicht automatisch in den Pool importiert werden, dürfen keinen Speicherplatz aus dem Pool zuweisen, es sei denn, sie befinden sich in diesem Gebietsschema.

15. (Optional) Wählen Sie Tags für den Pool.
16. Wählen Sie Pool erstellen.
17. Siehe Erstellen eines IPv6-Entwicklungspool.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Erstellen oder Bearbeiten eines regionalen IPv6-Pools in Ihrem IPAM:

1. Erstellen eines Pools: create-ipam-pool.
2. Bearbeiten Sie den Pool, nachdem Sie ihn erstellt haben, um die Zuordnungsregeln zu ändern: modify-ipam-pool.

Erstellen eines IPv6-Entwicklungspool

Führen Sie die Schritte in diesem Abschnitt aus, um einen Entwicklungspool innerhalb Ihres regionalen IPv6-Pools zu erstellen. Wenn Sie nur einen regionalen Pool und keine Entwicklungspools benötigen, fahren Sie mit Zuweisen von CIDRs fort.

Das folgende Beispiel zeigt die Hierarchie der Poolstruktur, die Sie mit den Anweisungen in diesem Leitfaden erstellen können. In diesem Schritt erstellen Sie einen IPAM-Entwicklungspool:

- IPAM operiert in AWS-Region 1 und AWS-Region 2
  - Öffentlicher Bereich
    - Regionaler Pool in AWS-Region 1 (2001:db8::/52)
      - Entwicklungspool (2001:db8::/54)
        - Zuweisung für eine VPC (2001:db8::/56)

Im obigen Beispiel sind die verwendeten CIDRs nur Beispiele. Sie veranschaulichen, dass jeder Pool innerhalb des Pools der obersten Ebene mit einem Teil des CIDR der obersten Ebene bereitgestellt wird.

AWS Management Console

So erstellen Sie einen Entwicklungspool innerhalb eines regionalen IPv6-Pools

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie Pool erstellen.
4. Wählen Sie unter IPAM-Bereich den öffentlichen Bereich aus. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.

   Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Pools im privaten Bereich müssen IPv4-Pools sein. Pools im öffentlichen Bereich können IPv4- oder IPv6-Pools sein. Der öffentliche Bereich ist für alle Bereiche gedacht, die von AWS im Internet beworben werden können oder derzeit beworben werden.
5. (Optional) Fügen Sie Name tag (Namenstag) für den Pool und eine Beschreibung für den Pool ein.
6. Wählen Sie unter Quelle die Option IPAM-Pool aus. Wählen Sie dann unter Quellpool den regionalen IPv6-Pool aus.

7. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
8. (Optional) Wählen Sie ein CIDR aus, das für den Pool bereitgestellt werden soll. Sie können nur ein CIDR bereitstellen, das für den Pool der obersten Ebene bereitgestellt wurde. Sie können einen Pool ohne CIDR erstellen, aber Sie können den Pool erst für Zuweisungen verwenden, wenn Sie ein CIDR dafür bereitgestellt haben. Sie können einem Pool jederzeit CIDRs hinzufügen, indem Sie den Pool bearbeiten.
9. Sie verfügen hier über die gleichen Zuweisungsregel-Optionen wie beim Erstellen des regionalen IPv6-Pools. Für eine Erläuterung der Optionen, die beim Erstellen von Pools verfügbar sind, siehe Erstellen eines regionalen IPv6-Pools. Die Zuordnungsregeln für den Pool werden nicht von dem darüber liegenden Pool in der Hierarchie geerbt. Wenn Sie hier keine Regeln anwenden, werden keine Zuteilungsregeln für den Pool festgelegt.
10. (Optional) Wählen Sie Tags für den Pool.
11. Wenn Sie mit der Konfiguration Ihres Pools fertig sind, wählen Sie Create pool (Pool erstellen) aus.
12. Siehe Zuweisen von CIDRs.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Erstellen eines regionalen IPv6-Pools in Ihrem IPAM:

1. Rufen Sie die ID des Bereichs ab, in dem Sie den Pool erstellen möchten: describe-ipam-scopes
2. Rufen Sie die ID des Pools ab, in dem Sie den Pool erstellen möchten: describe-ipam-pools
3. Erstellen Sie den Pool: create-ipam-pool
4. Sehen Sie sich den neuen Pool an: describe-ipam-pools

Wiederholen Sie diese Schritte, um nach Bedarf weitere Entwicklungspools innerhalb des regionalen IPv6-Pools zu erstellen.

Zuweisen von CIDRs

Führen Sie die Schritte in diesem Abschnitt aus, um einer Ressource ein CIDR aus einem IPAM-Pool zuzuweisen.

> **Note**
>
> Die Ausdrücke provision (Bereitstellung) und allocate (zuweisen) werden in diesem Benutzerhandbuch und in der IPAM-Konsole verwendet. Provision (Bereitstellen) wird verwendet, wenn Sie einem IPAM-Pool einen CIDR hinzufügen. Allocate (Zuweisen) wird verwendet, wenn Sie ein CIDR aus einem IPAM-Pool mit einer Ressource verknüpfen.

Sie können CIDRs wie folgt aus einem IPAM-Pool zuweisen:

- Verwenden Sie einen AWS-Service, der in IPAM integriert ist, wie Amazon VPC, und wählen Sie die Option aus, einen IPAM-Pool für das CIDR zu verwenden. IPAM erstellt automatisch die Zuteilung im Pool für Sie.
- Weisen Sie ein CIDR in einem IPAM-Pool manuell zu, um es für eine spätere Verwendung mit einem AWS-Service, der in IPAM integriert ist, wie Amazon VPC zu verwenden.

In diesem Abschnitt werden Sie durch beide Optionen geführt: wie Sie die AWS-Services, die mit IPAM integriert sind, um ein IPAM-Pool-CIDR bereitzustellen und den IP-Adressraum manuell zu reservieren.

Inhalt

Erstellen Sie eine VPC, die ein IPAM-Pool-CIDR verwendet

Führen Sie die Schritte unter Creating a VPC (Erstellen einer VPC) im Benutzerhandbuch zu Amazon VPC aus. Wenn Sie den Schritt zur Auswahl eines CIDR für die VPC erreichen, haben Sie die Möglichkeit, ein CIDR aus einem IPAM-Pool zu verwenden.

Wenn Sie beim Erstellen der VPC die Option zum Verwenden eines IPAM-Pool auswählen, weist AWS ein CIDR im IPAM-Pool zu. Sie können die Zuweisung in IPAM anzeigen, indem Sie im Inhaltsbereich der IPAM-Konsole einen Pool auswählen und die Registerkarte Ressourcen für den Pool anzeigen.

> **Note**
>
> Vollständige Anweisungen finden Sie unter AWS-CLI, einschließlich des Erstellens einer VPC, welche Sie im Tutorials für Amazon VPC IP Address Manager-Abschnitt finden.

Weisen Sie einem Pool manuell ein CIDR zu, um den IP-Adressraum zu reservieren

Um einem Pool manuell einen CIDR zuzuweisen, führen Sie die Schritte in diesem Abschnitt aus. Sie können dies tun, um ein CIDR in einem IPAM-Pool zur späteren Verwendung zu reservieren. Sie können auch Speicherplatz in Ihrem IPAM-Pool reservieren, um ein On-Premises-Netzwerk darzustellen. IPAM verwaltet diese Reservierung für Sie und gibt an, ob sich CIDRs mit Ihrem On-Premises-IP-Bereich überschneiden.

AWS Management Console

So weisen Sie ein CIDR manuell zu

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Standardmäßig ist der private Standardbereich ausgewählt. Wenn Sie den privaten Standardbereich nicht verwenden möchten, wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie im Inhaltsbereich die Option Pool aus.
5. Wählen Sie Actions (Aktionen) > Create custom allocation (Benutzerdefinierte Zuordnung erstellen) aus.
6. Wählen Sie aus, ob Sie ein bestimmtes CIDR zur Zuweisung hinzufügen möchten (z. B. `10.0.0.0/24` für IPv4 oder `2001:db8::/52` für IPv6), oder ob Sie ein CIDR nach Größe hinzufügen möchten, indem Sie nur die Netzmaskenlänge auswählen (z. B. `/24` für IPv4 oder `/52` für IPv6).

7. Wählen Sie Allocate aus.
8. Sie können die Zuweisung in IPAM anzeigen, indem Sie im Navigationsbereich Pools auswählen, einen Pool auswählen und die Registerkarte Allocations (Zuweisungen) für den Pool anzeigen.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum manuellen Zuweisen eines CIDR zu einem Pool:

1. Rufen Sie die ID des IPAM-Pools ab, in dem Sie die Zuweisung: describe-ipam-pools erstellen.
2. Erstellen Sie die Zuteilung: allocate-ipam-pool-cidr.
3. Sehen Sie sich die Zuteilung an: get-ipam-pool-allocations.

Um einen manuell zugewiesenen CIDR freizugeben, siehe Eine Zuweisung freigeben.

Verwalten des IP-Adressraums in IPAM

Die Aufgaben in diesem Abschnitt sind optional. Wenn Sie die Aufgaben in diesem Abschnitt ausführen möchten und ein IPAM-Konto delegiert haben, sollten die Aufgaben vom IPAM-Administrator erledigt werden.

Führen Sie die Schritte in diesem Abschnitt aus, um Ihren IP-Adressraum in IPAM zu verwalten.

Inhalt

Durchsetzung der IPAM-Verwendung für die VPC-Erstellung

> **Note**
>
> Dieser Abschnitt gilt nur für Sie, wenn Sie IPAM für die Integration mit AWS Organizations aktiviert haben. Weitere Informationen finden Sie unter Integrieren von IPAM mit Konten in einer - AWS Organisation.

In diesem Abschnitt wird beschrieben, wie Sie eine Dienstkontrollrichtlinie in AWS Organizations erstellen, die die Mitglieder Ihrer Organisation verpflichtet, IPAM zu verwenden, wenn sie eine VPC erstellen. Service-Kontrollrichtlinien (Service Control Policies, SCPs) sind eine Art von Organisationsrichtlinien, die Sie zum Verwalten von Berechtigungen in Ihrer Organisation verwenden können. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.

IPAM beim Erstellen von VPCs erzwingen

Führen Sie die Schritte in diesem Abschnitt aus, um zu verlangen, dass Mitglieder Ihrer Organisation IPAM verwenden, wenn Sie VPCs erstellen.

So erstellen Sie einen SCP und beschränken die VPC-Erstellung auf IPAM

1. Befolgen Sie die Schritte unter Erstellen eines SCP im AWS Organizations-Benutzerhandbuch und geben Sie den folgenden Text in den JSON-Editor ein:

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

2. Fügen Sie die Richtlinie einer oder mehreren Organisationseinheiten in Ihrem Unternehmen zu. Weitere Informationen finden Sie unter Anfügen und Trennen von Service-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.

IPAM-Pool beim Erstellen von VPCs erzwingen

Führen Sie die Schritte in diesem Abschnitt aus, um zu verlangen, dass Mitglieder Ihrer Organisation bei der Erstellung von VPCs einen bestimmten IPAM-Pool verwenden.

So erstellen Sie einen SCP und beschränken die VPC-Erstellung auf einen IPAM-Pool

1. Befolgen Sie die Schritte unter Erstellen eines SCP im AWS Organizations-Benutzerhandbuch und geben Sie den folgenden Text in den JSON-Editor ein:

```
{
    "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. Ändern Sie den `ipam-pool-0123456789abcdefg`-Beispielwert für die IPv4-Pool-ID, auf die Sie Benutzer beschränken möchten.
3. Fügen Sie die Richtlinie einer oder mehreren Organisationseinheiten in Ihrem Unternehmen zu. Weitere Informationen finden Sie unter Anfügen und Trennen von Service-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.

Erzwingen der Nutzung von IPAM für alle Organisationseinheiten außer einer bestimmten Liste von Organisationseinheiten

Führen Sie die Schritte in diesem Abschnitt aus, um IPAM für alle Organisationseinheiten außer einer bestimmten Liste von Organisationseinheiten zu erzwingen. Gemäß der in diesem Abschnitt beschriebenen Richtlinie müssen mit Ausnahme der Organisationseinheiten, die Sie in `aws:PrincipalOrgPaths` festlegen, alle Organisationseinheiten in der Organisation VPCs mithilfe von IPAM erstellen und erweitern. Die aufgelisteten Organisationseinheiten können beim Erstellen von VPCs entweder IPAM nutzen oder einen IP-Adressbereich manuell angeben.

So erstellen Sie eine SCP und erzwingen die Nutzung von IPAM für alle Organisationseinheiten außer einer bestimmten Liste von Organisationseinheiten

1. Befolgen Sie die Schritte unter Erstellen eines SCP im AWS Organizations-Benutzerhandbuch und geben Sie den folgenden Text in den JSON-Editor ein:

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

2. Entfernen Sie die Beispielwerte (wie `o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/`) und fügen Sie die AWS-Organizations-Entitätspfade der Organisationseinheiten hinzu, bei denen die Option (aber nicht der Zwang) zur Nutzung von IPAM bestehen soll. Weitere Informationen zum Entitätspfad finden Sie unter Erläuterung des Entitätspfads von AWS Organizations und aws:PrincipalOrgPaths im Benutzerhandbuch von AWS Identity and Access Management.
3. Fügen Sie die Richtlinie zum Organisations-Root hinzu. Weitere Informationen finden Sie unter Anfügen und Trennen von Service-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.

Teilen Sie einen IPAM-Pool mit AWS RAM

Führen Sie die Schritte in diesem Abschnitt aus, um einen IPAM-Pool mit AWS Resource Access Manager (RAM) freizugeben. Wenn Sie einen IPAM-Pool mit RAM teilen, können „Prinzipale“ CIDRs aus dem Pool AWS-Ressourcen wie VPCs von ihren jeweiligen Konten zuweisen. Ein Prinzipal

ist ein Konzept in RAM, das jedes AWS-Konto, jede IAM-Rolle, jeden IAM-Benutzer oder jede Organisationseinheit in AWS Organizations zusammenfasst. Weitere Informationen finden Sie unter Teilen Ihrer AWS-Ressourcen im AWS-RAM-Benutzerhandbuch.

> **Note**
>
> - Sie können einen IPAM-Pool nur mit AWS RAM freigeben wenn Sie IPAM mit AWS Organizations integriert haben. Weitere Informationen finden Sie unter Integrieren von IPAM mit Konten in einer - AWS Organisation. Sie können einen IPAM-Pool nicht mit AWS RAM freigeben wenn Sie ein IPAM-Benutzer eines einzelnen Kontos sind.
> - Sie müssen die Ressourcenfreigabe mit AWS Organizations im AWS RAM aktivieren. Weitere Informationen finden Sie unter Ressourcenfreigabe innerhalb von AWS Organizations aktivieren im AWS-RAM-Benutzerhandbuch.
> - RAM-Freigabe ist nur in der AWS-Heimatregion Ihres IPAM verfügbar. Sie müssen die Freigabe in der AWS-Region erstellen, in der sich das IPAM befindet, nicht in der Region des IPAM-Pools.
> - Das Konto, das IAM-Pool-Ressourcenfreigaben erstellt und löscht, muss die folgenden Berechtigungen in der an ihre IAM-Rolle angehängte IAM-Richtlinie haben:
>   - `ec2:PutResourcePolicy`
>   - `ec2:DeleteResourcePolicy`
> - Sie können einer RAM-Freigabe mehrere IPAM-Pools hinzufügen.

AWS Management Console

So teilen Sie einen IPAM-Pool mit RAM

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Standardmäßig ist der private Standardbereich ausgewählt. Wenn Sie den privaten Standardbereich nicht verwenden möchten, wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie im Inhaltsbereich den Pool aus, den Sie freigeben möchten, und wählen Sie Actions (Aktionen) > View details (Details anzeigen) aus.

5. Unter Resource sharing (Ressourcenfreigabe), wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus. Infolgedessen wird die AWS-RAM-Konsole geöffnet. Sie erstellen den gemeinsam genutzten Pool in AWS RAM.
6. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.
7. Fügen Sie Name (Namen) für die freigegebene Ressource hinzu.
8. Unter Select resource type (Ressourcentyp auswählen), wählen Sie IPAM-Pools aus und wählen Sie einen oder mehrere IPAM-Pools aus.
9. Wählen Sie Next (Weiter).
10. Wählen Sie eine der Berechtigungen für die Ressourcenfreigabe aus:

    - AWSRAMDefaultPermissionsIpamPool: Wählen Sie diese Berechtigung, damit Prinzipale die CIDRs und Zuweisungen im freigegebenen IPAM-Pool anzeigen und CIDRs im Pool zuweisen/freigeben können.
    - AWSRAMPermissionIpamPoolByoipCidrImport: Wählen Sie diese Berechtigung, damit Prinzipale BYOIP-CIDRs in den freigegebenen IPAM-Pool importieren können. Sie benötigen diese Berechtigung nur, wenn Sie über vorhandene BYOIP-CIDRs verfügen und diese in IPAM importieren und mit Prinzipalen teilen möchten. Weitere Informationen zu BYOIP-CIDRs zu IPAM finden Sie unter Tutorial: Übertragen eines vorhandenen BYOIP-IPv4-CIDR an IPAM.
11. Wählen Sie die Hauptbenutzer aus, die auf diese Ressource zugreifen dürfen. Wenn Prinzipale vorhandene BYOIP-CIDRs in diesen freigegebenen IPAM-Pool importieren, fügen Sie das BYOIP-CIDR-Eigentümerkonto als Prinzipal hinzu.
12. Überprüfen Sie die Optionen für die Ressourcenfreigabe und die Hauptbenutzer, mit denen Sie teilen werden, und wählen Sie Create (Erstellen) aus.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Dort finden Sie detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Teilen eines IPAM-Pool mit RAM:

1. Abrufen des ARN des IPAM: describe-ipam-pools
2. Erstellen Sie die Ressourcenfreigabe: create-resource-share

3. Zeigen Sie die Ressourcenfreigabe an: get-resource-share

Als Ergebnis der Erstellung der Ressourcenfreigabe im RAM können andere Prinzipale jetzt CIDRs Ressourcen zuweisen, die den IPAM-Pool verwenden. Hinweise zur Überwachung von Prinzipals erstellten Ressourcen finden Sie unter Überwachen Sie die CIDR-Nutzung nach Ressourcen. Weitere Informationen zum Erstellen einer VPC und zum Zuweisen eines CIDR aus einem freigegebenen IPAM-Pool finden Sie unter Creating a VPC (Eine VPC erstellen) im Benutzerhandbuch zu Amazon VPC.

Bereitstellen von CIDRs für einen Pool

Führen Sie die Schritte in diesem Abschnitt aus, um CIDRs für einen Pool bereitzustellen. Wenn Sie beim Erstellen des Pools bereits ein CIDR bereitgestellt haben, müssen Sie möglicherweise zusätzliche CIDRs bereitstellen, wenn sich ein Pool der vollständigen Zuweisung nähert. Um die Poolauslastung zu überwachen, siehe Überwachen der CIDR-Nutzung mit dem IPAM-Dashboard.

> **Note**
>
> Die Ausdrücke provision (Bereitstellung) und allocate (zuweisen) werden in diesem Benutzerhandbuch und in der IPAM-Konsole verwendet. Provision (Bereitstellen) wird verwendet, wenn Sie einem IPAM-Pool einen CIDR hinzufügen. Zuweisen wird verwendet, wenn Sie ein CIDR aus einem IPAM-Pool einer VPC- oder Elastic-IP-Adresse zuordnen.

AWS Management Console

Bereitstellen von CIDRs für einen Pool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Standardmäßig ist der private Standardbereich ausgewählt. Wenn Sie den privaten Standardbereich nicht verwenden möchten, wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie im Inhaltsbereich den Pool aus, dem Sie ein CIDR hinzufügen möchten.
5. Klicken Sie auf Actions (Aktionen) > Provision CIDRs (CIDRs bereitstellen).

6. Geben Sie das CIDR ein, das Sie hinzufügen möchten, und wählen Sie dann Add new CIDR (Neue CIDR hinzufügen) für zusätzliche CIDRs.

   > **Note**
   >
   > - Standardmäßig können Sie einem regionalen Pool einen von Amazon bereitgestellten IPv6-CIDR-Block hinzufügen. Informationen zum Erhöhen des Standardlimits finden Sie unter Kontingente für Ihr IPAM.
   > - Das CIDR, den Sie bereitstellen möchten, muss im Bereich verfügbar sein.
   > - Wenn Sie CIDRs für einen Pool innerhalb eines Pools bereitstellen, muss der CIDR-Bereich, den Sie bereitstellen möchten, im Pool verfügbar sein.

7. Klicken Sie auf Request Bereitstellung (Bereitstellen von Anfragen).
8. Sie können die CIDR in IPAM anzeigen, indem Sie im Navigationsbereich Pools auswählen, einen Pool auswählen und die Registerkarte CIDRs für den Pool anzeigen.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Bereitstellen von CIDRs für einen Pool:

1. Abrufen der ID eines IPAM-Pools: describe-ipam-pools
2. Holen Sie sich die CIDRs, die für den Pool bereitgestellt werden: get-ipam-pool-cidrs
3. Stellen Sie einen neuen CIDR für den Pool bereit: provision-ipam-pool-cidr
4. Holen Sie sich die CIDRs, die für den Pool bereitgestellt werden, und sehen Sie sich das neue CIDR an: get-ipam-pool-cidrs

Deprovisionierung von CIDRs aus einem Pool

Um die Bereitstellung von CIDRs aus einem IPAM-Pool aufzuheben, führen Sie die Schritte in diesem Abschnitt aus. Wenn Sie die Bereitstellung aller Pool-CIDRs aufheben, kann der Pool nicht mehr für Zuweisungen verwendet werden. Sie müssen zuerst ein neues CIDR für den Pool bereitstellen, bevor Sie den Pool für Zuweisungen verwenden können.

> **Important**
>
> Sie können die Bereitstellung des CIDR nicht aufheben, wenn der Pool Zuweisungen enthält. Um Zuweisungen zu entfernen, siehe Eine Zuweisung freigeben.

AWS Management Console

So heben Sie die Bereitstellung eines Pool-CIDR auf

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie im Dropdown-Menü oben im Inhaltsbereich den gewünschten Bereich aus. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie im Inhaltsbereich den Pool aus, dessen CIDRs Sie die Bereitstellung aufheben möchten.
5. Wählen Sie die Registerkarte CIDRs.
6. Wählen Sie mindestens ein CIDR aus und wählen Sie Deprovision CIDRs (Bereitstellung von CIDRs aufheben) aus.
7. Wählen Sie Deprovision CIDR (Bereitstellung von CIDR aufheben).

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Aufheben der Bereitstellung eines Pool-CIDRs:

1. Holen Sie sich eine IPAM-Pool-ID: describe-ipam-Pools
2. Sehen Sie sich Ihre aktuellen CIDRs für den Pool an: get-ipam-pool-cidrs
3. Bereitstellung von CIDRs aufheben: deprovision-ipam-pool-cidr
4. Sehen Sie sich Ihre aktualisierten CIDRs an: get-ipam-pool-cidrs

Um einen neuen CIDR für den Pool bereitzustellen, siehe Deprovisionierung von CIDRs aus einem Pool. Informationen wie Sie den Pool löschen können, finden Sie unter Einen Pool löschen.

Einen Pool bearbeiten

Um einen IPAM-Pool zu bearbeiten, führen Sie die Schritte in diesem Abschnitt aus. Möglicherweise möchten Sie einen Pool bearbeiten, um die Zuweisungsregeln im Pool zu ändern. Weitere Informationen zu Zuweisungsregeln finden Sie unter Erstellen eines IPv4-Pools der obersten Ebene.

AWS Management Console

So bearbeiten Sie einen Pool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Standardmäßig ist der private Standardbereich ausgewählt. Wenn Sie den privaten Standardbereich nicht verwenden möchten, wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM
4. Wählen Sie im Inhaltsbereich den Pool aus, dessen CIDR Sie die bearbeiten möchten.
5. Wählen Sie Actions (Aktionen) und Edit (Bearbeiten).
6. Nehmen Sie alle Änderungen an den Pools vor. Informationen zu Pool-Konfigurationsoptionen finden Sie unter Erstellen eines IPv4-Pools der obersten Ebene.
7. Wählen Sie Update (Aktualisieren).

Command line

Verwenden Sie die folgenden AWS CLI-Befehle zum Bearbeiten eines Pools:

1. Holen Sie sich eine IPAM-Pool-ID: describe-ipam-Pools
2. Ändern Sie den Pool: modify-ipam-pool

Einen Pool löschen

Um einen IPAM-Pool zu löschen, führen Sie die Schritte in diesem Abschnitt aus.

> **Important**
>
> Sie können einen IP-Adresspool nicht löschen, wenn es Zuweisungen gibt. Sie müssen zuerst die Allokationen und Deprovisionierung von CIDRs aus einem Pool freigeben, bevor Sie den Pool löschen können.

AWS Management Console

So löschen Sie einen Pool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie im Dropdown-Menü oben im Inhaltsbereich den gewünschten Bereich aus. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie im Inhaltsbereich den Pool aus, dessen CIDR Sie die löschen möchten.
5. Wählen Sie Actions (Aktionen) und Delete Pool (Pool Löschen).
6. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie den folgenden AWS CLI-Befehl, um den Pool zu löschen:

1. Pools ansehen und eine IPAM-Pool-ID erhalten: describe-ipam-pools
2. Einen Pool löschen: delete-ipam-pool
3. Ihre Pools ansehen: describe-ipam-pools

Um einen neuen Pool zu erstellen, siehe Erstellen eines IPv4-Pools der obersten Ebene.

Arbeiten mit Ressourcenergebnissen

Eine Ressourcenerkennung ist eine IPAM-Komponente, die es IPAM ermöglicht, Ressourcen zu verwalten und zu überwachen, die dem Besitzerkonto gehören. Ein Ressourcenerkennung wird

standardmäßig erstellt, wenn Sie ein IPAM erstellen. Sie können eine Ressourcenerkennung auch unabhängig von einem IPAM erstellen und in ein IPAM integrieren, das einem anderen Konto oder einer anderen Organisation gehört. Wenn der Besitzer der Ressourcenerkennung der delegierte Administrator einer Organisation ist, überwacht IPAM die Ressourcen für alle Mitglieder der Organisation.

> **Note**
>
> Das Erstellen, Freigeben und Zuordnen von Ressourcenergebnissen ist Teil des Integrationsprozesses von IPAM mit Konten außerhalb Ihrer Organisationen (siehe Integrieren von IPAM mit Konten außerhalb Ihrer Organisation). Wenn Sie kein IPAM erstellen und es mit Konten außerhalb Ihrer Organisation integrieren, müssen Sie keine Ressourcenergebnisse erstellen, freigeben oder zuordnen.

Inhalt

Erstellen einer Ressourcenerkennung

In diesem Abschnitt wird beschrieben, wie eine Ressourcenerkennung erstellt wird. Eine Ressourcenerkennung wird standardmäßig erstellt, wenn Sie ein IPAM erstellen. Das Standardkontingent für Ressourcenergebnisse pro Region ist 1. Weitere Hinweise zu IPAM-Kontingenten finden Sie unter Kontingente für Ihr IPAM.

> **Note**
>
> Das Erstellen, Freigeben und Zuordnen von Ressourcenergebnissen ist Teil des Integrationsprozesses von IPAM mit Konten außerhalb Ihrer Organisationen (siehe Integrieren von IPAM mit Konten außerhalb Ihrer Organisation). Wenn Sie kein IPAM

erstellen und es mit Konten außerhalb Ihrer Organisation integrieren, müssen Sie keine Ressourcenergebnisse erstellen, freigeben oder zuordnen.

Wenn Sie ein IPAM mit Konten außerhalb Ihrer Organisation integrieren, ist dies ein erforderlicher Schritt, der vom Administratorkonto der sekundären Organisation abgeschlossen werden muss. Weitere Informationen zu den an diesem Prozess beteiligten Rollen finden Sie unter Prozessübersicht.

AWS Management Console

Erstellen einer Ressourcenerkennung

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Ressourcenergebnisse aus.
3. Wählen Sie Ressourcenerkennung erstellen aus.
4. Wählen Sie Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Replizieren von VPC aus Quellkonten in das Replizieren von Daten aus Quellkonten in das IPAM-Delegate-Konto erlauben) aus. Wenn Sie diese Option nicht auswählen, können Sie keine Ressourcenerkennung erstellen.
5. (Optional) Fügen Sie der Ressourcenerkennung ein Name-Tag hinzu. Ein Tag ist eine Markierung, die Sie einer AWS-Ressource zuordnen. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Mithilfe von Tags können Sie Ressourcen suchen und filtern oder Ihre AWS-Kosten verfolgen.
6. (Optional) Fügen Sie eine Beschreibung hinzu.
7. Wählen Sie unter Betriebsregionen die AWS-Regionen aus, in denen Ressourcen erkannt werden. Die aktuelle Region wird automatisch als eine der Betriebsregionen festgelegt. Wenn Sie die Ressourcenerkennung erstellen, damit Sie sie mit einem IPAM für eine Betriebsregion `us-east-1` freigeben können, stellen Sie sicher, dass Sie hier `us-east-1` auswählen. Wenn Sie eine Betriebsregion vergessen haben, können Sie zu einem späteren Zeitpunkt zurückkehren und Ihre Einstellungen zur Ressourcenerkennung bearbeiten.

> **Note**
>
> In den meisten Fällen sollte die Ressourcenerkennung die gleichen Betriebsregionen wie IPAM haben, oder Sie erhalten die Ressourcenerkennung nur in dieser einen Region.

8. (Optional) Wählen Sie weitere Tags für den Pool.
9. Wählen Sie Erstellen aus.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

- Erstellen einer Ressourcenerkennung: create-ipam-resource-discovery

Anzeigen von Details der Ressourcenerkennung

In diesem Abschnitt wird beschrieben, wie Sie die Details für eine Ressourcenerkennung anzeigen. Dazu gehören die Ressourcen-CIDRs und der Erkennungsstatus von Konten, die im Rahmen Ihrer Ressourcenerkennung überwacht werden.

AWS Management Console

So zeigen Sie Details zur Ressourcenerkennung an

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Ressourcenergebnisse aus.
3. Wählen Sie eine Ressourcenerkennung aus.
4. Zeigen Sie unter Details zur Ressourcenerkennung Details zur Ressourcenerkennung an, z. B. Standard, der angibt, ob die Ressourcenerkennung die Standardeinstellung ist. Die standardmäßige Ressourcenerkennung ist die Ressourcenerkennung, die automatisch erstellt wird, wenn Sie ein IPAM erstellen.
5. Zeigen Sie auf den Registerkarten die Details einer Ressourcenerkennung an:

- Erkannte Ressourcen – Ressourcen, die im Rahmen einer Ressourcenerkennung überwacht werden. IPAM überwacht CIDRs der folgenden Ressourcentypen: VPCs, öffentliche IPv4-Pools, VPC-Subnetze und Elastic-IP-Adressen.
  - Name (Ressourcen-ID) – Ressourcenerkennungs-ID.
  - IP-Nutzung – Der Prozentsatz des IP-Adressbereich in der verwendeten Ressource. Um die Dezimalzahl in einen Prozentsatz umzurechnen, multiplizieren Sie die Dezimalzahl mit 100. Beachten Sie Folgendes –
    - Bei Ressourcen, bei denen es sich um VPCs handelt, ist dies der Prozentsatz des IP-Adressbereich in der VPC, der von Subnetz-CIDRs belegt wird.
    - Für Ressourcen, die Subnetze sind und für das Subnetz ein IPv4-CIDR bereitgestellt wurde, ist dies der Prozentsatz des IPv4-Adressraums im Subnetz, der verwendet wird. Wenn für das Subnetz ein IPv6-CIDR bereitgestellt ist, wird der Prozentsatz des verwendeten IPv6-Adressraums nicht dargestellt. Der Prozentsatz des verwendeten IPv6-Adressraums kann derzeit nicht berechnet werden.
    - Bei Ressourcen, bei denen es sich um öffentliche IPv4-Pools handelt, ist dies der Prozentsatz des IP-Adressbereich im Pool, der Elastic-IP-Adressen (EIPs) zugewiesen wurde.
  - CIDR – Ressourcen-CIDR.
  - Region – Ressourcenregion.
  - Besitzer-ID – Ressourcenbesitzer-ID.
  - Beispielzeit – Der Zeitpunkt der letzten erfolgreichen Ressourcenerkennung.
- Erkannte Konten: AWS-Konten, die im Rahmen einer Ressourcenerkennung überwacht werden. Wenn Sie IPAM in AWS Organizations integriert haben, handelt es sich bei allen Konten in der Organisation um erkannte Konten.
  - Konto-ID – Die Konto-ID.
  - Region – Die AWS-Region, aus der die Kontoinformationen zurückgegeben werden.
  - Zeitpunkt des letzten Erkennungsversuchs – Der Zeitpunkt des letzten Versuchs der Ressourcenerkennung.
  - Zeitpunkt der letzten erfolgreichen Suche – Der Zeitpunkt der letzten erfolgreichen Ressourcenerkennung.
  - Status – Grund für den Fehler bei der Ressourcenerkennung.
- Betriebsregionen – Die Betriebsregionen für die Ressourcenerkennung.

- Freigabe von Ressourcen – Wenn die Ressourcenerkennung freigegeben wurde, wird der Ressourcenfreigabe-ARN aufgeführt.
  - Ressourcenfreigabe-ARN – Ressourcenfreigabe-ARN.
  - Status – Der aktuelle Status der Ressourcenfreigabe. Die möglichen Werte sind:
    - Aktiv – Ressourcenfreigabe ist aktiv und kann verwendet werden.
    - Gelöscht – Ressourcenfreigabe wird gelöscht und steht nicht mehr zur Nutzung zur Verfügung.
    - Ausstehend – Eine Einladung zur Annahme der Ressourcenfreigabe wartet auf eine Antwort.
  - Erstellt am – Wann die Ressourcenfreigabe erstellt wurde.
- Tags – Ein Tag ist eine Markierung, die Sie einer AWS-Ressource zuordnen. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Mithilfe von Tags können Sie Ressourcen suchen und filtern oder Ihre AWS-Kosten verfolgen.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

- Anzeigen von Details zur Ressourcenerkennung: describe-ipam-resource-discovery

Freigabe einer Ressourcenerkennung

Befolgen Sie die Schritte in diesem Abschnitt, um einen Ressourcenerkennung mithilfe von AWS Resource Access Manager freizugeben. Weitere Informationen zu AWS RAM finden Sie unter Freigeben Ihrer AWS-Ressourcen im AWS RAM-Benutzerhandbuch.

> **Note**
>
> Das Erstellen, Freigeben und Zuordnen von Ressourcenergebnissen ist Teil des Integrationsprozesses von IPAM mit Konten außerhalb Ihrer Organisationen (siehe Integrieren von IPAM mit Konten außerhalb Ihrer Organisation). Wenn Sie kein IPAM erstellen und es mit Konten außerhalb Ihrer Organisation integrieren, müssen Sie keine Ressourcenergebnisse erstellen, freigeben oder zuordnen.

Wenn Sie ein IPAM erstellen, das Konten außerhalb Ihrer Organisation überwacht, gibt Administratorkonto der sekundären Organisation seine Ressourcenerkennung mithilfe von AWS RAM für das IPAM-Konto der primären Organisation frei. Sie müssen zuerst eine Ressourcenerkennung für das IPAM-Konto der primären Organisation freigeben, bevor das IPAM-Konto der primären Organisation die Ressourcenerkennung ihrem IPAM zuordnen kann. Weitere Informationen über die an diesem Prozess beteiligten Rollen finden Sie unter Prozessübersicht.

Note

- Wenn Sie eine Ressourcenfreigabe mit AWS RAM erstellen, um eine Ressourcenerkennung freizugeben, müssen Sie die Ressourcenerkennung in der Heimatregion des IPAM der primären Organisation erstellen.
- Das Konto, das eine Ressourcenfreigabe für die Ressourcenerkennung erstellt und löscht, muss in seiner IAM-Richtlinie über die folgenden Berechtigungen verfügen:
  - ec2:PutResourcePolicy
  - ec2:DeleteResourcePolicy

Wenn Sie ein IPAM mit Konten außerhalb Ihrer Organisation integrieren, ist dies ein erforderlicher Schritt, der vom Administratorkonto der sekundären Organisation abgeschlossen werden muss.

AWS Management Console

So geben Sie eine Ressourcenerkennung frei

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Ressourcenergebnisse aus.
3. Wählen Sie die Registerkarte Ressourcenfreigabe.
4. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus. Die AWS RAM-Konsole, in der Sie die Ressourcenfreigabe erstellen, wird geöffnet.
5. Wählen Sie in der AWS RAM-Konsole Settings (Einstellungen).
6. Wählen Sie Freigabe mit AWS Organizations aktivieren und dann Einstellungen speichern aus.
7. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.
8. Fügen Sie Name (Namen) für die freigegebene Ressource hinzu.

9. Wählen Sie unter Ressourcentyp auswählen die Option IPAM-Ressourcenerkennung aus, und wählen Sie die Ressourcenerkennung aus.
10. Wählen Sie Next (Weiter).
11. Unter Berechtigungen zuordnen können Sie die Standardberechtigung anzeigen, die für Prinzipale aktiviert wird, denen Zugriff auf diese Ressourcenfreigabe gewährt wird:
    - AWSRAMPermissionIpamResourceDiscovery
    - Durch diese Berechtigung erlaubte Aktionen:
      - ec2:AssociateIpamResourceDiscovery
      - ec2:GetIpamDiscoveredAccounts
      - ec2:GetIpamDiscoveredPublicAddresses
      - ec2:GetIpamDiscoveredResourceCidrs
12. Geben Sie die Prinzipale an, die Zugriff auf die gemeinsam genutzte Ressource haben. Wählen Sie unter Prinzipale das IPAM-Konto der primären Organisation und dann Hinzufügen aus.
13. Wählen Sie Next (Weiter).
14. Überprüfen Sie die Optionen zum Teilen von Ressourcen und die Prinzipale, mit denen Sie freigeben werden. Wählen Sie Ressourcenfreigabe erstellen aus.
15. Nachdem eine Ressourcenerkennung freigegeben wurde, muss sie vom IPAM-Konto der primären Organisation akzeptiert und dann vom IPAM-Konto der primären Organisation einem IPAM zugeordnet werden. Weitere Informationen finden Sie unter Zuordnung einer Ressourcenerkennung zu einem IPAM.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

1. Erstellen Sie die Ressourcenfreigabe: create-resource-share
2. Zeigen Sie die Ressourcenfreigabe an: get-resource-share

Zuordnung einer Ressourcenerkennung zu einem IPAM

In diesem Abschnitt wird beschrieben, wie Sie eine Ressourcenerkennung einem IPAM zuordnen. Wenn Sie eine Ressourcenerkennung einem IPAM zuordnen, überwacht das IPAM alle Ressourcen-CIDRs und -Konten, die unter der Ressourcenerkennung erkannt wurden. Wenn Sie ein IPAM erstellen, wird eine standardmäßige Ressourcenerkennung für Ihr IPAM erstellt und automatisch Ihrem IPAM zugeordnet.

Das Standardkontingent für Zuordnungen zur Ressourcenerkennung ist 5. Weitere Informationen (einschließlich der Anpassung dieses Kontingents) finden Sie unter Kontingente für Ihr IPAM.

> **Note**
>
> Das Erstellen, Freigeben und Zuordnen von Ressourcenergebnissen ist Teil des Integrationsprozesses von IPAM mit Konten außerhalb Ihrer Organisationen (siehe Integrieren von IPAM mit Konten außerhalb Ihrer Organisation). Wenn Sie kein IPAM erstellen und es mit Konten außerhalb Ihrer Organisation integrieren, müssen Sie keine Ressourcenergebnisse erstellen, freigeben oder zuordnen.

Wenn Sie ein IPAM mit Konten außerhalb Ihrer Organisation integrieren, ist dies ein erforderlicher Schritt, der vom IPAM-Konto der primären Organisation abgeschlossen werden muss. Weitere Informationen über die an diesem Prozess beteiligten Rollen finden Sie unter Prozessübersicht.

AWS Management Console

So weisen Sie einen Ressourcenerkennung zu

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich die Option IPAMs.
3. Wählen Sie Zugeordnete Erkennungen und dann Ressourcenerkennungen zuordnen aus.
4. Wählen Sie unter IPAM-Ressourcenergebnisse eine Ressourcenerkennung aus, die vom Administratorkonto der sekundären Organisation für Sie freigegeben wurde.
5. Wählen Sie Associate aus.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

- Zuordnen einer Ressourcenerkennung associate-ipam-resource-discovery

Aufhebung der Zuordnung einer Ressourcenerkennung

In diesem Abschnitt wird beschrieben, wie Sie eine Ressourcenerkennung von einem IPAM trennen. Wenn Sie die Zuordnung einer Ressourcenerkennung zu einem IPAM aufheben, überwacht das IPAM nicht mehr alle Ressourcen-CIDRs und Konten, die im Rahmen der Ressourcenerkennung erkannt wurden.

> **Note**
>
> Sie können die Zuordnung einer Standard-Ressourcenerkennung nicht aufheben. Eine Standardzuordnung zur Ressourcenerkennung wird automatisch erstellt, wenn Sie ein IPAM erstellen. Die standardmäßige Zuordnung der Ressourcenerkennung wird jedoch gelöscht, wenn Sie das IPAM löschen.

Dieser Schritt muss vom IPAM-Konto der primären Organisation abgeschlossen werden. Weitere Informationen über die an diesem Prozess beteiligten Rollen finden Sie unter Prozessübersicht.

AWS Management Console

So heben Sie die Zuordnung einer Ressourcenerkennung auf

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich die Option IPAMs.
3. Wählen Sie Zugeordnete Erkennungen und dann Ressourcenergebnisse aufheben aus.
4. Wählen Sie unter IPAM-Ressourcenergebnisse eine Ressourcenerkennung aus, die vom Administratorkonto der sekundären Organisation für Sie freigegeben wurde.
5. Wählen Sie Disassociate (Zuordnung aufheben) aus.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

- So heben Sie die Zuordnung einer Ressourcenerkennung auf: disassociate-ipam-resource-discovery

Löschen einer Ressourcenerkennung

In diesem Abschnitt wird beschrieben, wie eine Ressourcenerkennung gelöscht wird.

> **Note**
>
> Sie können eine standardmäßige Ressourcenerkennung nicht löschen. Eine standardmäßige Ressourcenerkennung wird automatisch erstellt, wenn Sie ein IPAM erstellen. Die standardmäßige Ressourcenerkennung wird jedoch gelöscht, wenn Sie das IPAM löschen.

Dieser Schritt muss vom Administratorkonto der sekundären Organisation abgeschlossen werden. Weitere Informationen über die an diesem Prozess beteiligten Rollen finden Sie unter Prozessübersicht.

AWS Management Console

So löschen Sie eine Ressourcenerkennung

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Ressourcenergebnisse aus.
3. Wählen Sie eine Ressourcenerkennung aus und wählen Sie Aktionen > Ressourcenerkennung löschen.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

- So löschen Sie eine Ressourcenerkennung: delete-ipam-resource-discovery

Erstellen von zusätzlichen Bereichen

Führen Sie die Schritte in diesem Abschnitt aus, um einen zusätzlichen Bereich zu erstellen.

Ein Bereich ist der Container auf höchster Ebene innerhalb von IPAM. Wenn Sie ein IPAM erstellen, erstellt IPAM zwei Standardbereiche für Sie. Jeder Bereich repräsentiert den IP-Bereich für ein einzelnes Netzwerk. Der private Bereich ist für den gesamten privaten Raum gedacht. Der öffentliche Bereich ist für den gesamten öffentlichen Raum bestimmt. Mit Bereichen können Sie IP-Adressen in mehreren nicht verbundenen Netzwerken wiederverwenden, ohne dass sich die IP-Adresse überschneidet oder Konflikte verursachen muss.

Wenn Sie ein IPAM erstellen, werden Standardbereiche (ein privater und ein öffentlicher) für Sie erstellt. Sie können zusätzliche private Bereiche erstellen. Sie können keine zusätzlichen öffentlichen Bereiche erstellen.

Sie können zusätzliche private Bereiche erstellen, wenn Sie Unterstützung für mehrere getrennte private Netzwerke benötigen. Zusätzliche private Bereiche ermöglichen es Ihnen, Pools zu erstellen und Ressourcen zu verwalten, die denselben IP-Bereich verwenden.

> **Important**
>
> Wenn IPAM Ressourcen mit privaten IPv4-CIDRs entdeckt, werden die Ressourcen-CIDRs in den privaten Standardbereich importiert und erscheinen in keinem zusätzlichen privaten Bereich, den Sie erstellen. Sie können CIDRs vom privaten Standardbereich in einen anderen privaten Bereich verschieben. Weitere Informationen finden Sie unter Verschieben von VPC CIDRs zwischen Bereichen.

AWS Management Console

Einen zusätzlichen privaten Bereich erstellen

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Scopes (Bereiche) aus.
3. Wählen Sie Create scope (Bereich erstellen).

4. Wählen Sie das IPAM aus, dem Sie den Bereich hinzufügen möchten.
5. Eine Beschreibung für den Bereich hinzufügen.
6. Wählen Sie Create scope (Bereich erstellen).
7. Sie können den Bereich in IPAM anzeigen, indem Sie Scopes (Bereiche) im Navigationsbereich wählen.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Erstellen eines zusätzlichen privaten Bereichs:

1. Zeigen Sie Ihre aktuellen Bereiche an: describe-ipam-scopes
2. Erstellen Sie einen neuen privaten Bereich: create-ipam-scope
3. Zeigen Sie Ihre aktuellen Bereiche an, um den neuen Bereich anzuzeigen: describe-ipam-scopes

Verschieben von VPC CIDRs zwischen Bereichen

Führen Sie die Schritte in diesem Abschnitt aus, um ein VPC CIDR von einem Bereich in einen anderen zu verschieben.

⚠ Important

- Sie können nur VPC CIDRs verschieben. Wenn Sie ein VPC CIDR verschieben, werden auch die Subnetz-CIDRs der VPC automatisch verschoben.
- Sie können VPC CIDRs nur von einem privaten Bereich in einen anderen verschieben. Sie können VPC CIDRs nicht aus einem öffentlichen Bereich in einen privaten Bereich oder aus einem privaten Bereich in einen öffentlichen Bereich verschieben.
- Dasselbe AWS-Konto muss beide Bereiche besitzen.
- Wenn ein VPC CIDR derzeit von einem Pool in einem privaten Bereich zugewiesen ist, ist die Verschiebungsanforderung erfolgreich, aber das VPC CIDR wird nicht verschoben, bis

Sie die VPC-CIDR-Zuweisung aus dem aktuellen Pool freigeben. Weitere Informationen zur Freigabe einer Zuordnung finden Sie unter Freigeben einer Zuordnung.

AWS Management Console

So verschieben Sie ein CIDR, das einer VPC zugewiesen ist

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Resources aus.
3. Wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten.
4. Wählen Sie im Inhaltsbereich eine VPC aus und zeigen Sie die Details der VPC an.
5. Wählen Sie unter VPC CIDRs eines der CIDRs aus, das der Ressource zugeordnet sind, und wählen Sie Actions (Aktionen) > Move CIDR to different scope (CIDR in einen anderen Bereich verschieben) aus.
6. Wählen Sie den Bereich aus, in den Sie das VPC CIDR verschieben möchten.
7. Wählen Sie CIDR in einen anderen Bereich verschieben aus.

Command line

Verwenden Sie die folgenden AWS CLI-Befehle, um ein VPC CIDR zu verschieben:

1. Erhalten Sie ein VPC CIDR im aktuellen Bereich: get-ipam-resource-cidrs
2. Verschieben Sie ein VPC CIDR: modify-ipam-resource-cidr
3. Erhalten Sie ein VPC CIDR im anderen Bereich: get-ipam-resource-cidrs

Ändern des Überwachungsstatus von VPC CIDRs

Führen Sie die Schritte in diesem Abschnitt aus, um den Überwachungsstatus eines VPC CIDR zu ändern. Möglicherweise möchten Sie ein VPC CIDR von „monitored“ (überwacht) in „ignored“ (ignoriert) ändern, wenn Sie nicht möchten, dass IPAM die VPC verwaltet oder überwacht und zulässt, dass der der VPC zugewiesene CIDR für die Verwendung verfügbar ist. Möglicherweise möchten Sie ein VPC CIDR von „ignored“ (ignoriert) in „monitored“ (überwacht) ändern, wenn IPAM das VPC CIDR verwaltet und überwacht.

> **Note**
>
> - Sie können VPC CIDRs im öffentlichen Bereich nicht ignorieren.
> - Wenn ein CIDR ignoriert wird, werden Ihnen trotzdem die aktiven IP-Adressen in der CIDR in Rechnung gestellt. Weitere Informationen finden Sie unter Preise für IPAM.
> - Wenn ein CIDR ignoriert wird, können Sie trotzdem den Verlauf der IP-Adressen im CIDR einsehen. Weitere Informationen finden Sie unter Verlauf der IP-Adresse anzeigen.

Sie können den Überwachungsstatus eines VPC CIDR in „monitored“ (überwacht) oder „ignored“ (ignoriert) ändern:

- Monitored (überwacht): Das VPC CIDR wurde von IPAM erkannt und wird auf Überschneidungen mit anderen CIDRs und Compliance von Zuordnungsregeln überwacht.
- Ignored (ignoriert): Das VPC CIDR wird von der Überwachung ausgenommen. Ignorierte VPC CIDRs werden nicht nach Überschneidungen mit anderen CIDRs oder Compliance von Zuordnungsregeln beurteilt. Sobald für ein VPC CIDR „ignore“ (ignorieren) ausgewählt wurde, wird jeglicher Speicherplatz, der ihm aus einem IPAM-Pool zugewiesen wurde, an den Pool zurückgegeben und das VPC CIDR wird nicht erneut per Auto-Import importiert (wenn die Zuweisungsregel für den Auto-Import für den Pool festgelegt ist).

AWS Management Console

So ändern Sie den Überwachungsstatus eines CIDR, das einer VPC zugewiesen ist

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Resources aus.
3. Wählen Sie im Dropdown-Menü oben im Inhaltsbereich den privaten Bereich aus, den Sie verwenden möchten.
4. Wählen Sie im Inhaltsbereich die VPC aus und zeigen Sie die Details der VPC an.
5. Wählen Sie unter VPC-CIDRs eines der dem VPC zugewiesenen CIDRs aus und wählen Sie Aktionen > Als ignoriert markieren oder Markierung als ignoriert aufheben.
6. Wählen Sie Mark as ignored (Als ignoriert markieren) oder Unmark as ignored (Markierung als ignoriert aufheben) aus.

Command line

Verwenden Sie die folgenden AWS CLI-Befehle zum Ändern des Überwachungsstatus eines VPC CIDR:

1. Holen Sie sich eine Bereichs-ID: describe-ipam-Scopes
2. Zeigen Sie den aktuellen Überwachungsstatus für das VPC CIDR an: get-ipam-resource-cidrs
3. Ändern Sie den Status des VPC CIDR: modify-ipam-resource-cidr
4. Zeigen Sie den neuen Überwachungsstatus für das VPC CIDR an: get-ipam-resource-cidrs

Einen Bereich löschen

Um einen IPAM-Bereich zu löschen, führen Sie die Schritte in diesem Abschnitt aus.

Important

Sie können einen Bereich nicht löschen, wenn einer der folgenden Punkte zutrifft:

- Der Bereich ist ein Standardbereich. Wenn Sie ein IPAM erstellen, werden zwei Standardbereiche (ein öffentlicher, ein privater) automatisch erstellt und können nicht gelöscht werden. Um zu sehen, ob ein Bereich ein Standardbereich ist, zeigen Sie den Bereichs-Typ in den Details des Bereichs.
- Es gibt eine oder mehrere Pools in dem Bereich. Sie müssen zuerst Einen Pool löschen wählen, bevor Sie den Bereich löschen können.

AWS Management Console

So löschen Sie einen Bereich

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Scopes (Bereiche) aus.
3. Wählen Sie im Inhaltsbereich den Bereich aus, den Sie löschen möchten.
4. Klicken Sie auf Actions (Aktionen) > Delete scope (Bereich löschen).
5. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie den folgenden Befehl AWS CLI, um einen Bereich zu löschen:

1. Bereichsbereiche anzeigen: describe-ipam-scopes
2. Einen Bereich löschen: delete-ipam-scope
3. Aktualisierte Bereiche anzeigen: describe-ipam-scopes

Um einen neuen Bereich zu erstellen, siehe Erstellen von zusätzlichen Bereichen. Um eine IPAM zu löschen, siehe Löschen Sie ein IPAM.

Eine Zuweisung freigeben

Führen Sie die Schritte in diesem Abschnitt aus, um eine CIDR-Zuweisung aus einem IPAM-Pool freizugeben. In der Zuweisung ist eine CIDR-Zuweisung von einem IPAM-Pool zu einer anderen Ressource oder einem IPAM-Pool.

Wenn Sie vorhaben, einen Pool zu löschen, müssen Sie möglicherweise eine Pool-Zuweisung freigeben. Sie können Pools nicht löschen, wenn für die Pools CIDRs bereitgestellt wurden und Sie können die Bereitstellung von CIDRs nicht aufheben, wenn den CIDRs Ressourcen zugeordnet sind.

Note

- Um eine manuelle Zuweisung freizugeben, führen Sie die Schritte in diesem Abschnitt aus oder rufen Sie ReleaseIpamPoolAllocation API auf.
- Um eine Zuweisung in einem privaten Bereich freizugeben, müssen Sie die Ressource-CIDR ignorieren oder löschen. Weitere Informationen finden Sie unter Ändern des Überwachungsstatus von VPC CIDRs. Nach einiger Zeit wird Amazon VPC IPAM die Zuteilung automatisch in Ihrem Namen freigeben.

  Example

  Beispiel

Wenn Sie eine VPC CIDR in einem privaten Bereich haben, müssen Sie das VPC CIDR entweder ignorieren oder löschen, um die Zuweisung freizugeben. Nach einiger Zeit wird Amazon VPC IPAM die VPC CIDR-Zuteilung automatisch aus dem IPAM-Pool freigeben.

- Um eine Zuweisung in einem öffentlichen Bereich freizugeben, müssen Sie die Ressource-CIDR löschen. Sie können CIDRs für öffentliche Ressourcen nicht ignorieren. Weitere Informationen finden Sie unter Bereinigen in Bringen Sie Ihr eigenes öffentliches IPv4-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS oder Bereinigen in Bringen Sie Ihr eigenes IPv6-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS. Nach einiger Zeit wird Amazon VPC IPAM die Zuteilung automatisch in Ihrem Namen freigeben.

Damit Amazon VPC IPAM Zuweisungen in Ihrem Namen freigeben kann, müssen alle Kontoberechtigungen für entweder die Verwendung eines Einzelkontos oder die Verwendung von mehreren Kontenrichtig konfiguriert sein.

Wenn Sie ein CIDR veröffentlichen, das von Ihrem IPAM verwaltet wird, recycelt Amazon VPC IPAM das CIDR wieder in einen IPAM-Pool. Es dauert einige Minuten, bis das CIDR für zukünftige Zuteilungen verfügbar ist. Weitere Informationen zu Pools und Zuweisungen finden Sie unter Funktionsweise von IPAM.

AWS Management Console

So geben Sie eine Pool-Zuweisung frei

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie im Inhaltsbereich den Pool aus, in dem sich die Zuweisung befindet.
5. Wählen Sie die Registerkarte Allocations (Zuweisungen).
6. Wählen Sie eine oder mehr Zuordnungen aus. Sie können Zuordnungen anhand ihres Ressourcentyps identifizieren:
   - custom:: Eine benutzerdefinierte Zuordnung.
   - vpc: Eine VPC-Zuordnung.

- ipam-pool: Eine IPAM-Pool-Zuordnung.
- ec2-public-ipv4-pool: Eine öffentliche IPv4-Pool-Zuordnung.

7. Wählen Sie Actions (Aktionen) > Release custom allocation (Benutzerdefinierte Zuordnung freigeben) aus.
8. Klicken Sie auf Deallocate CIDR (Zuweisungen von CIDR aufheben).

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zum Freigeben einer Pool-Zuweisung:

1. Holen Sie sich eine IPAM-Pool-ID: describe-ipam-Pools
2. Sehen Sie sich Ihre aktuellen Zuweisungen im Pool an: get-ipam-pool-allocations
3. Eine Zuweisung freigeben: release-ipam-pool-allocation
4. Sehen Sie sich Ihre aktualisierten Zuweisungen an: get-ipam-pool-allocations

Um eine neue Zuweisung hinzuzufügen, siehe Zuweisen von CIDRs. Um den Pool nach der Freigabe von Zuweisungen zu löschen, müssen Sie zuerst Deprovisionierung von CIDRs aus einem Pool.

Ändern eines IPAMs

Um einen IPAM zu ändern, führen Sie die Schritte in diesem Abschnitt aus.

Inhalt

Ändern einer IPAM-Stufe

Um eine IPAM-Stufe zu ändern, führen Sie die Schritte in diesem Abschnitt aus. IPAM bietet zwei Stufen: das kostenlose Kontingent und das erweiterte Kontingent. Weitere Informationen zu den im

kostenlosen Kontingent verfügbaren Features und den Kosten des erweiterten Kontingents finden Sie unter Preise für Amazon VPC auf der Registerkarte „IPAM“.

> **Important**
>
> Bevor Sie vom erweiterten Kontingent zum kostenlosen Kontingent wechseln können, müssen Sie:
>
> - Pools mit privatem Geltungsbereich löschen.
> - Private Nicht-Standard-Pools löschen.
> - Pools mit anderen Gebietsschemas als der IPAM-Heimatregion löschen.
> - Nicht standardmäßige Ressourcenerkennungszuordnungen löschen.
> - Poolzuweisungen für Konten löschen, die nicht der IPAM-Besitzer sind.

AWS Management Console

So ändern Sie die IPAM-Stufe

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich die Option IPAMs.
3. Wählen Sie im Inhaltsbereich Ihr IPAM aus.
4. Wählen Sie Actions (Aktionen) und Edit (Bearbeiten).
5. Wählen Sie die IPAM-Stufe aus, die Sie für den IPAM verwenden möchten.
6. Wählen Sie Save Changes.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle, um eine IPAM-Stufe anzuzeigen und zu ändern:

1. Zeigen Sie aktuelle IPAMs an: describe-ipams
2. Ändern Sie die IPAM-Stufe: modify-ipam
3. Sehen Sie sich Ihre aktualisierten IPAMs unter: describe-ipams an

Ändern der IPAM-Betriebsregionen

Um die IPAM-Betriebsregionen zu ändern, führen Sie die Schritte in diesem Abschnitt aus. Betriebsregionen sind AWS-Regionen, in denen das IPAM IP-Adressen-CIDRs verwalten darf. IPAM entdeckt und überwacht Ressourcen nur in AWS-Regionen, die Sie als Betriebsregionen auswählen.

AWS Management Console

So ändern Sie die IPAM-Betriebsregionen

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich die Option IPAMs.
3. Wählen Sie im Inhaltsbereich Ihr IPAM aus.
4. Wählen Sie Actions (Aktionen) und Edit (Bearbeiten).
5. Wählen Sie unter IPAM-Einstellungen die Betriebsregionen aus, die Sie für den IPAM verwenden möchten.
6. Wählen Sie Save Changes.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle, um IPAM-Betriebsregionen anzuzeigen und zu ändern:

1. Zeigen Sie aktuelle IPAMs an: describe-ipams
2. Hinzufügen oder Entfernen der IPAM-Betriebsregionen: modify-ipam
3. Sehen Sie sich Ihre aktualisierten IPAMs unter: describe-ipams an

Löschen Sie ein IPAM

Um einen IPAM zu löschen, führen Sie die Schritte in diesem Abschnitt aus. Informationen zum Erhöhen der Standardanzahl von IPAMs, die Sie verwenden können, anstatt ein vorhandenes IPAM zu löschen, finden Sie unter Kontingente für Ihr IPAM.

> **Important**
>
> Durch das Löschen eines IPAM werden alle überwachten Daten entfernt, die mit dem IPAM verbunden sind, einschließlich der Verlaufsdaten für CIDRs.

AWS Management Console

So löschen Sie einen IPAM

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich die Option IPAMs.
3. Wählen Sie im Inhaltsbereich Ihr IPAM aus.
4. Wählen Sie Actions (Aktionen) und Delete IPAM (IPAM löschen).
5. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf Cascade delete (Cascaden-löschen), um das IPAM, private Bereiche, Pools in privaten Bereichen und alle Zuweisungen in den Pools in privaten Bereichen zu löschen. Sie können das IPAM mit dieser Option nicht löschen, wenn sich in Ihrem öffentlichen Bereich ein Pool befindet. Wenn Sie diese Option verwenden, führt IPAM Folgendes aus:
     - Gibt alle CIDRs frei, die VPC-Ressourcen (wie VPCs) in Pools in privaten Bereichen zugewiesen sind.

       > **Note**
       >
       > Durch die Aktivierung dieser Option werden keine VPC-Ressourcen gelöscht. Der mit der Ressource verbundene CIDR wird nicht mehr aus einem IPAM-Pool zugewiesen, aber der CIDR selbst bleibt unverändert.

     - Hebt alle IPv4-CIDRs, die für IPAM-Pools bereitgestellt werden, in privaten Bereichen auf.
     - Löscht alle IPAM-Pools in privaten Bereichen.
     - Löscht alle nicht standardmäßigen privaten Bereiche im IPAM.
     - Löscht die standardmäßigen öffentlichen und privaten Bereiche sowie das IPAM.
   - Wenn Sie die Checkbox Cascade delete (Cascaden-löschen) nicht auswählen, bevor Sie ein IPAM löschen können, müssen Sie Folgendes tun:

- Geben Sie Zuweisungen innerhalb der IPAM-Pools frei. Weitere Informationen finden Sie unter Eine Zuweisung freigeben.
- Heben Sie die Bereitstellung von CIDRs auf, die für Pools innerhalb des IPAM bereitgestellt wurden. Weitere Informationen finden Sie unter Deprovisionierung von CIDRs aus einem Pool.
- Löschen Sie alle zusätzlichen nicht standardmäßigen Bereiche. Weitere Informationen finden Sie unter Einen Bereich löschen.
- Löschen Sie Ihre IPAM-Pools. Weitere Informationen finden Sie unter Einen Pool löschen.

6. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie den folgenden Befehl AWS CLI, um ein IPAM zu löschen:

1. Zeigen Sie aktuelle IPAMs an: describe-ipams
2. Löschen Sie ein IPAM: delete-ipam
3. Sehen Sie sich Ihre aktualisierten IPAMs unter: describe-ipams an

Um eine neue IPAM zu erstellen, siehe Erstellen eines IPAM.

Verfolgung der IP-Adressnutzung in IPAM

Die in diesem Abschnitt beschriebenen Aufgaben sind optional. Wenn Sie die Aufgaben in diesem Abschnitt erledigen möchten und ein IPAM-Konto delegiert haben, sollten die Aufgaben vom IPAM-Konto erledigt werden.

Führen Sie zum Nachverfolgen der Verwendung der IP-Adresse mit IPAM die Schritte in diesem Abschnitt aus.

Inhalt

Überwachen der CIDR-Nutzung mit dem IPAM-Dashboard

Führen Sie die Schritte in diesem Abschnitt aus, um auf das IPAM-Dashboard zuzugreifen und den Status aller CIDRs innerhalb eines bestimmten IPAM-Bereichs anzuzeigen.

AWS Management Console

So überwachen Sie die CIDR-Nutzung mit dem IPAM-Dashboard

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Wenn Sie das Dashboard anzeigen, ist standardmäßig der private Standardbereich ausgewählt. Wenn Sie den privaten Standardbereich nicht verwenden möchten, wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Das Dashboard bietet einen Überblick über Ihre IPAM-Pools und CIDRs innerhalb eines Bereichs. Sie können Widgets hinzufügen, entfernen, verschieben und die Größe ändern, um das Dashboard zu personalisieren.

- Scope (Bereich): Die Details zu diesem Bereich. Ein Bereich ist der Container auf höchster Ebene innerhalb von IPAM. Ein IPAM enthält zwei Standardbereiche, einen privaten Bereich und einen öffentlichen Bereich. Jeder Bereich repräsentiert den IP-Bereich für ein einzelnes Netzwerk. Sie können mehrere private Bereiche haben, aber Sie können nur einen öffentlichen Bereich haben.
  - Scope ID (Bereich ID): Die ID für diesen Bereich.
  - Scope type (Bereich-Typ): Die Art des Bereichs.
  - IPAM ID (IPAM-ID): Die ID des IPAM, in dem sich der Bereich befindet.
  - IPAM-Pools in diesem Bereich: Die ID des IPAM, in dem sich der Bereich befindet.
  - Netzwerkressourcen in diesem Bereich anzeigen: Führt Sie zum Abschnitt Ressourcen der IPAM-Konsole.
  - In diesem Bereich den Verlauf einer IP-Adresse durchsuchen: Führt Sie zum Abschnitt IP-Verlauf durchsuchen der IPAM-Konsole.
- Ressourcen-CIDR-Typen: Die Arten von Ressourcen-CIDRs im Bereich.
  - Subnetz: Die Anzahl der CIDRs für Subnetze.
  - VPC: Die Anzahl der CIDRs für VPCs.
  - EIPs: Die Anzahl der CIDRs für Elastic-IP-Adressen.
  - Öffentliche IPv4-Pools: Die Anzahl der CIDRs für öffentliche IPv4-Pools.
- Verwaltungsstatus: Der Verwaltungsstatus der CIDRs.
  - Managed CIDRs (Nicht verwaltete CIDRs): Die Anzahl der Ressourcen-CIDRs für nicht verwaltete Ressourcen in diesem Bereich.
  - Ignored CIDRs (Ignorierte CIDRs): Die Anzahl der Ressourcen-CIDRs, die Sie ausgewählt haben, um von der Überwachung mit IPAM befreit zu sein. IPAM wertet ignorierte Ressourcen nicht auf Überschneidungen oder Compliance innerhalb eines Bereichs aus. Wenn eine Ressource ignoriert wird, wird der ihr zugewiesene Speicherplatz aus einem IPAM-Pool an den Pool zurückgegeben und die Ressource wird nicht erneut durch automatischen Import importiert (wenn die automatische Importzuordnungsregel für den Pool festgelegt ist).
  - Managed CIDRs (Verwaltete CIDRs): Die Anzahl der Ressourcen-CIDRs für verwaltbare Ressourcen (VPCs oder öffentliche IPv4-Pools), die aus einem IPAM-Pool im Bereich zugewiesen werden.

- Überlappende Ressourcen-CIDRs: Die Anzahl der überlappenden und nicht überlappenden CIDRs. Überlappende CIDRs können zu einem falschen Routing in Ihren VPCs führen.
  - Overlapping CIDRs (Überlappende CIDRs): Die Anzahl der CIDRs, die sich in diesem Bereich derzeit innerhalb der IPAM-Pools überschneiden. Überlappende CIDRs können zu einem falschen Routing in Ihren VPCs führen.
  - Überlappende CIDRs: Die Anzahl der Ressourcen-CIDRs, die sich innerhalb der IPAM-Pools im Bereich nicht überlappen.
- Konforme Ressourcen-CIDRs: Die Anzahl der konformen Ressourcen-CIDRs.
  - Compliant CIDRs (Konforme CIDRs): Die Anzahl der Ressourcen-CIDRs, die den Zuordnungsregeln für IPAM-Pools im Bereich entsprechen.
  - Noncompliant CIDRs (Nicht konforme CIDRs): Die Anzahl der Ressourcen-CIDRs, die nicht den Zuteilungsregeln für die IPAM-Pools im Bereich entsprechen.
- Überlappungsstatus: Die Anzahl der CIDRs, die sich im Laufe der Zeit überschneiden.
  - Überlappende Ressourcen-CIDRs: Die Anzahl der CIDRs, die sich in diesem Bereich innerhalb der IPAM-Pools überlappen. Überlappende CIDRs können zu einem falschen Routing in Ihren VPCs führen.
- Konformitätsstatus: Die Anzahl der CIDRs, die den Zuordnungsregeln für IPAM-Pools im Bereich im Bereich im Bereich im Bereich im Verlauf der Zeit entsprechen oder nicht entsprechen.
  - Konforme Ressourcen-CIDRs: Die Anzahl der Ressourcen-CIDRs, die den Zuordnungsregeln entsprechen.
  - Nicht konforme Ressourcen-CIDRs: Die Anzahl der Ressourcen-CIDRs, die den Zuordnungsregeln nicht entsprechen.
- VPC-Auslastung: VPCs (IPv4 und IPv6) mit der höchsten oder geringsten IP-Auslastung. Mithilfe dieser Informationen können Sie Amazon-CloudWatch-Alarme konfigurieren, die ausgelöst werden, wenn ein Schwellenwert der IP-Auslastung überschritten wird. Weitere Informationen finden Sie unter Metriken zur Ressourcenauslastung.
- Subnetz-Auslastung: Subnetze (nur IPv4) mit der höchsten oder geringsten IP-Auslastung. Anhand dieser Informationen können Sie entscheiden, ob Sie wenig ausgelastete Ressourcen behalten oder löschen möchten. Weitere Informationen finden Sie unter Metriken zur Ressourcenauslastung.

- VPCs mit den höchsten zugewiesenen IP-Adressen: Die VPCs mit dem höchsten Prozentsatz an IP-Adressraum, der Subnetzen zugewiesen ist. Dies ist nützlich, um Ihnen zu zeigen, ob Sie den VPCs zusätzlichen IP-Adressraum bereitstellen müssen.
- Subnetze mit den höchsten zugewiesenen IP-Adressen: Die Subnetze mit dem höchsten Prozentsatz an IP-Adressraum, der Ressourcen zugewiesen ist. Dies ist nützlich, um Ihnen zu zeigen, ob Sie den Subnetzen zusätzlichen IP-Adressraum bereitstellen müssen.
- Pool-Zuweisung: Der Prozentsatz des IP-Raums, der Ressourcen und manuellen Zuweisungen im Bereich im Verlauf der Zeit zugewiesen wurde.
- Pool-Zuordnung: Der Prozentsatz des IP-Raums eines Pools, der anderen Pools im Bereich im Verlauf der Zeit zugeordnet wurde.

Command line

Die im Dashboard angezeigten Informationen stammen aus Metriken, die in Amazon CloudWatch gespeichert sind. Für weitere Informationen zu den in Amazon CloudWatch gespeicherten Metriken siehe Überwachen Sie IPAM mit Amazon CloudWatch. Verwenden Sie die Amazon-CloudWatch-Optionen in der AWS-CLI-Referenz, um Metriken für Zuweisungen in Ihren IPAM-Pools und IPAM-Bereichen anzuzeigen.

Wenn Sie feststellen, dass das für einen Pool bereitgestellte CIDR fast vollständig zugewiesen ist, müssen Sie möglicherweise zusätzliche CIDRs bereitstellen. Weitere Informationen finden Sie unter Bereitstellen von CIDRs für einen Pool.

Überwachen Sie die CIDR-Nutzung nach Ressourcen

In IPAM ist eine Ressource eine AWS-Serviceeinheit, der eine IP-Adresse oder ein CIDR-Block zugewiesen ist. IPAM verwaltet einige Ressourcen, überwacht aber nur andere Ressourcen.

- Managed resource (Verwaltete Ressource): Eine verwaltete Ressource hat ein CIDR aus einem IPAM-Pool zugewiesen. IPAM überwacht das CIDR auf mögliche Überschneidungen der IP-Adresse mit anderen CIDRs im Pool und überwacht die Compliance der Zuweisungsregeln eines Pools durch das CIDR. IPAM unterstützt die Verwaltung der folgenden Arten von Ressourcen:
  - VPCs
  - Öffentliche IPv4-Pools

> **Important**
>
> Öffentliche IPv4-Pools und IPAM-Pools werden von unterschiedlichen Ressourcen in AWS verwaltet. Öffentliche IPv4-Pools sind Einzelkonto-Ressourcen, mit denen Sie Ihre öffentlichen CIDRs in elastische IP-Adressen konvertieren können. IPAM-Pools können verwendet werden, um Ihren öffentlichen Raum öffentlichen IPv4-Pools zuzuweisen.

- Monitored resource (Überwachte Ressource): Wenn eine Ressource von IPAM überwacht wird, wurde die Ressource von IPAM erkannt und Sie können Details zum CIDR der Ressource anzeigen, wenn Sie `get-ipam-resource-cidrs` mit der AWS-CLI verwenden oder wenn Sie Resources (Ressourcen) im Navigationsbereich anzeigen. IPAM unterstützt die Überwachung der folgenden Ressourcen:
  - VPCs
  - Öffentliche IPv4-Pools
  - VPC-Subnetze
  - Elastic-IP-Adressen

Die folgenden Schritte zeigen, wie Sie die Compliance von CIDR-Nutzungs- und Zuweisungsregeln nach Ressource überwachen.

AWS Management Console

Überwachen der CIDR-Nutzung nach Ressourcen

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Resources aus.
3. Wählen Sie im Dropdown-Menü oben im Inhaltsbereich den gewünschten Bereich aus. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Verwenden Sie die Ressourcen-CIDR-Map, um den verfügbaren, zugewiesenen und sich überschneidenden IP-Adressraum in einem Bereich anzuzeigen:
   - Verfügbar: Ein IP-Adressbereich steht für die Zuweisung zur Verfügung.
   - Konform und nicht überlappend: Ein IP-Adressbereich wird einer von IPAM verwalteten Ressource zugewiesen.
   - Belegt: Einer Ressource ist ein IP-Adressbereich zugewiesen.

- Überlappend: Ein IP-Adressbereich wurde mehreren Ressourcen zugewiesen und überlappt sich.
- Nicht konform: Ein IP-Adressbereich ist nicht konform. Es gibt eine Ressource, die den IP-Adressbereich verwendet und nicht den für den Pool festgelegten Zuweisungsregeln entspricht.

Wählen Sie in der CIDR-Map einen IP-Adressblock im unteren Bereich der Map aus, um die Ressourcen in kleineren CIDR-Blöcken anzuzeigen. Wählen Sie in der CIDR-Map einen IP-Adressblock im oberen Bereich der Map aus, um die Ressourcen in größeren CIDR-Blöcken anzuzeigen.

5. In der Tabelle finden Sie die folgenden Details zu den Ressourcen im Bereich:

- Name (Ressourcen-ID): Der Name und die Ressourcen-ID der Ressource.
- CIDR: Das mit der Ressource verknüpfte CIDR.
- Management state (Status des Managements): Der Status der Ressource.
  - Managed (Verwaltet): Der Ressource ist ein CIDR aus einem IPAM-Pool zugewiesen und wird von IPAM auf potenzielle CIDR-Überlappungen und die Compliance der Pool-Zuweisungsregeln überwacht.
  - Unmanaged (Nicht verwaltet): Der Ressource ist kein CIDR aus einem IPAM-Pool zugewiesen und wird von IPAM nicht auf mögliche CIDR-Compliance der Pool-Zuweisungsregeln überwacht. Das CIDR wird auf Überlappungen überwacht.
  - Ignored (Ignoriert): Die Ressource wurde ausgewählt, um von der Überwachung ausgenommen zu sein. Ignorierte Ressourcen werden nicht auf Überschneidungs- oder Zuweisungsregel-Compliance bewertet. Wenn eine Ressource ignoriert wird, wird der ihr zugewiesene Speicherplatz aus einem IPAM-Pool an den Pool zurückgegeben und die Ressource wird nicht erneut durch automatischen Import importiert (wenn die automatische Importzuordnungsregel für den Pool festgelegt ist).
  - –: Diese Ressource gehört nicht zu den Ressourcentypen, die von IPAM verwaltet werden können.
- Compliance status (Compliance-Status): Der Compliance-Status des CIDR.
  - Compliant (Konform): Eine verwaltete Ressource entspricht den Zuordnungsregeln des IPAM-Pools.
  - Noncompliant (Nicht konform): Das Ressourcen-CIDR entspricht nicht einer oder mehreren der Zuweisungsregeln des IPAM-Pools.

Example

Wenn eine VPC über ein CIDR verfügt, das die Netzmaskenlängenparameter des IPAM-Pools nicht erfüllt, oder wenn sich die Ressource nicht in derselben AWS-Region befindet wie der IPAM-Pool wird er als nicht konform gekennzeichnet.

- Unmanaged (Nicht verwaltet): Der Ressource ist kein CIDR aus einem IPAM-Pool zugewiesen und wird von IPAM nicht auf mögliche CIDR-Compliance der Pool-Zuweisungsregeln überwacht. Das CIDR wird auf Überlappungen überwacht.
- Ignored (Ignoriert): Die Ressource wurde ausgewählt, um von der Überwachung ausgenommen zu sein. Ignorierte Ressourcen werden nicht auf Überschneidungs- oder Zuweisungsregel-Compliance bewertet. Wenn eine Ressource ignoriert wird, wird der ihr zugewiesene Speicherplatz aus einem IPAM-Pool an den Pool zurückgegeben und die Ressource wird nicht erneut durch automatischen Import importiert (wenn die automatische Importzuordnungsregel für den Pool festgelegt ist).
- –: Diese Ressource gehört nicht zu den Ressourcentypen, die von IPAM verwaltet werden können.

- Overlap status (Überlappungsstatus): Der Überlappungsstatus vom CIDR.
  - Nonoverlapping (Nicht überlappend): Die Ressource CIDR überlappt sich nicht mit einem anderen CIDR im gleichen Bereich.
  - Overlapping (Überlappend): Das Ressourcen-CIDR überlappt sich mit einem anderen CIDR im gleichen Bereich. Beachten Sie, dass wenn sich ein Ressourcen-CIDR überlappt, es möglicherweise mit einer manuellen Zuordnung überlappen kann.
  - Ignored (Ignoriert): Die Ressource wurde ausgewählt, um von der Überwachung ausgenommen zu sein. IPAM wertet ignorierte Ressourcen nicht auf Überschneidungen oder die Compliance von Zuweisungsregeln aus. Wenn eine Ressource ignoriert wird, wird der ihr zugewiesene Speicherplatz aus einem IPAM-Pool an den Pool zurückgegeben und die Ressource wird nicht erneut durch automatischen Import importiert (wenn die automatische Importzuordnungsregel für den Pool festgelegt ist).
  - –: Diese Ressource gehört nicht zu den Ressourcentypen, die von IPAM verwaltet werden können.
- IP-Nutzung: Bei Ressourcen, die VPCs sind, entspricht dies dem Prozentsatz des IP-Adressraums in der VPC, der von Subnetz-CIDRs belegt wird. Für Ressourcen, die Subnetze sind und für das Subnetz ein IPv4-CIDR bereitgestellt wurde, ist dies der Prozentsatz des IPv4-Adressraums im Subnetz, der verwendet wird. Wenn für das Subnetz

ein IPv6-CIDR bereitgestellt ist, wird der Prozentsatz des verwendeten IPv6-Adressraums nicht dargestellt. Der Prozentsatz des verwendeten IPv6-Adressraums kann derzeit nicht berechnet werden. Bei Ressourcen, bei denen es sich um öffentliche IPv4-Pools handelt, ist dies der Prozentsatz des IP-Adressbereich im Pool, der Elastic-IP-Adressen (EIPs) zugewiesen wurde.

- Region: Die AWS-Region der Ressource.
- Owner ID (ID des Eigentümers): Die AWS-Konto-ID der Person, die diese Ressource erstellt hat.
- Ressourcentyp: Ob es sich bei der Ressource um eine VPC, ein Subnetz, eine Elastic IP-Adresse oder einen öffentlichen IPv4-Pool handelt.
- Pool-ID: Die ID des IPAM-Pools, in dem sich die Ressource befindet.

6. Verwenden Sie Ressourcen filtern, um die Ressourcentabelle nach Spalteneigenschaften wie VPC-ID oder Konformitätsstatus zu filtern.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

Verwenden Sie die folgenden AWS CLI-Befehle zur Überwachung der CIDR-Nutzung nach Ressource:

1. Fordern Sie die Bereichs-ID an: describe-ipam-scopes
2. Ressourceninformationen anfordern: get-ipam-resource-cidrs

Überwachen Sie IPAM mit Amazon CloudWatch

IPAM speichert automatisch Metriken zur Nutzung von IP-Adressen (z. B. den in Ihren IPAM-Pools verfügbaren IP-Adressraum und die Anzahl der Ressourcen-CIDRs, die den Zuweisungsregeln entsprechen) und zur Ressourcenauslastung im Amazon-CloudWatch-Namespace von `AWS/IPAM` in der Heimatregion Ihres IPAM.

Inhalt

IPAM-Pool- und -Bereichsmetriken

IPAM veröffentlicht Daten über Ihre IPAM-Pools und -Bereiche in Amazon CloudWatch. Sie können diese Metriken verwenden, um Alarme für IPAM-Pools zu erstellen, die Sie benachrichtigen, wenn die Adresspools fast erschöpft sind oder wenn Ressourcen die für einen Pool festgelegten Zuweisungsregeln nicht einhalten. Das Erstellen von Alarmen und das Einrichten von Benachrichtigungen mit Amazon CloudWatch ist nicht Gegenstand dieses Abschnitts. Weitere Informationen finden Sie unter Verwenden von Amazon CloudWatch-Alarmen im Amazon CloudWatch-Benutzerhandbuch.

Die Speichermetriken und Dimensionen, die IPAM an Amazon CloudWatch sendet, sind unten aufgeführt.

Metriken zu IPAM-Pools

Metrikname	Beschreibung
CompliantResourceCidrs	Die Anzahl der verwalteten Ressourcen-CIDRs, die den Zuordnungsregeln für IPAM-Pools im Bereich entsprechen. Weitere Informationen zu Zuweisungsregeln finden Sie unter Erstellen eines IPv4-Pools der obersten Ebene.
NoncompliantResourceCidrs	Die Anzahl der verwalteten Ressourcen-CIDRs, die den Zuordnungsregeln für IPAM-Pools im Bereich nicht entsprech en. Weitere Informationen zu Zuweisungsregeln finden Sie unter Erstellen eines IPv4-Pools der obersten Ebene.
PercentAllocated	Der Prozentsatz des IP-Speicherplatzes eines Pools, der anderen Pools zugewiesen wurde.
PercentAssigned	Der Prozentsatz eines Pool-IP-Speicherplatzes, der Ressourcen zugewiesen wurde, einschließlich manueller Zuweisungen.
PercentAvailable	Der Prozentsatz des IP-Speicherplatzes eines Pools, der anderen Pools nicht zugewiesen wurde.

Metriken zu IPAM-Bereichen

Metrikname	Beschreibung
CompliantResourceCidrs	Die Anzahl der Ressourcen-CIDRs, die den Zuordnungsregeln für IPAM-Pools im Bereich entsprechen.
ManagedResourceCidrs	Die Anzahl der Ressourcen-CIDRs für verwaltbare Ressourcen (VPCs oder öffentliche IPv4-Pools), die aus einem IPAM-Pool im Bereich zugewiesen werden.
NoncompliantResourceCidrs	Die Anzahl der Ressourcen-CIDRs, die nicht den Zuteilung sregeln für die IPAM-Pools im Bereich entsprechen.
OverlappingResourceCidrs	Die Anzahl der Ressourcen-CIDRs, die sich innerhalb eines Pools im Bereich überschneiden.
UnmanagedResourceCidrs	Die Anzahl der Ressourcen-CIDRs im Geltungsbereich, die derzeit mit verwaltbaren Ressourcen verknüpft sind, aber nicht von IPAM verwaltet werden.

Die Dimensionen, die Sie verwende können, um IPAM-Metriken zu filtern, sind nachstehend aufgeführt.

Dimension	Beschreibung
AddressFamily	Die IP-Adressfamilie für Ressourcen-CIDRs (IPv4 oder IPv6).
Locale	Das Gebietsschemas ist die AWS-Region, in der ein IPAM-Pool für Zuweisungen verfügbar ist.
PoolID	Die ID eines Pools.
ScopeID	Die ID eines Bereichs.

Informationen zur Überwachung von VPCs mit Amazon CloudWatch finden Sie unter CloudWatch-Metriken für Ihre VPCs im Benutzerhandbuch für Amazon Virtual Private Cloud.

Metriken zur Ressourcenauslastung

IPAM veröffentlicht IP-Auslastungsmetriken für Ressourcen, die IPAM überwacht, in Amazon CloudWatch. Zu diesen Ressourcen gehören:

- VPCs (IPv4 und IPv6)
- Subnetze (IPv4)
- Öffentliche IPv4-Pools

IPAM berechnet und veröffentlicht IP-Auslastungsmetriken getrennt nach IP-Adressfamilie (IPv4 oder IPv6). Die IP-Auslastung einer Ressource wird für alle CIDRs derselben Adressfamilie berechnet.

Für jede Kombination aus Ressourcentyp und Adressfamilie bestimmt IPAM anhand von drei Regeln, welche Metriken veröffentlicht werden sollen:

- Bis zu 50 Ressourcen mit der höchsten IP-Auslastung. Mithilfe dieser Informationen können Sie Alarme konfigurieren, die ausgelöst werden, wenn ein Schwellenwert der IP-Auslastung überschritten wird.
- Bis zu 50 Ressourcen mit der geringsten IP-Auslastung. Anhand dieser Informationen können Sie entscheiden, ob Sie wenig ausgelastete Ressourcen behalten oder löschen möchten.
- Bis zu 50 weitere Ressourcen. Mithilfe dieser Informationen können Sie die IP-Auslastung von Ressourcen kontinuierlich verfolgen, die in der Gruppe mit hoher oder geringer Auslastung möglicherweise nicht erfasst werden.
  - Bis zu 50 VPCs mit einem CIDR, das aus einem IPAM-Pool zugewiesen wurde (priorisiert nach der Gesamtgröße der CIDR-Blöcke).
  - Bis zu 50 Subnetze, deren VPC ein CIDR enthält, das aus einem IPAM-Pool zugewiesen wurde (priorisiert nach der Gesamtgröße der CIDR-Blöcke).
  - Bis zu 50 öffentliche IPv4-Pools mit einem CIDR, das aus einem IPAM-Pool zugewiesen wurde (priorisiert nach der Gesamtgröße der CIDR-Blöcke).

Nach Anwendung der einzelnen Regeln werden die Metriken aggregiert und für jeden Ressourcentyp unter demselben Metriknamen veröffentlicht. Im Folgenden finden Sie ausführliche Informationen zu den Metriknamen und den Dimensionen.

> **Important**
>
> Für jede Kombination aus Ressourcentyp, Adressfamilie und Regel gibt es jeweils ein eigenes Limit. Der Standardwert der Limits beträgt 50. Diese Limits können Sie anpassen, indem Sie das AWS Support Center kontaktieren, wie unter AWS-Servicekontingente in der Allgemeine AWS-Referenz beschrieben.

Example Beispiel

Angenommen, IPAM überwacht 2 500 VPCs und 10 000 Subnetze, alle mit IPv4- und IPv6-CIDRs. IPAM veröffentlicht die folgenden Metriken zur IP-Auslastung:

- Bis zu 150 Metriken für die VPC-IPv4-Auslastung, darunter:
  - Die 50 VPCs mit der höchsten IPv4-Auslastung
  - Die 50 VPCs mit der geringsten IPv4-Auslastung
  - Bis zu 50 VPCs mit einem IPv4-CIDR, das aus einem IPAM-Pool zugewiesen wurde
- Bis zu 150 Metriken für die VPC-IPv6-Auslastung, darunter:
  - Die 50 VPCs mit der höchsten IPv6-Auslastung
  - Die 50 VPCs mit der geringsten IPv6-Auslastung
  - Bis zu 50 VPCs mit einem IPv6-CIDR, das aus einem IPAM-Pool zugewiesen wurde
- Bis zu 150 Metriken für die Subnetz-IPv4-Auslastung, darunter:
  - Die 50 Subnetze mit der höchsten IPv4-Auslastung
  - Die 50 Subnetze mit der geringsten IPv4-Auslastung
  - Bis zu 50 Subnetze, deren VPC ein IPv4-CIDR enthält, das aus einem IPAM-Pool zugewiesen wurde

VPC-Metriken

Der Name und die Beschreibung der VPC-Metriken sind nachfolgend aufgeführt.

Metrikname	Beschreibung
VpcIPUsage	Die Gesamtzahl der durch CIDRs abgedeckten IP-Adressen in den Subnetzen der VPC, dividiert durch die Gesamtzahl der

Metrikname	Beschreibung
	durch CIDRs abgedeckten IP-Adressen in der VPC. Dies wird für alle VPC-CIDRs im selben IPAM-Bereich sowie getrennt für IPv4- und IPv6-CIDRs berechnet.

Die Dimensionen, mit deren Hilfe Sie IPAM-Metriken filtern können, sind nachstehend aufgeführt.

Dimension	Beschreibung
AddressFamily	Die IP-Adressfamilie für Ressourcen-CIDRs (IPv4 oder IPv6).
OwnerID	Die ID des VPC-Eigentümers.
Region	Die AWS-Region, in der sich die VPC befindet.
ScopeID	Die ID des IPAM-Bereichs, dem die VPC angehört.
VpcID	Die ID des VPC.

Subnetzmetriken

Der Name und die Beschreibung der Subnetzmetriken sind nachfolgend aufgeführt.

Metrikname	Beschreibung
SubnetIPUsage	Die Anzahl der aktiven IP-Adressen, dividiert durch die Gesamtzahl der IP-Adressen im IPv4-CIDR des Subnetzes.

Die Dimensionen, mit deren Hilfe Sie Subnetzmetriken filtern können, sind nachstehend aufgeführt.

Dimension	Beschreibung
AddressFamily	Die IP-Adressfamilie für Ressourcen-CIDRs (nur IPv4).
OwnerID	Die ID des Subnetzeigentümers.

Dimension	Beschreibung
Region	Die AWS-Region, in der sich das Subnetz befindet.
ScopeID	Die ID des IPAM-Bereichs, dem das Subnetz angehört.
SubnetID	Die ID des Subnetzes.
VpcID	Die ID der VPC, der das Subnetz angehört.

Metriken zu öffentlichen IPv4-Pools

Der Name und die Beschreibung der Metriken zu öffentlichen IPv4-Pools sind nachfolgend aufgeführt.

Metrikname	Beschreibung
PublicIPv4PoolIPUsage	Die Anzahl der EIP-Adressen aus dem öffentlichen IPv4-Pool, dividiert durch die Gesamtzahl der IP-Adressen im Pool.

Die Dimensionen, mit deren Hilfe Sie Metriken zu öffentlichen IPv4-Pools filtern können, sind nachstehend aufgeführt.

Dimension	Beschreibung
OwnerID	Die ID des Eigentümers des öffentlichen IPv4-Pools.
PublicIPv4PoolID	Die ID des öffentlichen IPv4-Pools.
Region	Die AWS-Region, in der sich der öffentliche IPv4-Pool befindet.
ScopeID	Die ID des IPAM-Bereichs, dem der öffentliche IPv4-Pool angehört.

Metriken von Einblicke in öffentliche IPs

Die Metriknamen und -beschreibungen von Einblicke in öffentliche IPs sind unten aufgeführt.

Metrikname	Beschreibung
AmazonOwnedElasticIPs	Die Anzahl der Amazon-eigenen Elastic-IP-Adressen, die Sie für Ressourcen in Ihrem AWS-Konto bereitgestellt oder zugewiesen haben.
AssociatedAmazonOwnedElasticIPs	Die Anzahl der Amazon-eigenen Elastic-IP-Adressen, die Sie Ressourcen in Ihrem AWS-Konto zugewiesen haben.
AssociatedBringYourOwnIPs	Die Anzahl der öffentlichen IPv4-Adressen, die Sie mit Bring your own IP addresses (BYOIP) in AWS eingebunden und Ressourcen in Ihrem AWS-Konto zugewiesen haben.
BringYourOwnIPs	Die Anzahl der öffentlichen IPv4-Adressen, die Sie mit Bring your own IP addresses (BYOIP) in AWS eingebunden haben.
EC2PublicIPs	Die Anzahl der öffentlichen IPv4-Adressen, die EC2-Instances zugewiesen wurden, als die Instances in einem Standards ubnetz oder in einem Subnetz gestartet wurden, das zur automatischen Zuweisung einer öffentlichen IPv4-Adresse konfiguriert ist.
ServiceManagedBringYourOwnIPs	Die Anzahl der öffentlichen IPv4-Adressen, die Sie mit Bring your own IP addresses (BYOIP) in AWS eingebunden haben und die durch einen AWS-Service bereitgestellt und verwaltet werden.
ServiceManagedIPs	Die Anzahl der öffentlichen IPv4-Adressen, die von einem AWS-Service bereitgestellt und verwaltet werden.
UnassociatedAmazonOwnedElasticIPs	Die Anzahl der Amazon-eigenen Elastic-IP-Adressen, die Sie keinen Ressourcen in Ihrem AWS-Konto zugewiesen haben.
UnassociatedBringYourOwnIPs	Die Anzahl der öffentlichen IPv4-Adressen, die Sie mit Bring your own IP addresses (BYOIP) in AWS eingebunden und keine Ressourcen in Ihrem AWS-Konto zugewiesen haben.

Die Dimensionen, mit deren Hilfe Sie Metriken zu Pools von Einblicke in öffentliche IPs filtern können, sind nachstehend aufgeführt.

Dimension	Beschreibung
IpamId	Die ID des IPAMs, dem die IP-Adresse angehört.
Region	Die AWS-Region, in der sich die öffentliche IP-Adresse befindet.

Kurzer Tipp zum Erstellen von Alarmen

Um schnell einen Amazon-CloudWatch-Alarm für Ressourcen mit hoher IP-Adressauslastung zu erstellen, öffnen Sie die CloudWatch-Konsole und wählen Sie Metriken und dann Alle Metriken. Öffnen Sie anschließend die Registerkarte Abfrage und wählen Sie nacheinander den Namespace `AWS/IPAM > VPC IP Usage Metrics`, `AWS/IPAM > Subnet IP Usage Metrics` oder `AWS/IPAM > Public IPv4 Pool IP Usage Metrics`, den Metriknamen `MAX(VpcIPUsage)`, `MAX(SubnetIPUsage)` oder `MAX(PublicIPv4PoolIPUsage)` und Alarm erstellen. Weitere Informationen finden Sie unter Alarme für Metrics-Insights-Abfragen erstellen im Benutzerhandbuch zu Amazon CloudWatch.

Verlauf der IP-Adresse anzeigen

Führen Sie die Schritte in diesem Abschnitt aus, um den Verlauf einer IP-Adresse oder eines CIDR in einem IPAM-Bereich anzuzeigen. Sie können die Verlaufsdaten verwenden, um Ihre Netzwerksicherheits- und Routing-Richtlinien zu analysieren und zu überprüfen. IPAM speichert Daten zur Überwachung der IP-Adresse automatisch für bis zu drei Jahre.

Sie können die IP-Verlaufsdaten verwenden, um nach der Statusänderung von IP-Adressen oder CIDRs für die folgenden Arten von Ressourcen zu suchen:

- VPCs
- VPC-Subnetze
- Elastic-IP-Adressen
- EC2-Instances
- An Instances angefügte EC2-Netzwerkschnittstellen

Important

Obwohl IPAM keine Amazon-EC2-Instances oder an Instances angefügte EC2-Netzwerkschnittstellen überwacht, können Sie die Funktion Suche IP-Verläufe verwenden, um nach Verlaufsdaten zu EC2-Instance- und Netzwerkschnittstellen-CIDRs zu suchen.

Note

- Wenn Sie eine Ressource von einem IPAM-Bereich in einen anderen verschieben, endet der vorherige Verlaufsdatensatz und unter dem neuen Bereich wird ein neuer Verlaufsdatensatz erstellt. Weitere Informationen finden Sie unter Verschieben von VPC CIDRs zwischen Bereichen.
- Wenn Sie eine Ressource löschen oder auf ein AWS Konto übertragen, das nicht von Ihrem IPAM überwacht wird, ist jeder neue Verlauf im Zusammenhang mit der Ressource nicht sichtbar und Ihr IPAM überwacht die Ressource nicht. Die IP-Adresse der Ressource ist jedoch weiterhin durchsuchbar.
- Wenn Sie Integrieren von IPAM mit Konten außerhalb Ihrer Organisation, kann der IPAM-Besitzer den IP-Adressverlauf aller Ressourcen-CIDRs anzeigen, die diesen Konten gehören.

AWS Management Console

So zeigen Sie den Verlauf eines CIDR an

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Suche IP-Verlauf aus.
3. Geben Sie eine IPv4- oder IPv6-IP-Adresse oder CIDR ein. Dies muss ein bestimmtes CIDR für die Ressource sein.
4. Wählen Sie eine IPAM-Bereichs-ID aus.
5. Wählen Sie einen Datums-/Uhrzeitbereich.
6. Wenn Sie die Ergebnisse nach VPC filtern möchten, geben Sie eine VPC-ID ein. Verwenden Sie diese Option, wenn das CIDR in mehreren VPCs angezeigt wird.
7. Wählen Sie Search (Suchen) aus.

Command line

Die Befehle in diesem Abschnitt verweisen auf die AWS-CLI-Referenzdokumentation. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

- Zeigen Sie den Verlauf eines CIDR an: get-ipam-address-history

Beispiele für die Verwendung von AWS CLI zum Analysieren und Prüfen der IP-Adressnutzung finden Sie unter Tutorial: Anzeigen des IP-Adressverlaufs mithilfe von AWS CLI.

Die Ergebnisse der Suche sind in folgende Spalten unterteilt:

- Sampled end time (Stichproben-Endzeit): Stichproben-Endzeit der Ressource-zu-CIDR-Zuordnung innerhalb des IPAM-Bereichs. Änderungen werden in regelmäßigen Snapshots aufgenommen, sodass die Endzeit möglicherweise vor diesem bestimmten Zeitpunkt eingetreten ist.
- Sampled start time (Stichproben-Startzeit): Stichproben-Startzeit der Ressource-zu-CIDR-Zuordnung innerhalb des IPAM-Bereichs. Änderungen werden in regelmäßigen Snapshots aufgenommen, sodass die Startzeit möglicherweise vor diesem bestimmten Zeitpunkt eingetreten ist.

  Example

  Sehen wir uns einen Beispiel-Anwendungsfall an, um die Zeiten zu erläutern, die Sie unter Stichproben-Startzeit und Stichproben-Endzeit sehen:

  Um 14:00 Uhr wurde eine VPC mit CIDR 10.0.0.0/16 erstellt. Um 15:00 Uhr erstellen Sie ein IPAM und einen IPAM-Pool mit CIDR 10.0.0.0/8 und wählen die Option für den automatischen Import, damit IPAM alle CIDRs erkennen und importieren kann, die in den IP-Adressbereich von 10.0.0.0/8 liegen. Da IPAM Änderungen an CIDRs in regelmäßigen Snapshots aufnimmt, erkennt es das vorhandene VPC CIDR erst um 15:05 Uhr. Wenn Sie mit der Funktion Suche IP-Verlauf nach der ID dieser VPC suchen, ist die abgetastete Startzeit für Ihre VPC 15:05 Uhr, das ist der Zeitpunkt, an dem IPAM sie entdeckt hat, und nicht 14:00 Uhr, als Sie die VPC erstellt haben. Nehmen wir an, Sie entscheiden sich, die VPC um 17:00 Uhr zu löschen. Wenn die VPC gelöscht wird, wird das CIDR 10.0.0.0/16, das der VPC zugewiesen wurde, wieder in den IPAM-Pool recycelt. IPAM erstellt seinen periodischen Snapshot um 17:05 Uhr und nimmt die Änderung auf. Wenn Sie in IP-Verläufen nach der ID dieses VPCs suchen, ist 17:05 Uhr die Endzeit für die CIDR des VPCs, nicht 17:00 Uhr, da dies der Zeitpunkt ist, an dem der VPC gelöscht wurde.

- Resouce ID (Ressourcen-ID): Die ID, die generiert wurde, als die Ressource mit dem CIDR verknüpft wurde.
- Name: Der Name der Ressource (falls zutreffend).
- Compliance status (Compliance-Status): Der Compliance-Status des CIDR.
  - Compliant (Konform): Eine verwaltete Ressource entspricht den Zuordnungsregeln des IPAM-Pools.
  - Noncompliant (Nicht konform): Das Ressourcen-CIDR entspricht nicht einer oder mehreren der Zuweisungsregeln des IPAM-Pools.

    Example

    Wenn eine VPC über ein CIDR verfügt, das die Netzmaskenlängenparameter des IPAM-Pools nicht erfüllt, oder wenn sich die Ressource nicht in derselben AWS-Region befindet wie der IPAM-Pool wird er als nicht konform gekennzeichnet.
  - Unmanaged (Nicht verwaltet): Der Ressource ist kein CIDR aus einem IPAM-Pool zugewiesen und wird von IPAM nicht auf mögliche CIDR-Compliance der Pool-Zuweisungsregeln überwacht. Das CIDR wird auf Überlappungen überwacht.
  - Ignored (Ignoriert): Die verwaltete Ressource wurde ausgewählt, um von der Überwachung ausgenommen zu sein. Ignorierte Ressourcen werden nicht auf Überschneidungs- oder Zuweisungsregel-Compliance bewertet. Wenn eine Ressource ignoriert wird, wird der ihr zugewiesene Speicherplatz aus einem IPAM-Pool an den Pool zurückgegeben und die Ressource wird nicht erneut durch automatischen Import importiert (wenn die automatische Importzuordnungsregel für den Pool festgelegt ist).
  - -: Diese Ressource gehört nicht zu den Arten von Ressourcen, die IPAM überwachen oder verwalten kann.
- Overlap status (Überlappungsstatus): Der Überlappungsstatus vom CIDR.
  - Nonoverlapping (Nicht überlappend): Die Ressource CIDR überlappt sich nicht mit einem anderen CIDR im gleichen Bereich.
  - Overlapping (Überlappend): Das Ressourcen-CIDR überlappt sich mit einem anderen CIDR im gleichen Bereich. Beachten Sie, dass wenn sich ein Ressourcen-CIDR überlappt, es möglicherweise mit einer manuellen Zuordnung überlappen kann.
  - Ignored (Ignoriert): Die verwaltete Ressource wurde ausgewählt, um von der Überwachung ausgenommen zu sein. IPAM wertet ignorierte Ressourcen nicht auf Überschneidungen oder die Compliance von Zuweisungsregeln aus. Wenn eine Ressource ignoriert wird, wird der ihr zugewiesene Speicherplatz aus einem IPAM-Pool an den Pool zurückgegeben und die

Ressource wird nicht erneut durch automatischen Import importiert (wenn die automatische Importzuordnungsregel für den Pool festgelegt ist).

  - -: Diese Ressource gehört nicht zu den Arten von Ressourcen, die IPAM überwachen oder verwalten kann.
- Ressourcentyp
  - vpc: Das CIDR ist mit einer VPC verbunden.
  - subnet (Subnetz): Das CIDR ist einem VPC-Subnetz zugeordnet.
  - eip: Das CIDR ist einer elastischen IP-Adresse zugeordnet.
  - instance (Instance): Das CIDR ist einer EC2-Instance zugeordnet.
  - network-interface: Das CIDR ist einer Netzwerkschnittstelle zugeordnet.
- VPC-ID: Die ID der VPC, zu der diese Ressource gehört (falls zutreffend).
- Region: Die AWS-Region dieser Ressource.
- Owner ID (Besitzer-ID): Die AWS-Konto-ID des Benutzers, der diese Ressource erstellt hat (falls zutreffend).

Anzeigen von Einblicken in öffentliche IP-Adressen

Bei einer öffentlichen IPv4-Adresse handelt es sich um eine IPv4-Adresse, die über das Internet erreichbar ist. Eine öffentliche IPv4-Adresse ist erforderlich, damit eine Ressource im Internet direkt über IPv4 erreichbar ist.

> **Note**
>
> AWS Gebühren für alle öffentlichen IPv4-Adressen, einschließlich öffentlicher IPv4-Adressen, die mit laufenden Instances verknüpft sind, und Elastic IP-Adressen. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.

Sie können Einblicke in die folgenden öffentlichen IPv4-Adresstypen anzeigen:

- Elastische IP-Adressen (EIPs): Von Amazon bereitgestellte statische, öffentliche IPv4-Adressen, die Sie einer EC2-Instance, einer elastic network interface oder einer Ressource zuordnen können. AWS

- Öffentliche EC2-IPv4-Adressen: Öffentliche IPv4-Adressen, die von Amazon einer EC2-Instance zugewiesen werden (wenn die EC2-Instance in einem Standardsubnetz oder in einem Subnetz gestartet wird, das zur automatischen Zuweisung einer öffentlichen IPv4-Adresse konfiguriert ist).
- BYOIPv4-Adressen: Öffentliche IPv4-Adressen im IPv4-Adressbereich, zu denen Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) gewechselt haben.
- Vom Dienst verwaltete IPv4-Adressen: Öffentliche IPv4-Adressen, die automatisch auf Ressourcen bereitgestellt und von einem Dienst verwaltet werden. AWS AWS Zum Beispiel öffentliche IPv4-Adressen auf Amazon ECS, Amazon RDS oder Amazon WorkSpaces.

Sie können Einblicke in öffentliche IPs verwenden, um Folgendes zu sehen:

- Wenn Ihr IPAM in Konten in einer AWS Organisation integriert ist, können Sie alle öffentlichen IPv4-Adressen anzeigen, die von Diensten in allen AWS Regionen für Ihr gesamtes Unternehmen verwendet werden. AWS
- Wenn Ihr IPAM in ein einzelnes Konto integriert ist, können Sie alle öffentlichen IPv4-Adressen, die von Diensten in allen AWS Regionen verwendet werden, in Ihrem Konto einsehen.

Einblicke in öffentliche IPs zeigen alle öffentlichen IPv4-Adressen, die von Services in diesen Regionen verwendet werden. Anhand dieser Einblicke können Sie die Nutzung öffentlicher IPv4-Adressen ermitteln und Empfehlungen zur Freigabe ungenutzter Elastic-IP-Adressen anzeigen.

- Öffentliche IP-Typen: Die Anzahl der öffentlichen IPv4-Adressen, geordnet nach Typ.
  - EIPs im Besitz von Amazon: Elastische IP-Adressen, die Sie bereitgestellt oder Ressourcen in Ihrem Konto zugewiesen haben. AWS
  - Öffentliche EC2-IPs: Öffentliche IPv4-Adressen, die EC2-Instances zugewiesen werden, wenn die Instances in einem Standardsubnetz oder in einem Subnetz gestartet wurden, das zur automatischen Zuweisung einer öffentlichen IPv4-Adresse konfiguriert ist.
  - BYOIP: Öffentliche IPv4-Adressen, auf die Sie AWS mithilfe von Bring Your Own IP-Adressen (BYOIP) zugegriffen haben.
  - Vom Dienst verwaltete IPs: Öffentliche IPv4-Adressen, die von einem Dienst bereitgestellt und verwaltet werden. AWS
- EIP-Nutzung: Die Anzahl der Elastic-IP-Adressen, geordnet nach ihrer Nutzungsweise.
  - Zugeordnete EIPs im Besitz von Amazon: Elastic IP-Adressen, die Sie in Ihrem AWS Konto bereitgestellt und die Sie einer EC2-Instance, Netzwerkschnittstelle oder Ressource zugeordnet haben. AWS

  - Zugeordnete BYOIP: Öffentliche IPv4-Adressen, die Sie AWS mithilfe von BYOIP verwendet haben und die Sie mit einer Netzwerkschnittstelle verknüpft haben.
  - Nicht verknüpfte EIPs im Besitz von Amazon: Elastic IP-Adressen, die Sie in Ihrem AWS Konto bereitgestellt, aber keiner Netzwerkschnittstelle zugeordnet haben.
  - Nicht zugeordnete BYOIP: Öffentliche IPv4-Adressen, die Sie AWS mithilfe von BYOIP verwendet haben, aber keiner Netzwerkschnittstelle zugeordnet haben.
- Öffentliche IP-Adressen: Eine Tabelle mit öffentlichen IPv4-Adressen und ihren Attributen.
  - IP-Adresse: Die öffentliche IPv4-Adresse.
  - Zugeordnet: Gibt an, ob die Adresse einer EC2-Instance, Netzwerkschnittstelle oder Ressource zugeordnet ist oder nicht. AWS
    - Zugeordnet: Die öffentliche IPv4-Adresse ist einer EC2-Instance, Netzwerkschnittstelle oder Ressource zugeordnet. AWS
    - Nicht verknüpft: Die öffentliche IPv4-Adresse ist keiner Ressource zugeordnet und befindet sich in Ihrem Konto im Leerlauf. AWS
  - Adresstyp: Der Typ der IP-Adresse.
    - Amazon-eigene EIP: Die öffentliche IPv4-Adresse ist eine Elastic-IP-Adresse.
    - BYOIP: Die öffentliche IPv4-Adresse wurde mithilfe von BYOIP eingerichtet. AWS
    - Öffentliche EC2-IP: Die öffentliche IPv4-Adresse wurde einer EC2-Instance automatisch zugewiesen.
    - Von IP verwalteter Dienst: Die öffentliche IPv4-Adresse wurde AWS mithilfe von Bring Your Own IP (BYOIP) eingerichtet.
    - Vom Dienst verwaltete IP: Die öffentliche IPv4-Adresse wurde bereitgestellt und wird von einem Dienst verwaltet. AWS
  - Service: Der Service, dem die IP-Adresse zugeordnet ist.
    - AGA: Ein. AWS Global Accelerator Wenn ein benutzerdefinierter Routing-Beschleuniger verwendet wird, werden seine öffentlichen IPs nicht aufgeführt. Informationen zum Anzeigen dieser öffentlichen IPs finden Sie unter Ihre benutzerdefinierten Routing-Beschleuniger anzeigen.
    - Database Migration Service: Eine AWS Database Migration Service (DMS-) Replikationsinstanz.
    - Redshift: Ein Amazon-Redshift-Cluster.
    - RDS: Eine Amazon-RDS-Instance (Relational Database Service).

  - Load Balancer (EC2): Ein Application Load Balancer oder ein Network Load Balancer.
  - NAT-Gateway (VPC): Ein öffentliches NAT-Gateway der Amazon VPC.
  - Site-to-Site VPN: Ein AWS Site-to-Site VPN virtuelles privates Gateway.
  - Sonstiges: Anderer, derzeit nicht identifizierbarer Service.
- Name (EIP-ID): Wenn diese öffentliche IPv4-Adresse eine Elastic-IP-Adresszuweisung ist, handelt es sich hierbei um den Namen und die ID der EIP-Zuweisung.
- Netzwerkschnittstellen-ID: Wenn diese öffentliche IPv4-Adresse einer Netzwerkschnittstelle zugeordnet ist, handelt es sich hierbei um die ID der Netzwerkschnittstelle.
- Instance-ID: Wenn diese öffentliche IPv4-Adresse einer EC2-Instance zugeordnet ist, handelt es sich hierbei um die Instance-ID.
- Sicherheitsgruppen: Wenn diese öffentliche IPv4-Adresse einer EC2-Instance zugeordnet ist, handelt es sich hierbei um den Namen und die ID der Sicherheitsgruppe, die der Instance zugewiesen ist.
- Pool öffentlicher IPv4-Adressen: Wenn es sich um eine Elastic-IP-Adresse aus einem IP-Adresspool handelt, der Amazon gehört und von Amazon verwaltet wird, lautet der Wert „-“. Handelt es sich um eine Elastic-IP-Adresse aus einem IP-Adressbereich, der Ihnen gehört und den Sie (über BYOIP) zu Amazon mitgebracht haben, ist der Wert die ID des öffentlichen IPv4-Pools.
- Netzwerkgrenzgruppe: Wenn die IP-Adresse bekannt gegeben wird, ist dies die AWS Region, aus der die IP-Adresse bekannt gegeben wird.
- Besitzer-ID: Die AWS Kontonummer des Ressourcenbesitzers.
- Samplezeit: Der Zeitpunkt der letzten erfolgreichen Ressourcenerkennung.
- Ressourcenerkennungs-ID: Die ID der Ressourcenerkennung, die diese öffentliche IPv4-Adresse erkannt hat.
- Service-Ressource: Ressourcen-ARN oder -ID.

Wenn Ihrem Konto eine Elastic-IP-Adresse zugewiesen ist, die aber keiner Netzwerkschnittstelle zugeordnet ist, wird ein Banner angezeigt, wonach Ihr Konto nicht zugeordnet EIPs enthält, die Sie freigeben müssen.

> **Important**
>
> Einblicke in öffentliche IPs wurde kürzlich aktualisiert. Wenn Sie aufgrund fehlender Anrufberechtigungen eine Fehlermeldung erhalten GetIpamDiscoveredPublicAddresses,

muss die verwaltete Berechtigung aktualisiert werden, die mit einer Ressourcenerkennung verknüpft ist, die mit Ihnen geteilt wurde. Wenden Sie sich an die Person, die die Ressourcenerkennung erstellt hat, und bitten Sie sie, die verwaltete Berechtigung `AWSRAMPermissionIpamResourceDiscovery` auf die Standardversion zu aktualisieren. Weitere Informationen finden Sie unter Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

AWS Management Console

So zeigen Sie Einblicke in öffentliche IP-Adressen an

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich die Option Öffentliche IP-Einblicke.
3. Um Details zu einer öffentlichen IP-Adresse anzuzeigen, wählen Sie eine IP-Adresse aus, indem Sie darauf klicken.
4. Sehen Sie sich die folgenden Informationen zur IP-Adresse an:

   - Details: Dieselben Informationen, die in den Spalten des Hauptfensters „Öffentliche IP-Einblicke“ sichtbar sind, z. B. Adresstyp und Service.
   - Regeln für Sicherheitsgruppen für eingehenden Datenverkehr: Wenn diese IP-Adresse einer EC2-Instance zugeordnet ist, handelt es sich hierbei um die Sicherheitsgruppenregeln, die den eingehenden Datenverkehr zur Instance steuern.
   - Regeln für Sicherheitsgruppen für ausgehenden Datenverkehr: Wenn diese IP-Adresse einer EC2-Instance zugeordnet ist, handelt es sich hierbei um die Sicherheitsgruppenregeln, die den ausgehenden Datenverkehr zur Instance steuern.
   - Tags: Schlüssel- und Wertepaare, die als Metadaten für die Organisation Ihrer AWS Ressourcen dienen.

Command line

Verwenden Sie den folgenden Befehl, um die öffentlichen IP-Adressen abzurufen, die von IPAM erkannt wurden: get-ipam-discovered-public -addresses

Tutorials für Amazon VPC IP Address Manager

Die folgenden Tutorials zeigen, wie Sie mit der AWS-CLI gängige IPAM-Aufgaben durchführen. Informationen zum Aufrufen der AWS CLI finden Sie unter Zugriff auf IPAM. Weitere Informationen zu den IPAM-Konzepten, die in diesen Tutorials erwähnt werden, finden Sie unter Funktionsweise von IPAM.

Inhalt

Tutorial: Erstellen eines IPAM und von Pools über die Konsole

In diesem Tutorial erstellen Sie einen IPAM und führen eine Integration in AWS Organizations durch. Außerdem erstellen Sie IP-Adresspools sowie eine VPC mit einem CIDR aus einem IPAM-Pool.

Das Tutorial zeigt Ihnen, wie Sie mit IPAM den IP-Adressraum entsprechend verschiedener Entwicklungsanforderungen organisieren können. Sobald Sie das Tutorial abgeschlossen haben, verfügen Sie über einen IP-Adresspool für Vorproduktionsressourcen. Anschließend können Sie je nach eigenen Routing- und Sicherheitsanforderungen weitere Pools erstellen, z. B. einen Pool für Produktionsressourcen.

Zwar lässt sich IPAM als Einzelbenutzer verwenden, doch durch die Integration in AWS Organizations können Sie IP-Adressen kontenübergreifend in Ihrer Organisation verwalten. In diesem Tutorial geht es um die Integration von IPAM in Konten einer Organisation. Das Thema Integrieren von IPAM mit Konten außerhalb Ihrer Organisation wird darin nicht behandelt.

> **Note**
>
> Im Rahmen des Tutorials werden Sie angewiesen, IPAM-Ressourcen auf eine bestimmte Weise zu benennen, IPAM-Ressourcen in bestimmten Regionen zu erstellen und bestimmte

CIDR-Bereiche von IP-Adressen für Pools zu verwenden. Dies soll die in IPAM verfügbaren Optionen optimieren und Ihnen einen schnellen Einstieg in IPAM ermöglichen. Nachdem Sie das Tutorial abgeschlossen haben, können Sie wahlweise einen neuen IPAM erstellen und ihn anders konfigurieren.

Inhalt

Voraussetzungen

Bevor Sie beginnen, müssen Sie ein AWS Organizations-Konto mit mindestens einem Mitgliedskonto eingerichtet haben. Entsprechende Anweisungen finden Sie unter Erstellen und Konfigurieren einer Organisation im Benutzerhandbuch von AWS Organizations.

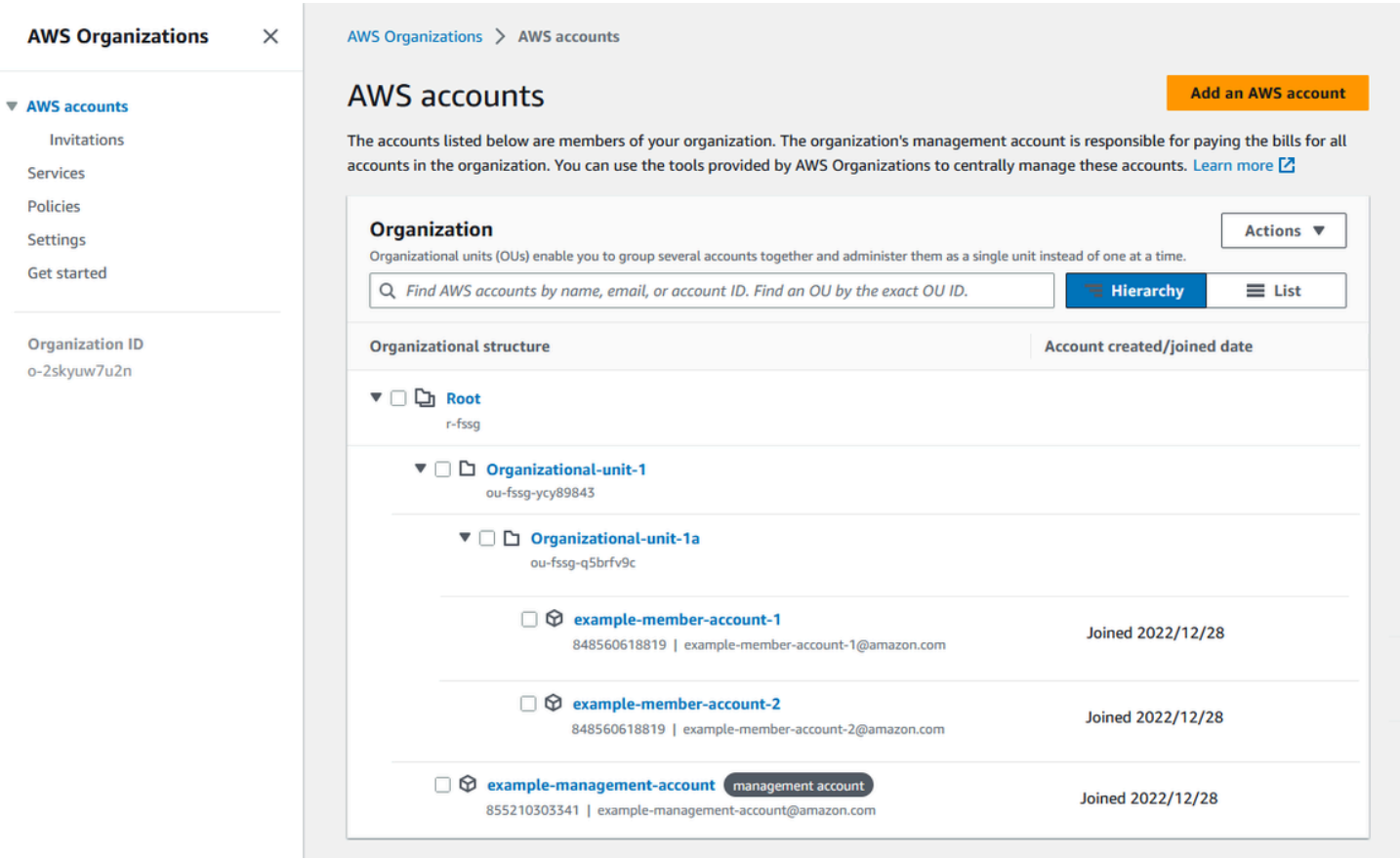
So lässt sich AWS Organizations in IPAM integrieren

Dieser Abschnitt enthält ein Beispiel für die AWS Organizations-Konten, die Sie in diesem Tutorial verwenden. In Ihrer Organisation gibt es drei Konten, die Sie im Tutorial bei der Integration in IPAM nutzen:

- Das Verwaltungskonto (in der folgenden Abbildung example-management-account genannt), um sich bei der IPAM-Konsole anzumelden und einen IPAM-Administrator zu delegieren. Das Verwaltungskonto der Organisation kann nicht als IPAM-Administrator verwendet werden.
- Ein Mitgliedskonto (in der folgenden Abbildung example-member-account-1 genannt) als IPAM-Administratorkonto. Das IPAM-Administratorkonto ist dafür zuständig, einen IPAM zu erstellen und

damit die Nutzung der IP-Adressen zu verwalten und zu überwachen. Jedes Mitgliedskonto in Ihrer Organisation kann als IPAM-Administrator delegiert werden.

- Ein Mitgliedskonto (in der Abbildung example-member-account-2 genannt) als Entwicklerkonto. Dieses Konto erstellt eine VPC mit einem CIDR, das aus einem IPAM-Pool zugewiesen wird.



Neben den Konten benötigen Sie die ID der Organisationseinheit (ou-fssg-q5brfv9c in der vorherigen Abbildung), die das Mitgliedskonto enthält, das Sie als Entwicklerkonto verwenden. Diese ID benötigen Sie, damit Sie bei der Freigabe des IPAM-Pools in einem späteren Schritt den Pool für diese Organisationseinheit freigeben können.

> **Note**
>
> Weitere Informationen zu Kontotypen von AWS Organizations wie etwa Verwaltungs- und Mitgliedskonten finden Sie unter Terminologie und Konzepte von AWS Organizations.

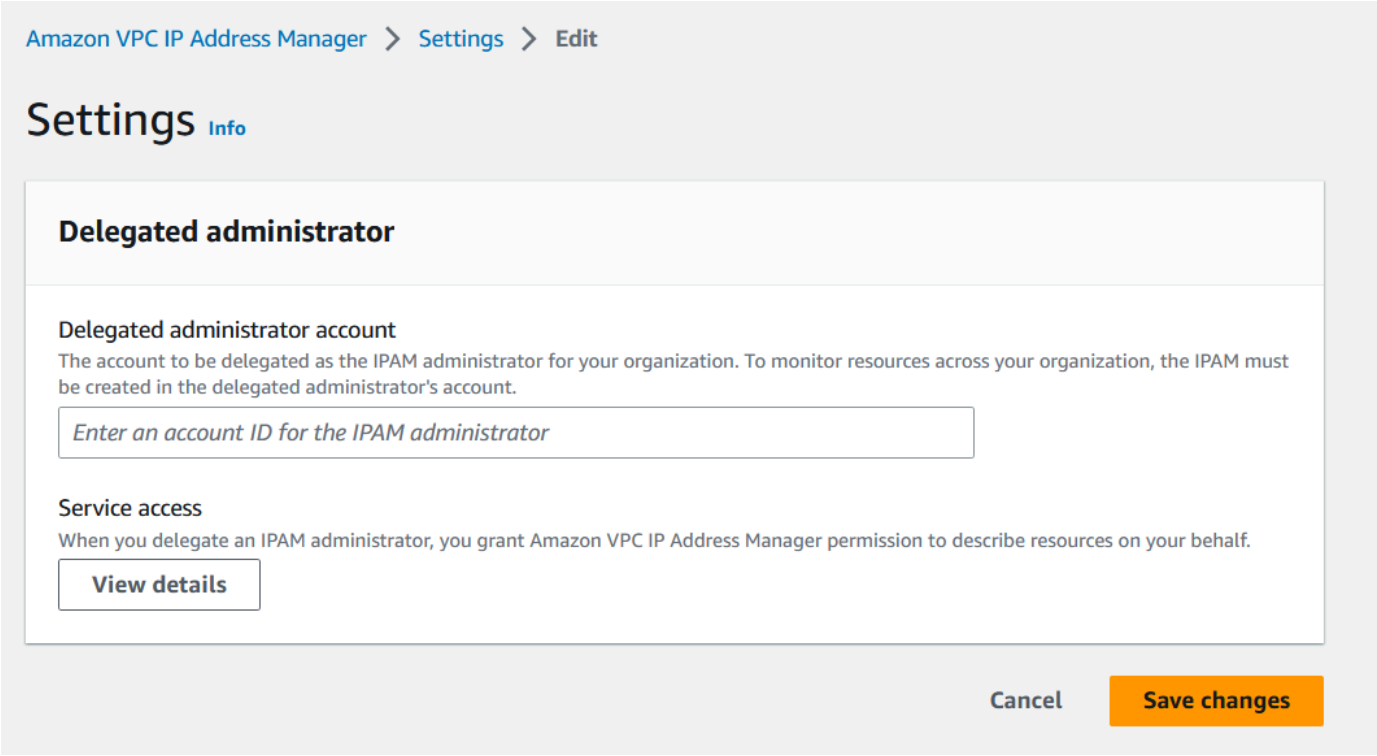
Schritt 1: Delegieren eines IPAM-Administrators

In diesem Schritt delegieren Sie ein Mitgliedskonto von AWS Organizations als IPAM-Administrator. Wenn Sie einen IPAM-Administrator delegieren, wird in jedem der Mitgliedskonten von AWS Organizations automatisch eine serviceverknüpfte Rolle erstellt. IPAM überwacht die Nutzung der IP-Adresse in diesen Konten durch Übernahme der serviceverknüpften Rolle in jedem Mitgliedskonto. Anschließend kann der Manager die Ressourcen und ihre CIDRs unabhängig von ihrer Organisationseinheit ermitteln.

Diesen Schritt können Sie nur durchführen, wenn Sie über die erforderlichen Berechtigungen für AWS Identity and Access Management (IAM) verfügen. Weitere Informationen finden Sie unter Integrieren von IPAM mit Konten in einer - AWS Organisation.

So delegieren Sie ein IPAM-Administratorkonto

1. Melden Sie sich mit dem Verwaltungskonto von AWS Organizations an und öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie in der AWS-Managementkonsole die AWS-Region, in der Sie mit IPAM arbeiten möchten.
3. Klicken Sie im Navigationsbereich auf Organization settings (Organisationseinstellungen).
4. Wählen Sie Delegate (Delegieren). Die Option Delegieren ist nur verfügbar, wenn Sie sich mit dem Verwaltungskonto von AWS Organizations bei der Konsole angemeldet haben.
5. Geben Sie die AWS-Konto-ID für ein Mitgliedskonto der Organisation ein. Der IPAM-Administrator muss ein Mitgliedskonto von AWS Organizations sein, nicht das Verwaltungskonto.



6. Wählen Sie Save Changes. Das Feld Delegierter Administrator wird mit Informationen zum Mitgliedskonto gefüllt.

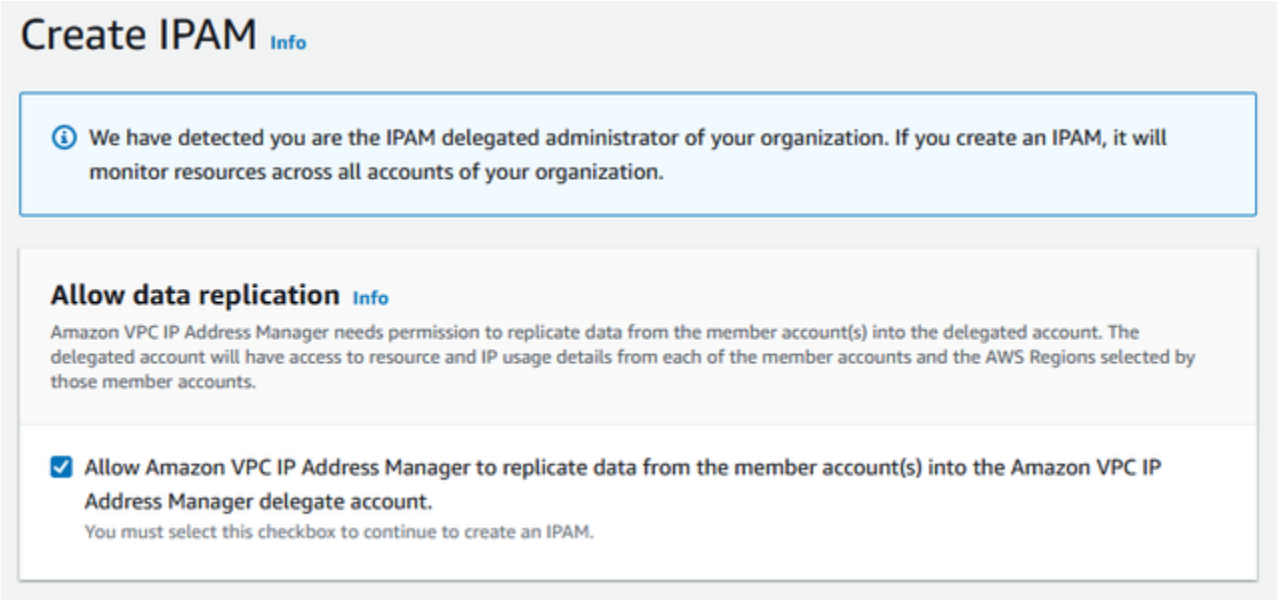
Schritt 2: Erstellen eines IPAMs

In diesem Schritt erstellen Sie einen IPAM. Wenn Sie einen IPAM erstellen, werden automatisch zwei Bereiche für den IPAM erstellt: der privaten Bereich, der für den gesamten privaten Adressraum vorgesehen ist, und der öffentliche Bereich für den gesamten öffentlichen Adressraum. Die Bereiche sind zusammen mit Pools und Allokationen Schlüsselkomponenten Ihres IPAM. Weitere Informationen finden Sie unter Funktionsweise von IPAM.

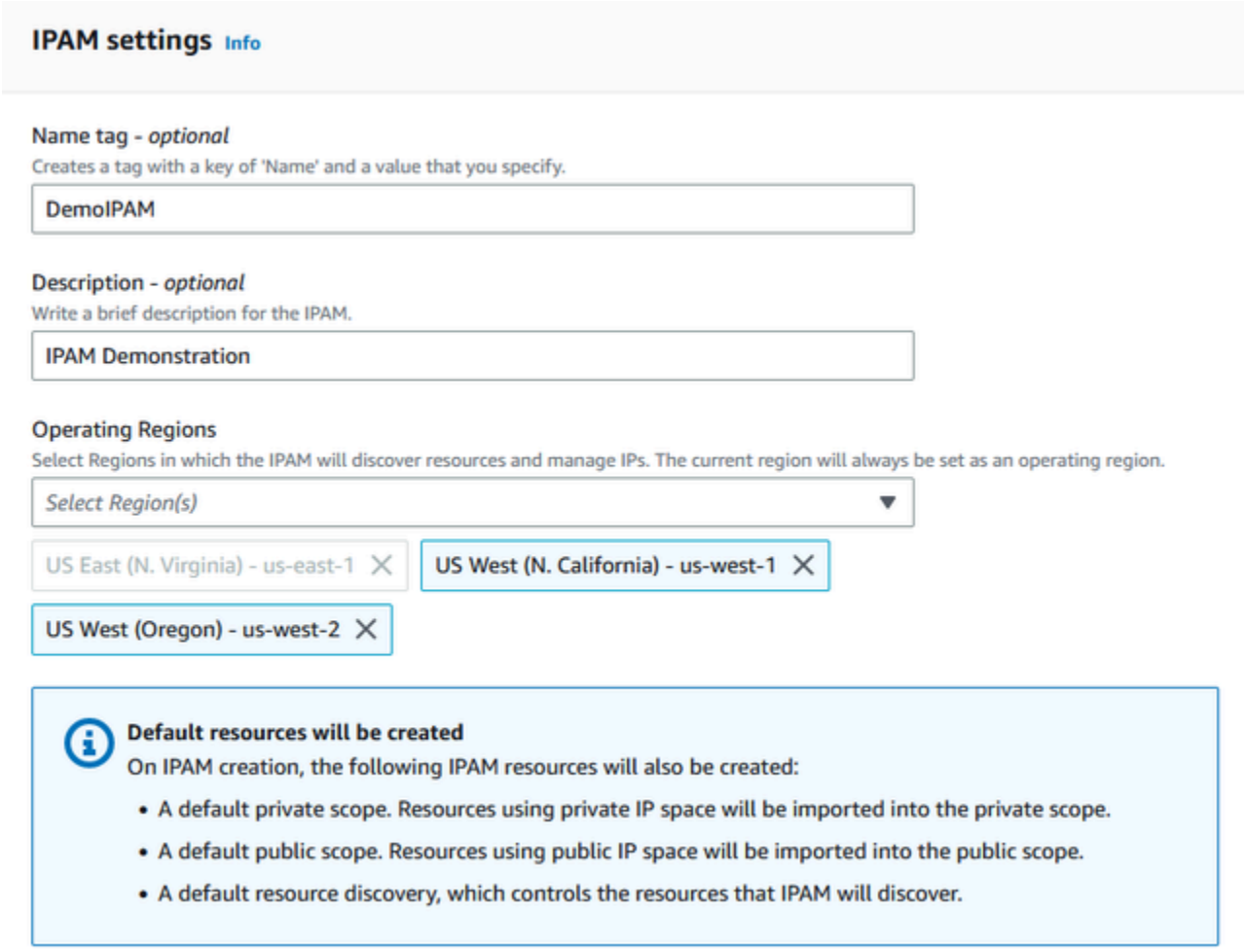
Erstellen eines IPAM

1. Öffnen Sie unter https://console.aws.amazon.com/ipam/ die IPAM-Konsole mithilfe des Mitgliedskontos von AWS Organizations, das im vorherigen Schritt als IPAM-Administrator delegiert wurde.
2. Wählen Sie in der AWS-Managementkonsole die AWS-Region, in der Sie das IPAM erstellen möchten. Erstellen Sie den IPAM in Ihrer Hauptbetriebsregion.
3. Wählen Sie auf der Service-Website Create IPAM (Eine IPAM erstellen).

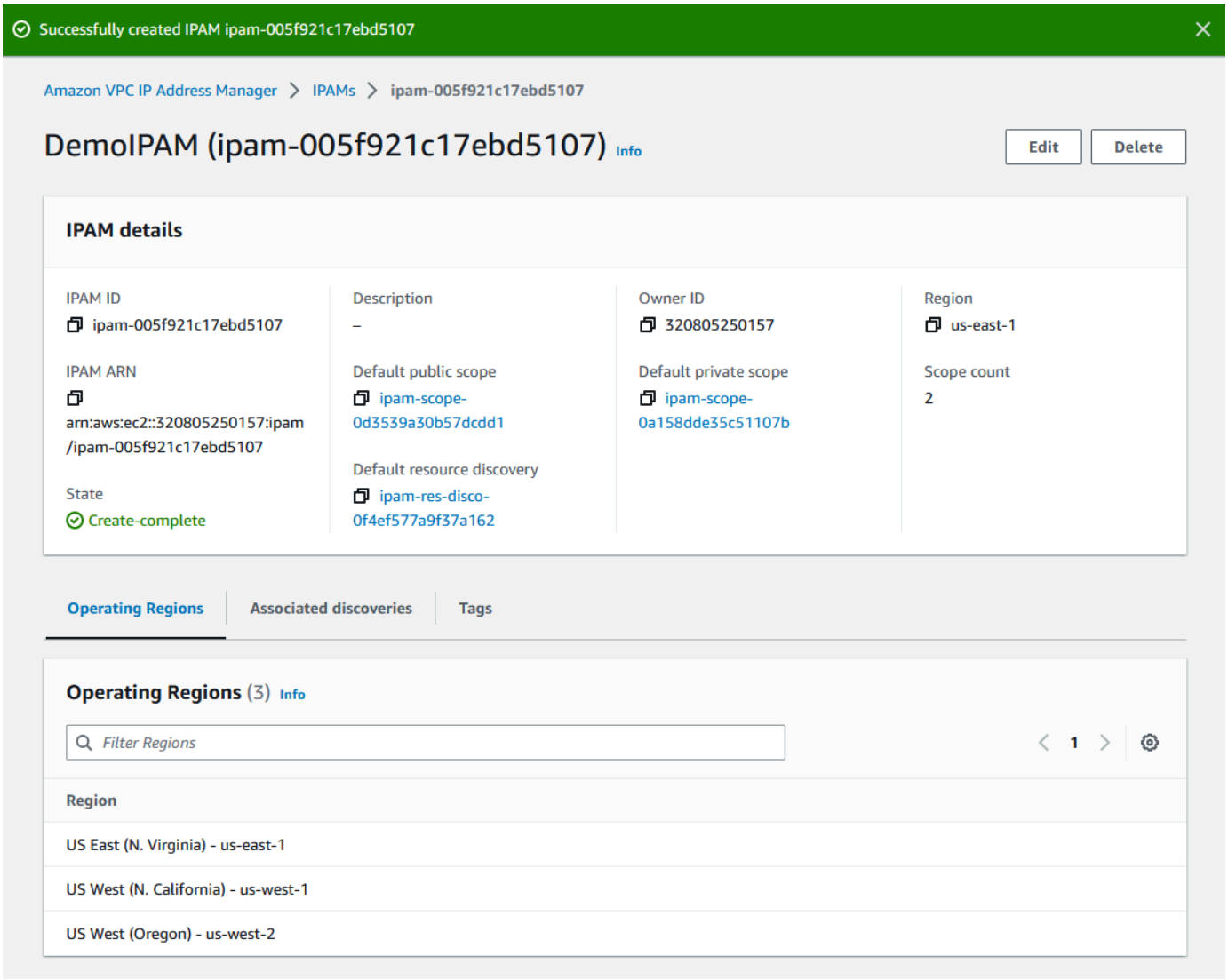
4. Wählen Sie Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Replizieren von VPC aus Quellkonten in das Replizieren von Daten aus Quellkonten in das IPAM-Delegate-Konto erlauben) aus. Wenn Sie diese Option nicht wählen, können Sie kein IPAM erstellen.



5. Wählen Sie unter Betriebsregionen die AWS-Regionen aus, in denen dieser IPAM Ressourcen verwalten und ermitteln kann. Die AWS-Region, in der Sie den IPAM erstellen, wird automatisch als eine der Betriebsregionen ausgewählt. In diesem Tutorial ist die Heimatregion des IPAM us-east-1. Daher wählen wir us-west-1 und us-west-2 als zusätzliche Betriebsregionen. Wenn Sie eine Betriebsregion vergessen, können Sie die IPAM-Einstellungen später bearbeiten und Regionen hinzufügen oder entfernen.



6. Wählen Sie Create IPAM (IPAM erstellen) aus.



Schritt 3: Erstellen Sie einen IPAM-Pool der obersten Ebene

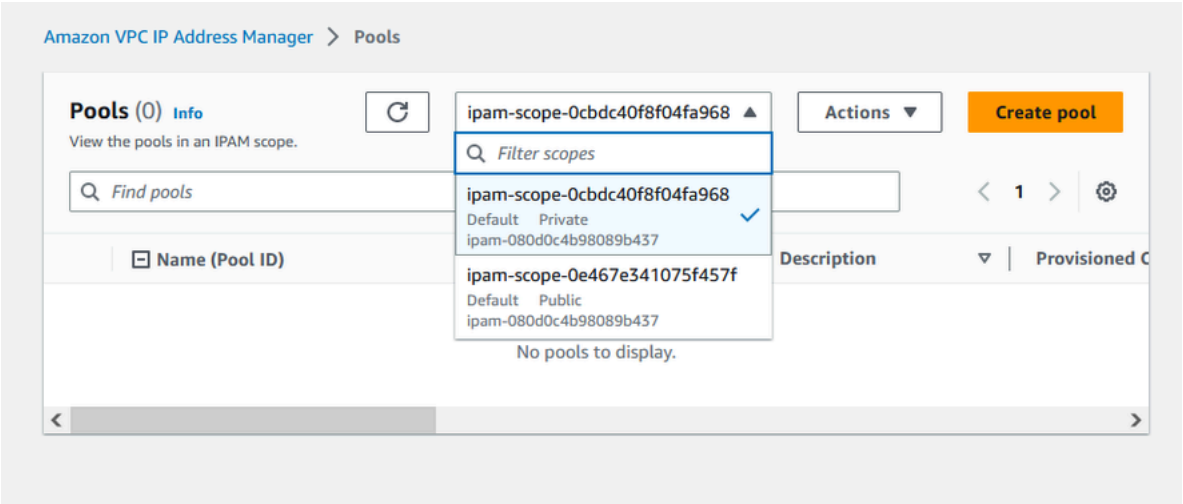
In diesem Tutorial erstellen Sie eine Poolhierarchie, wobei Sie mit dem IPAM-Pool der obersten Ebene beginnen. In den nachfolgenden Schritten erstellen Sie zwei regionale Pools und einen Entwicklungspool für die Vorproduktion in einem der regionalen Pools.

Weitere Informationen zu Poolhierarchien, die Sie mit IPAM erstellen können, finden Sie unter Beispiel für IPAM-Poolpläne.

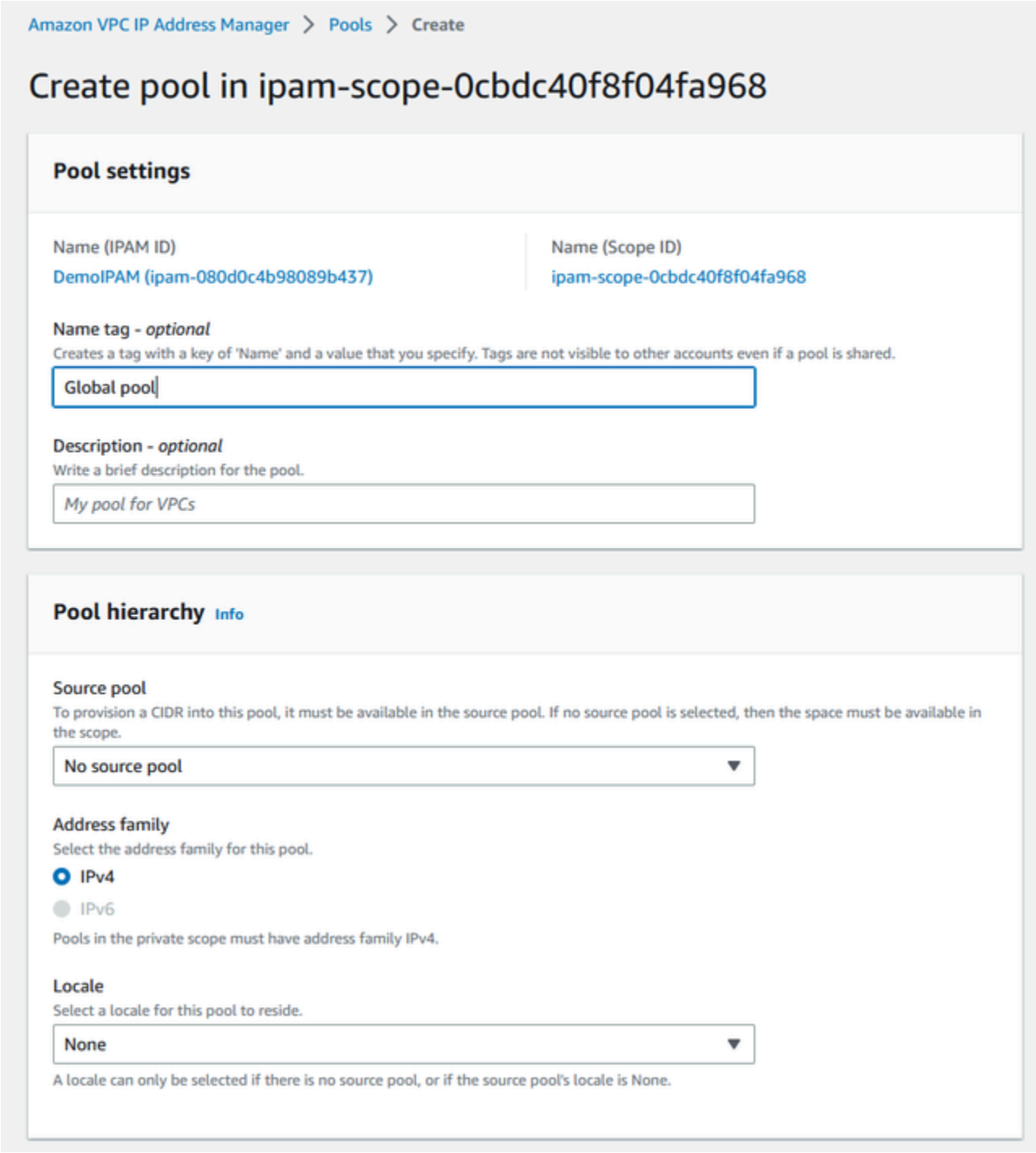
So erstellen Sie einen Pool der obersten Ebene

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.

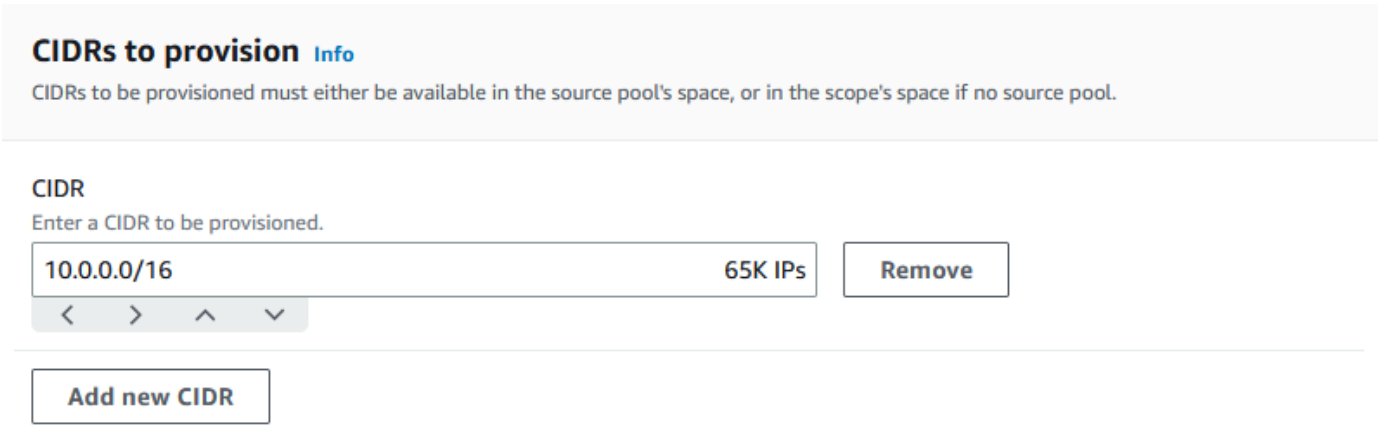
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich aus.



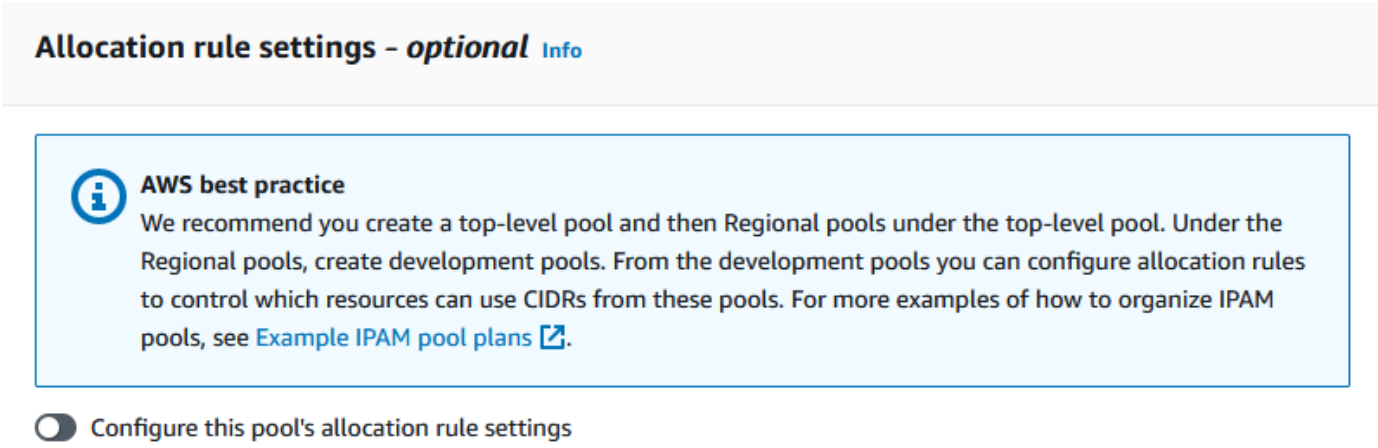
4. Wählen Sie Pool erstellen.
5. Lassen Sie unter IPAM-Bereich den privaten Bereich ausgewählt.
6. (Optional) Fügen Sie ein Namens-Tag und eine Beschreibung für den Pool hinzu, z. B. „Globaler Pool“.
7. Wählen Sie unter Quelle die Option IPAM-Bereich aus. Da es sich hierbei um den Pool der obersten Ebene handelt, verfügt er über keinen Quellpool.
8. Wählen Sie unter Adressfamilie IPv4 aus.
9. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
10. Wählen Sie für das Locale (Gebietsschema) None (Keine) aus. Gebietsschemata sind die AWS-Regionen, in denen dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Das Gebietsschema legen Sie für die regionalen Pools fest, die Sie im nächsten Abschnitt dieses Tutorials erstellen.



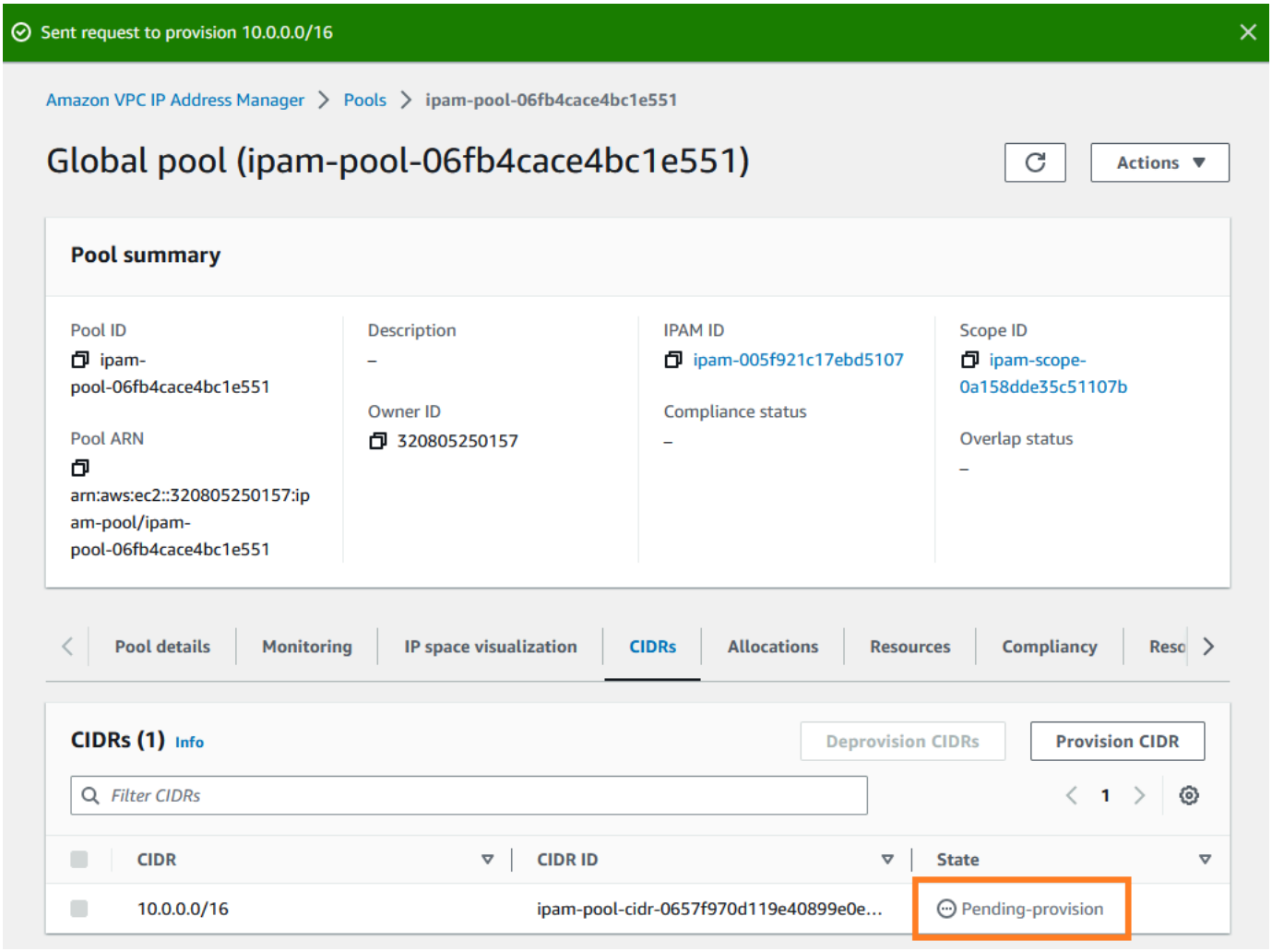
11. Wählen Sie ein CIDR aus, das für den Pool bereitgestellt werden soll. In diesem Beispiel stellen wir 10.0.0.0/16 bereit.



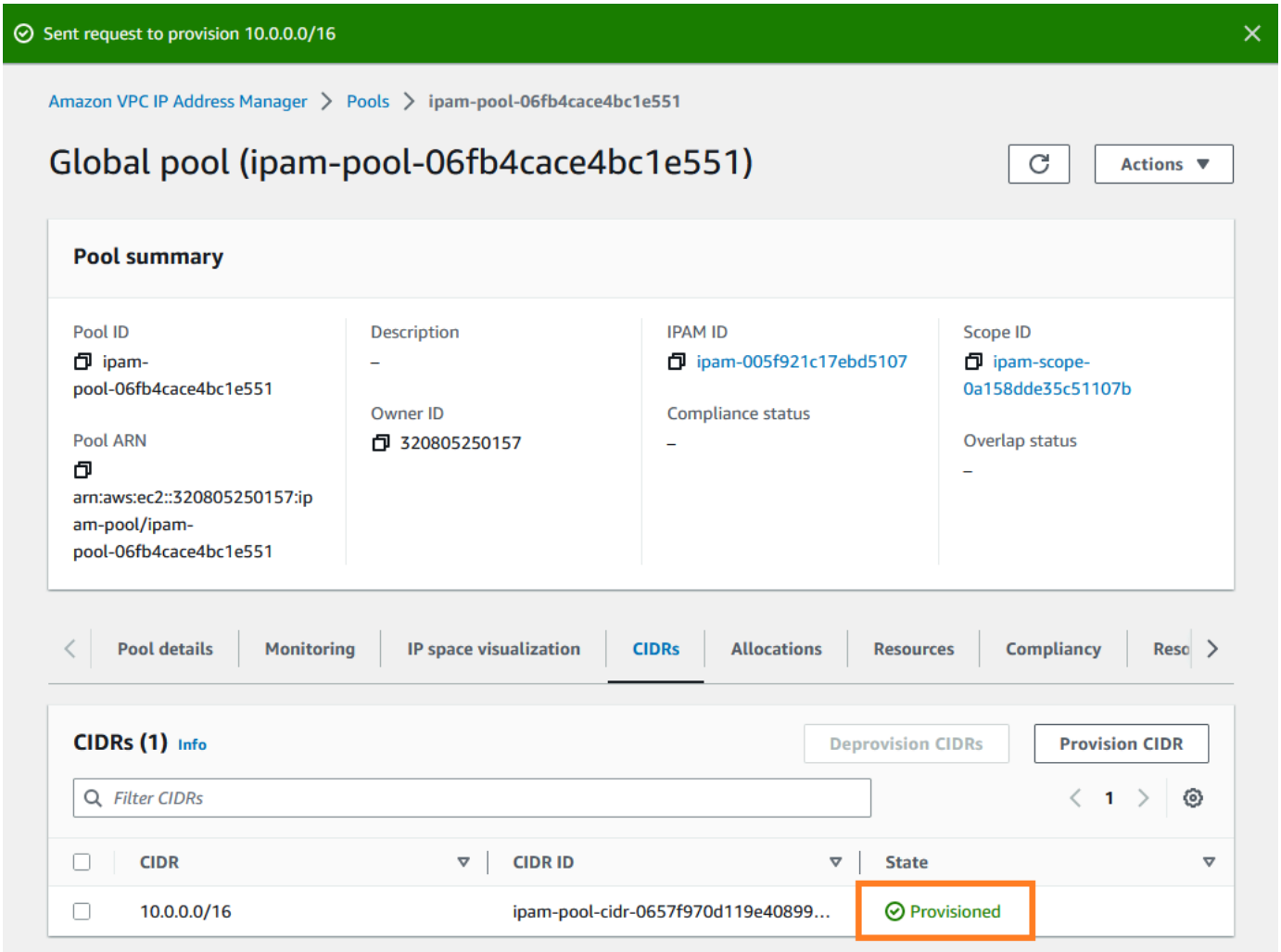
12. Lassen Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren deaktiviert. Hierbei handelt es sich um den Pool der obersten Ebene. Sie weisen keine CIDRs direkt aus diesem Pool den VPCs zu. Stattdessen weisen Sie sie aus einem Unterpool zu, den Sie anhand dieses Pools erstellen.



13. Wählen Sie Pool erstellen. Der Pool wird erstellt und das CIDR befindet sich im Status Ausstehende Bereitstellung:



14. Warten Sie, bis der Status Bereitgestellt lautet, bevor Sie mit dem nächsten Schritt fortfahren.



Nachdem Sie den Pool der obersten Ebene erstellt haben, erstellen Sie regionale Pools in us-west-1 und us-west-2.

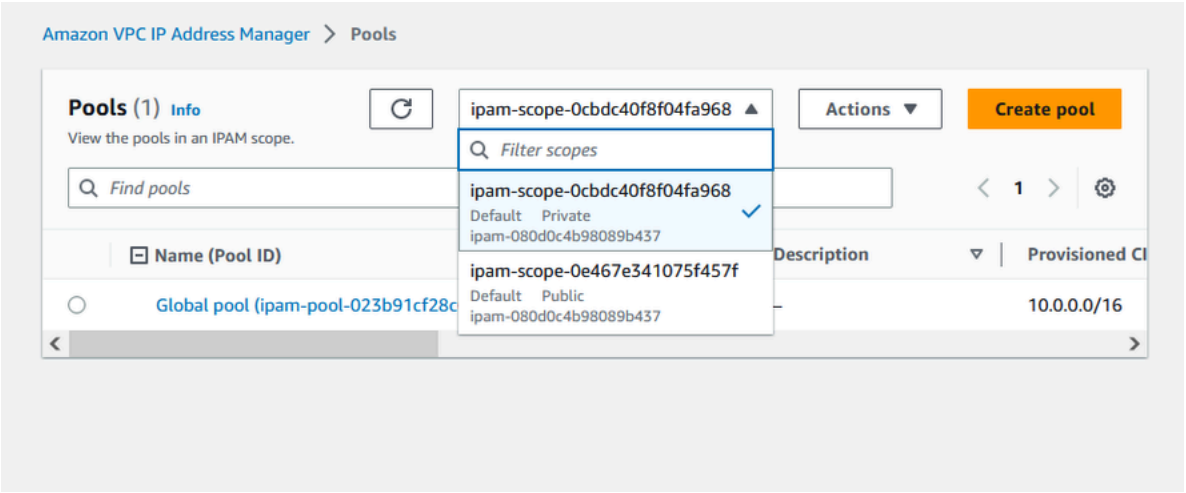
Schritt 4: Erstellen regionaler IPAM-Pools

Dieser Abschnitt veranschaulicht, wie Sie die IP-Adressen mithilfe von zwei regionalen Pools organisieren. In diesem Tutorial folgen wir einem der beispielhaften IPAM-Poolpläne und erstellen zwei regionale Pools, mit deren Hilfe Mitgliedskonten in Ihrer Organisation CIDRs den VPCs zueisen können.

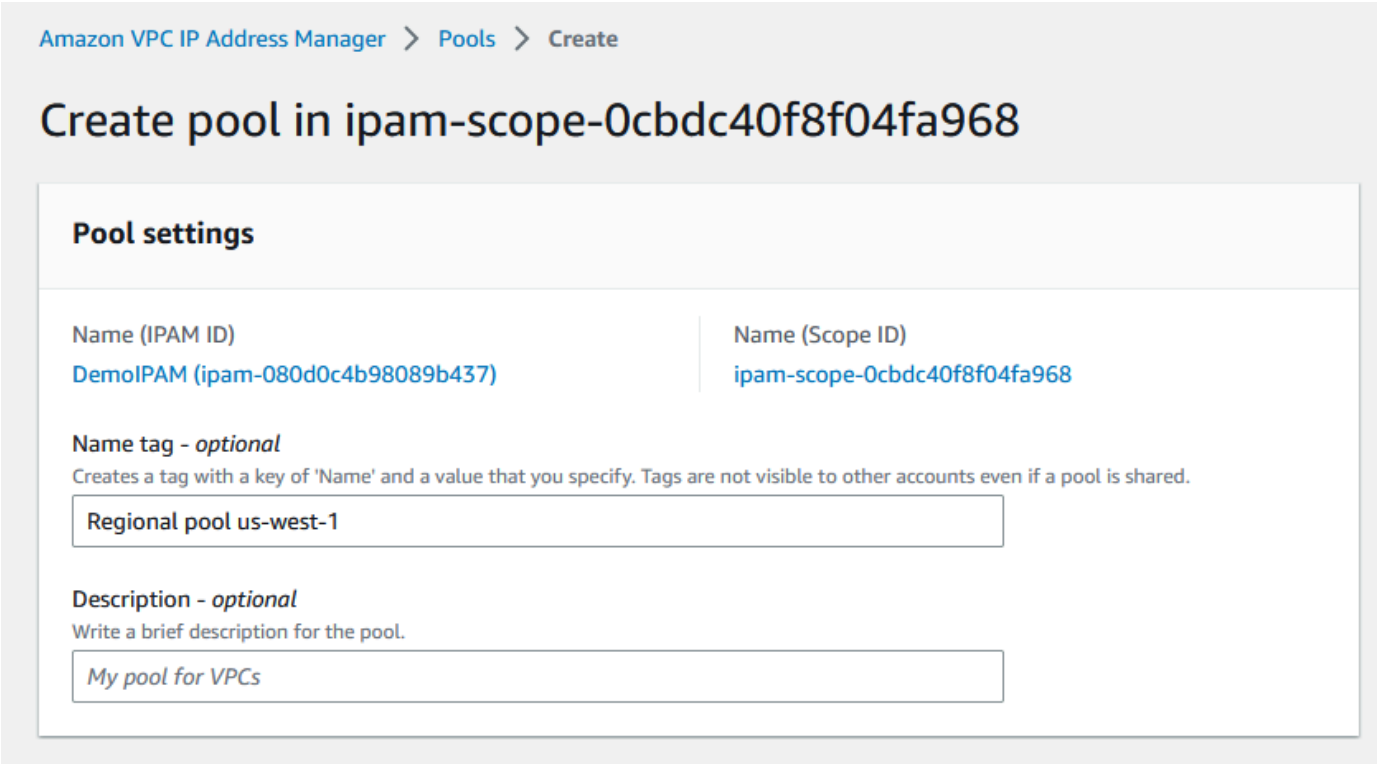
So erstellen Sie einen regionalen Pool

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.

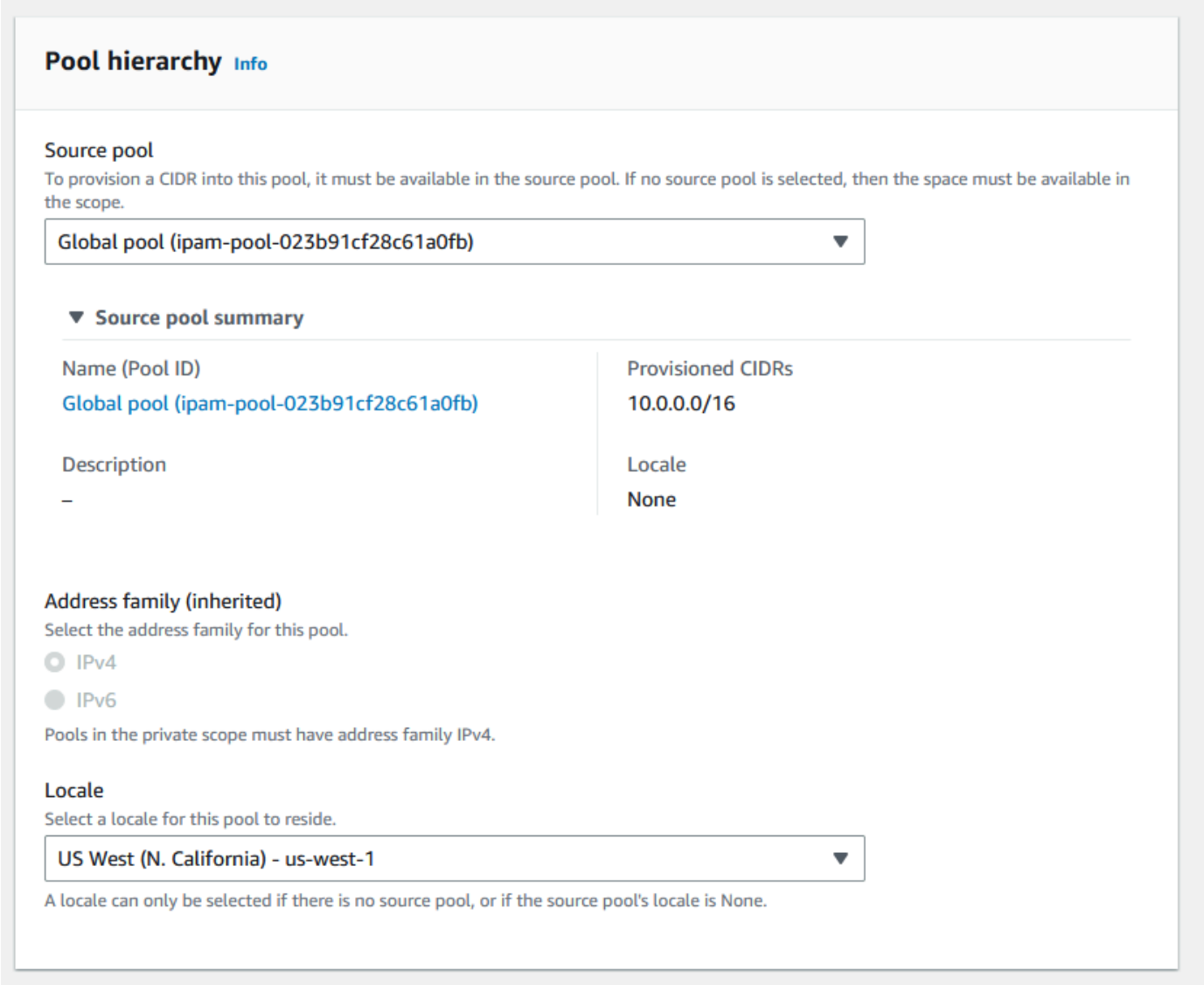
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich aus.



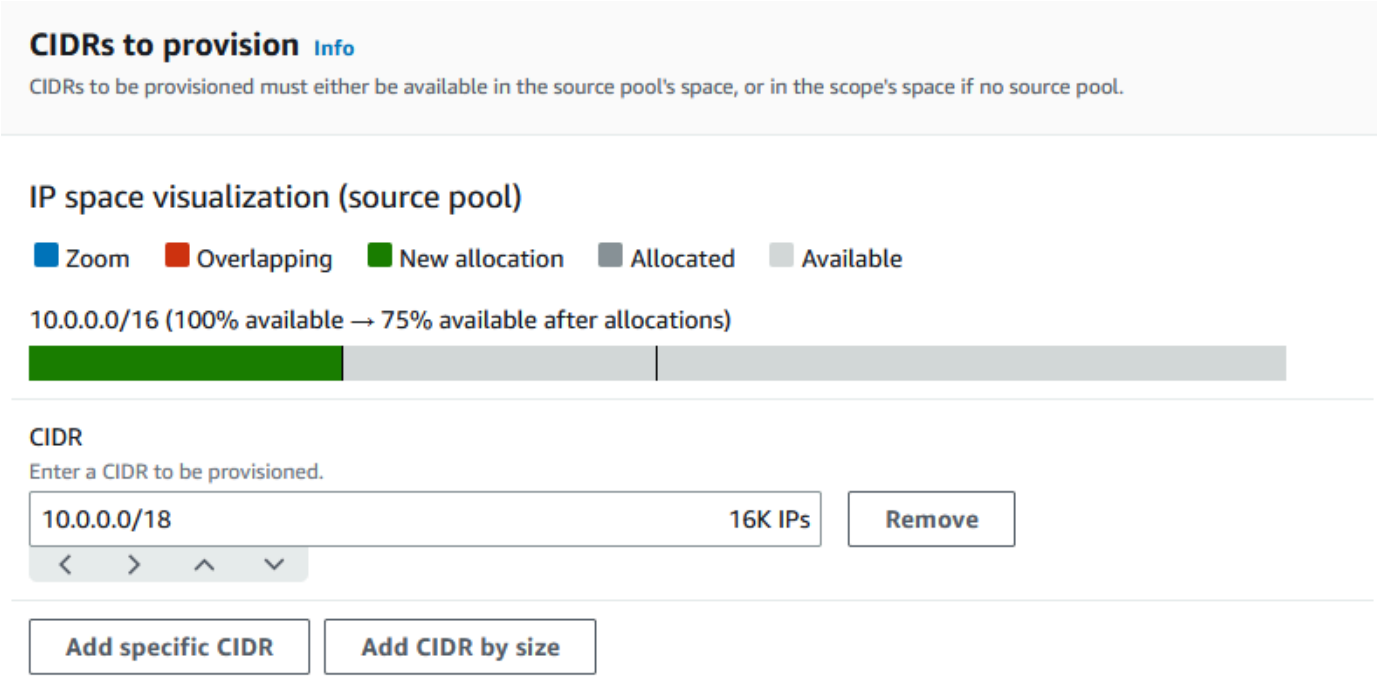
4. Wählen Sie Pool erstellen.
5. Lassen Sie unter IPAM-Bereich den privaten Bereich ausgewählt.
6. (Optional) Fügen Sie ein Namens-Tag und eine Beschreibung für den Pool hinzu, z. B. Regionaler Pool us-west-1.



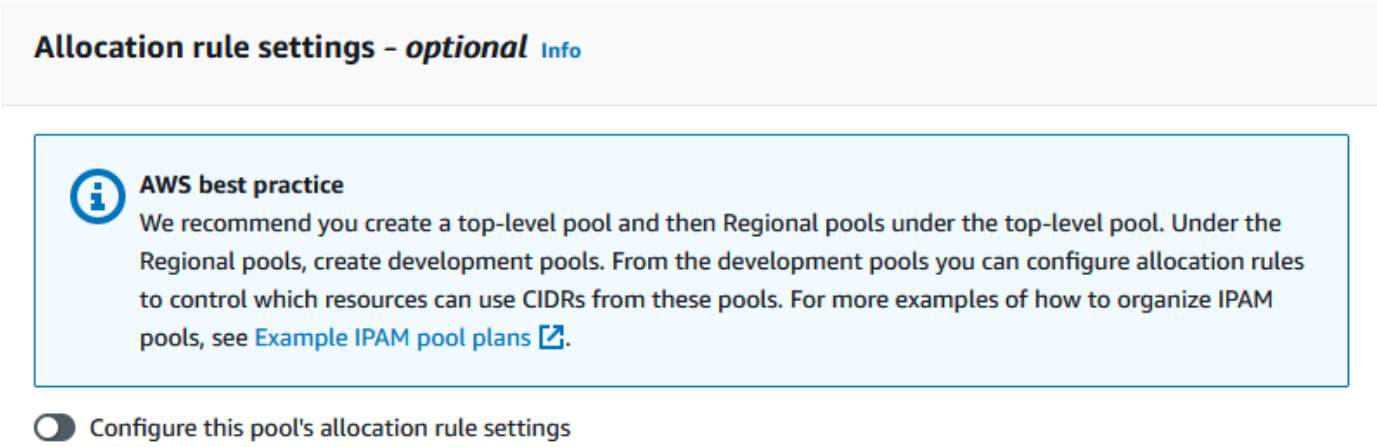
7. Wählen Sie unter Quelle die Option IPAM-Pool und den Pool der obersten Ebene aus („Globaler Pool“), den Sie in Schritt 3: Erstellen Sie einen IPAM-Pool der obersten Ebene erstellt haben. Wählen Sie dann unter Gebietsschema die Option us-west-1 aus.



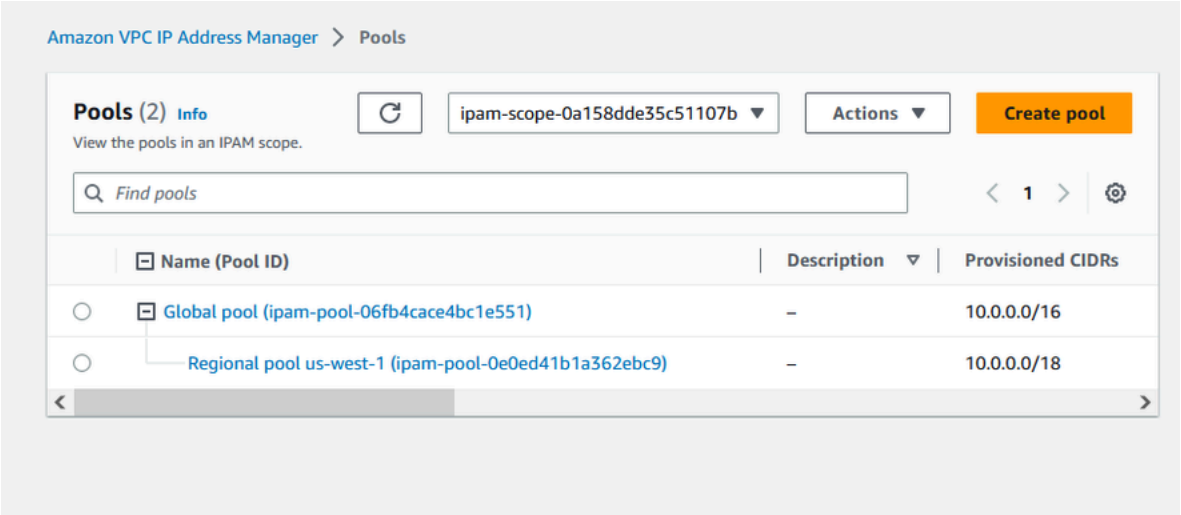
8. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
9. Geben Sie unter Bereitzustellende CIDRs die Zahlenfolge „10.0.0.0/18“ ein. Dadurch erhält dieser Pool rund 16 000 verfügbare IP-Adressen.



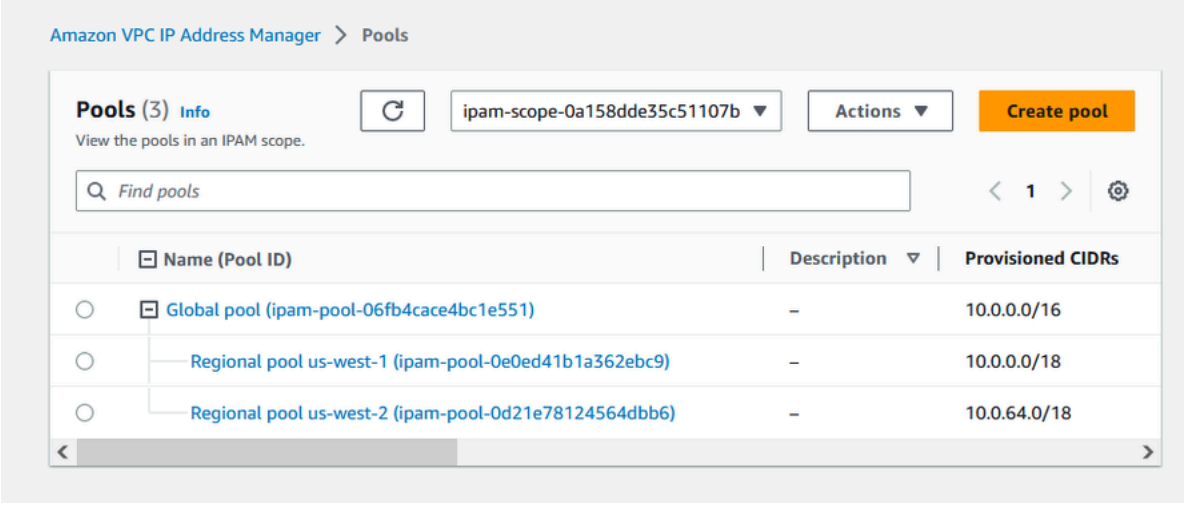
10. Lassen Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren deaktiviert. Sie weisen keine CIDRs direkt aus diesem Pool den VPCs zu. Stattdessen weisen Sie sie aus einem Unterpool zu, den Sie anhand dieses Pools erstellen.



11. Wählen Sie Pool erstellen.
12. Kehren Sie zur Ansicht Pools zurück, um die Hierarchie der von Ihnen erstellten IPAM-Pools anzuzeigen.



13. Wiederholen Sie die Schritte in diesem Abschnitt und erstellen Sie einen zweiten regionalen Pool im Gebietsschema us-west-2. Stellen Sie für diesen das CIDR 10.0.64.0/18 bereit. Nach Abschluss dieses Vorgangs haben Sie drei Pools in einer Hierarchie, die der folgenden ähnelt:

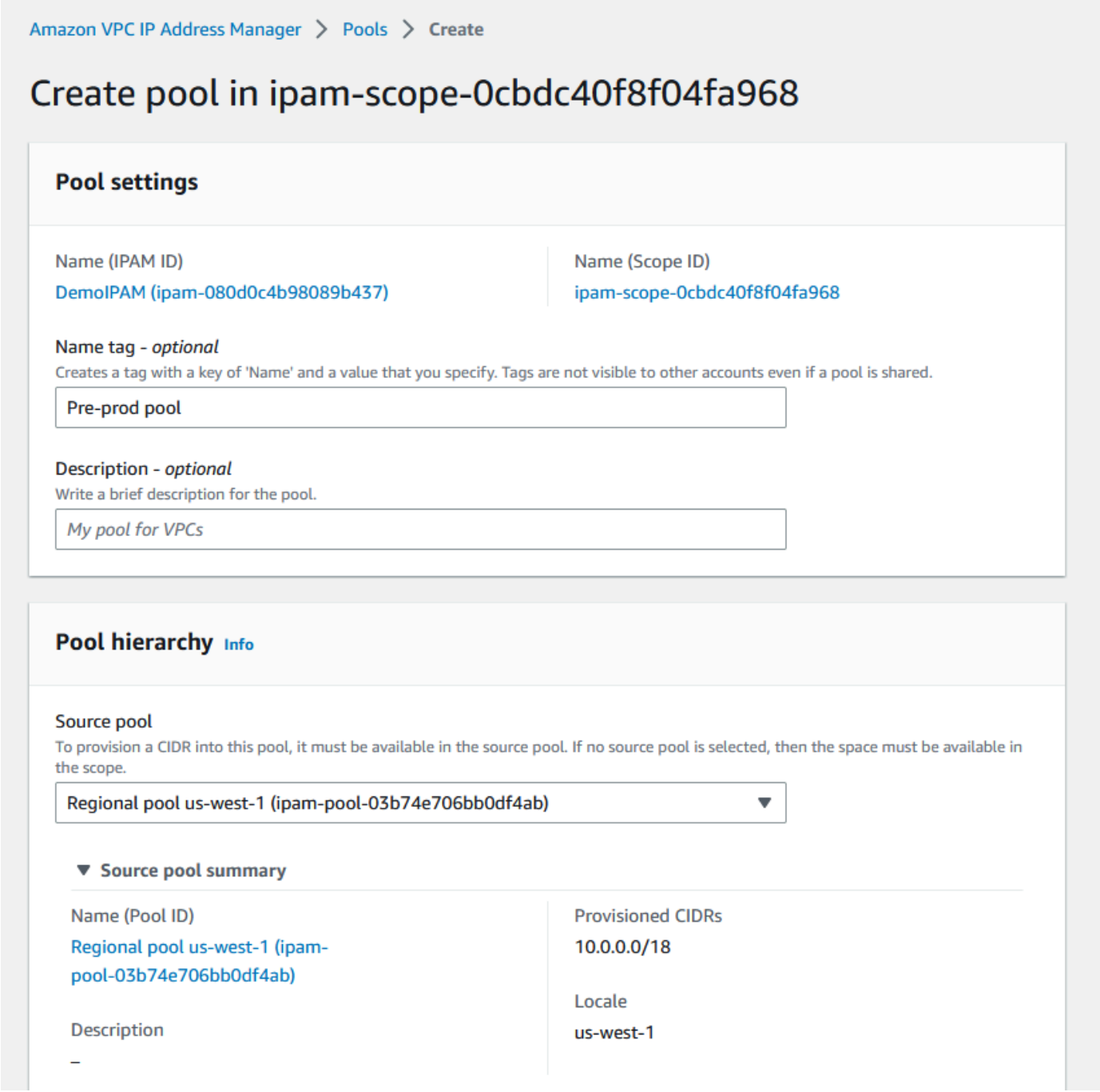


Schritt 5: Erstellen eines Entwicklungspools für die Vorproduktion

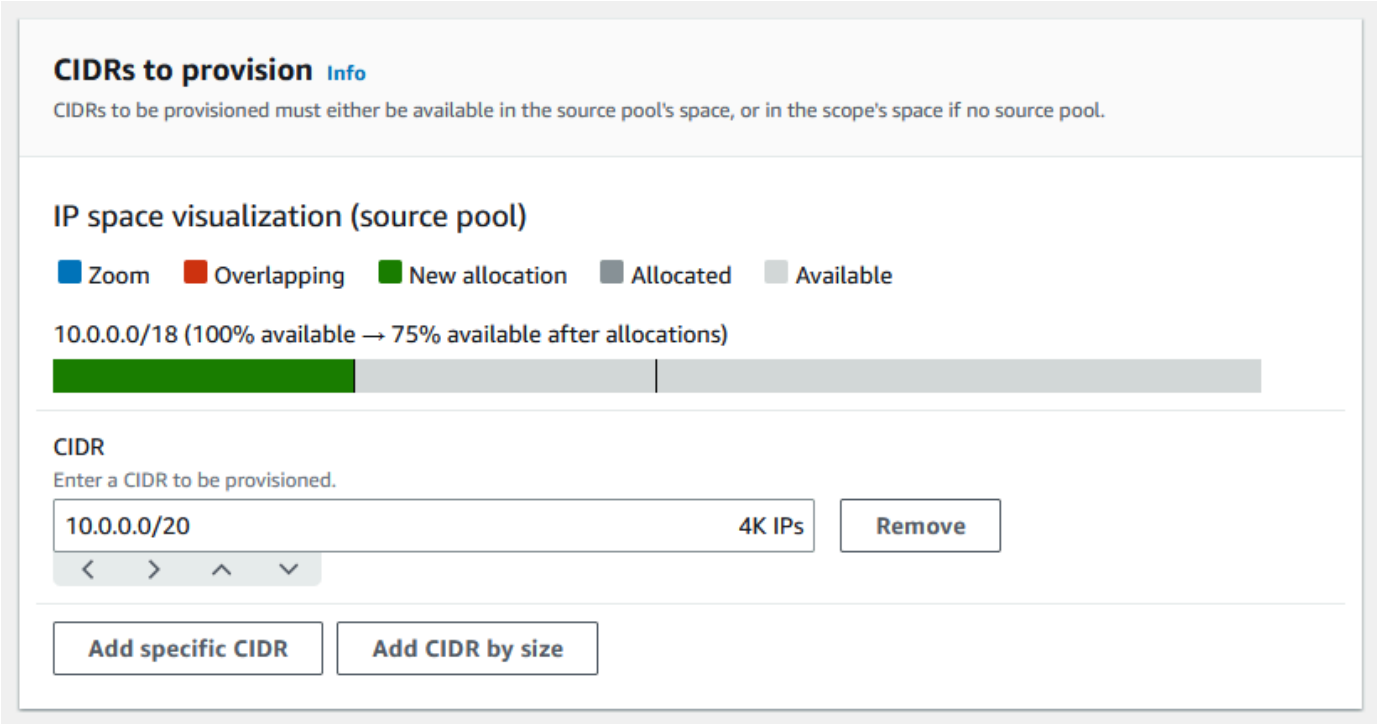
Führen Sie die Schritte in diesem Abschnitt aus, um in einem Ihrer regionalen Pools einen Entwicklungspool für Vorproduktionsressourcen zu erstellen.

So erstellen Sie einen Entwicklungspool für die Vorproduktion

1. Erstellen Sie genauso wie im vorherigen Abschnitt mithilfe des IPAM-Administratorkontos einen Pool namens Vorproduktions-Pool. Nutzen Sie diesmal jedoch den regionalen Pool us-west-1 als Quellpool.

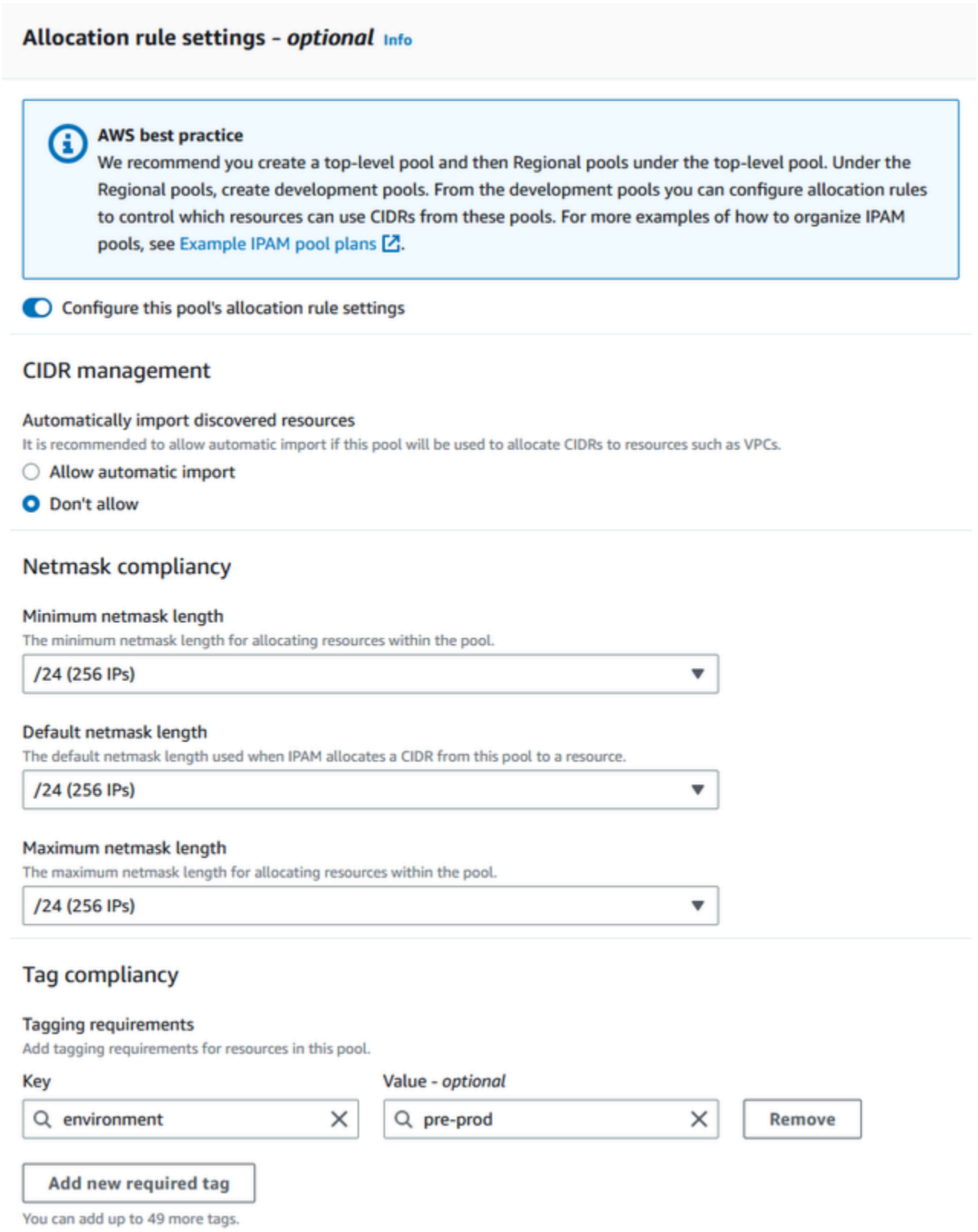


2. Geben Sie als bereitzustellenden CIDR „10.0.0.0/20“ an. Dadurch erhält dieser Pool rund 4 000 IP-Adressen.



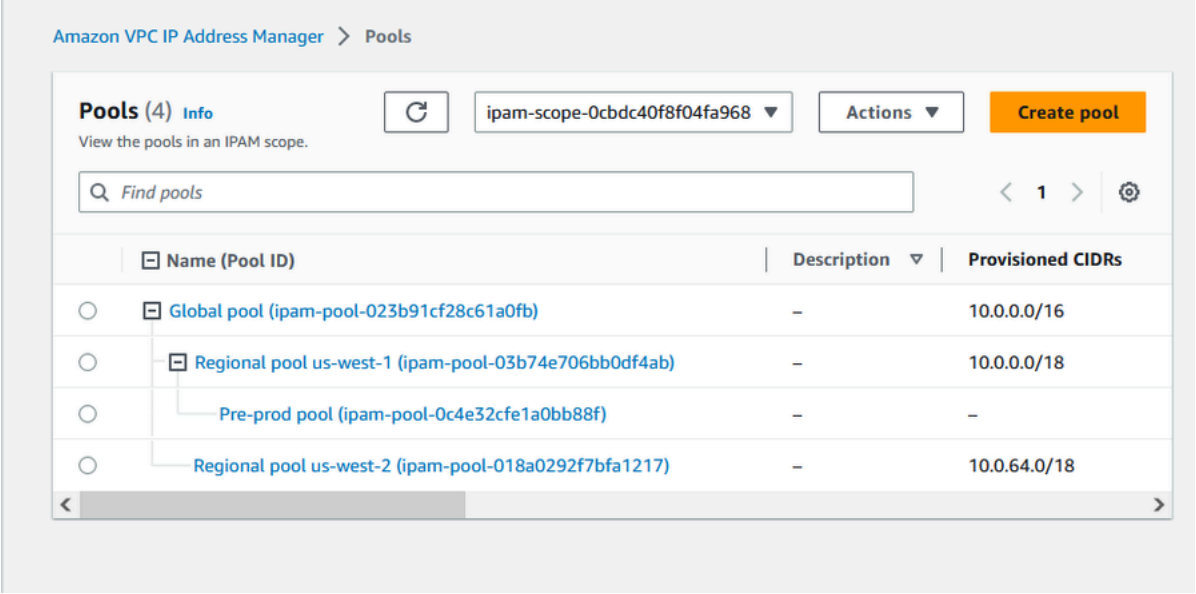
3. Schalten Sie die Option Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren um. Gehen Sie wie folgt vor:

   1. Lassen Sie unter CIDR-Verwaltung für Entdeckte Ressourcen automatisch importieren die Standardoption Nicht erlauben aktiviert. Diese Option würde es IPAM ermöglichen, automatisch Ressourcen-CIDRs zu importieren, die es im Gebietsschema des Pools ermittelt. Eine detaillierte Beschreibung dieser Option würde den Rahmen dieses Tutorials sprengen. Unter Erstellen eines IPv4-Pools der obersten Ebene können Sie jedoch mehr über die Option erfahren.
   2. Wählen Sie unter Netzmasken-Konformität die Option /24 für die minimale, standardmäßige und maximale Netzmaskenlänge aus. Eine detaillierte Beschreibung dieser Option würde den Rahmen dieses Tutorials sprengen. Unter Erstellen eines IPv4-Pools der obersten Ebene können Sie jedoch mehr über die Option erfahren. Wichtiger Hinweis: Die VPC, die Sie später mit einem CIDR aus diesem Pool erstellen, ist auf Grundlage der hier vorgenommenen Einstellung auf /24 begrenzt.
   3. Geben Sie unter Tag-Compliance den Wert Umgebung/Vorproduktion ein. Dieses Tag wird benötigt, damit VPCs Adressraum aus dem Pool zuweisen können. Wir zeigen später, wie das funktioniert.



4. Wählen Sie Pool erstellen.

5. Die Poolhierarchie umfasst nun einen zusätzlichen Unterpool unter dem regionalen Pool us-west-1:



Jetzt können Sie den IPAM-Pool für ein anderes Mitgliedskonto in Ihrer Organisation freigeben und diesem Konto erlauben, zur Erstellung einer VPC ein CIDR aus dem Pool zuzuweisen.

Schritt 6: Freigeben des IPAM-Pools

Führen Sie die Schritte in diesem Abschnitt aus, um den IPAM-Pool für die Vorproduktion mithilfe von AWS Resource Access Manager (RAM) freizugeben.

Dieser Abschnitt besteht aus zwei Unterabschnitten:

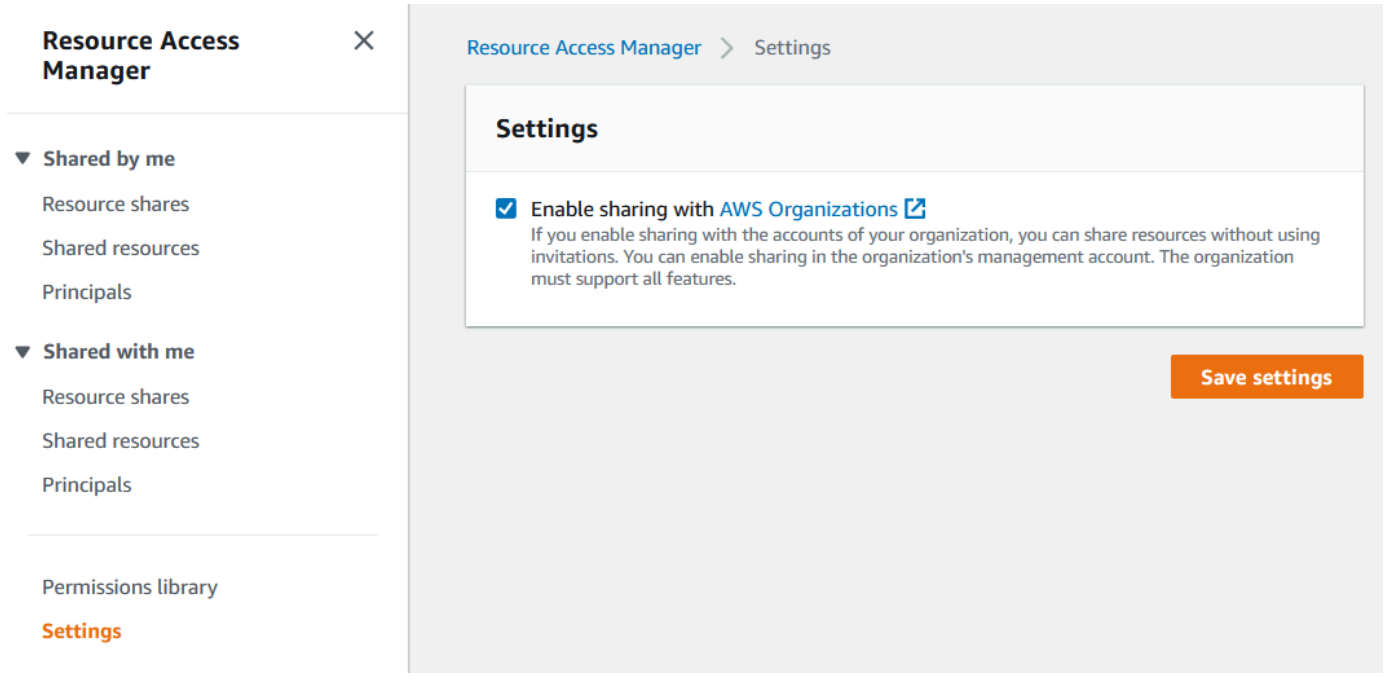
- Schritt 6.1. Aktivieren der Ressourcenfreigabe in AWS RAM: Dieser Schritt muss über das AWS Organizations-Verwaltungskonto ausgeführt werden.
- Schritt 6.2. Freigeben eines IPAM-Pools mit AWS RAM: Dieser Schritt muss vom IPAM-Administrator ausgeführt werden.

Schritt 6.1. Aktivieren der Ressourcenfreigabe in AWS RAM

Nachdem Sie den IPAM erstellt haben, sollten Sie IP-Adresspools für andere Konten in Ihrer Organisation freigeben. Führen Sie vor der Freigabe eines IPAM-Pools die Schritte in diesem Abschnitt aus, um die Ressourcenfreigabe mit AWS RAM zu aktivieren.

So aktivieren Sie die Ressourcenfreigabe

1. Öffnen Sie mit dem Verwaltungskonto von AWS Organizations die AWS RAM-Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie im linken Navigationsbereich nacheinander Einstellungen, Freigabe aktivieren mit AWS Organizations und Einstellungen speichern aus.



Nun können Sie einen IPAM-Pool für andere Mitglieder der Organisation freigeben.

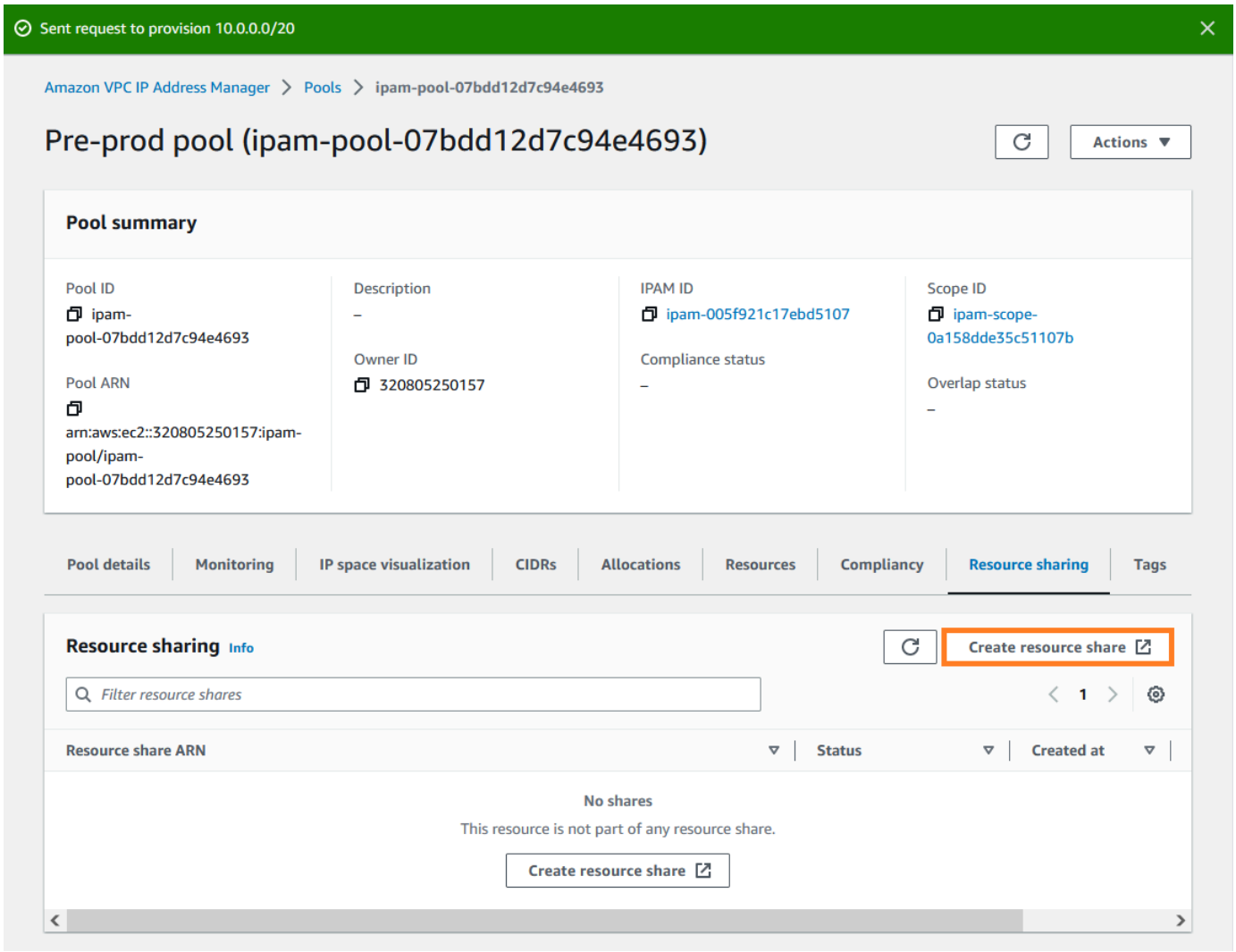
Schritt 6.2. Freigeben eines IPAM-Pools mit AWS RAM

In diesem Abschnitt geben Sie den Entwicklungspool für die Vorproduktion für ein anderes Mitgliedskonto von AWS Organizations frei. Vollständige Anweisungen zur Freigabe von IPAM-Pools, einschließlich Informationen zu den erforderlichen IAM-Berechtigungen, finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM.

So geben Sie einen IPAM-Pool mit AWS RAM frei

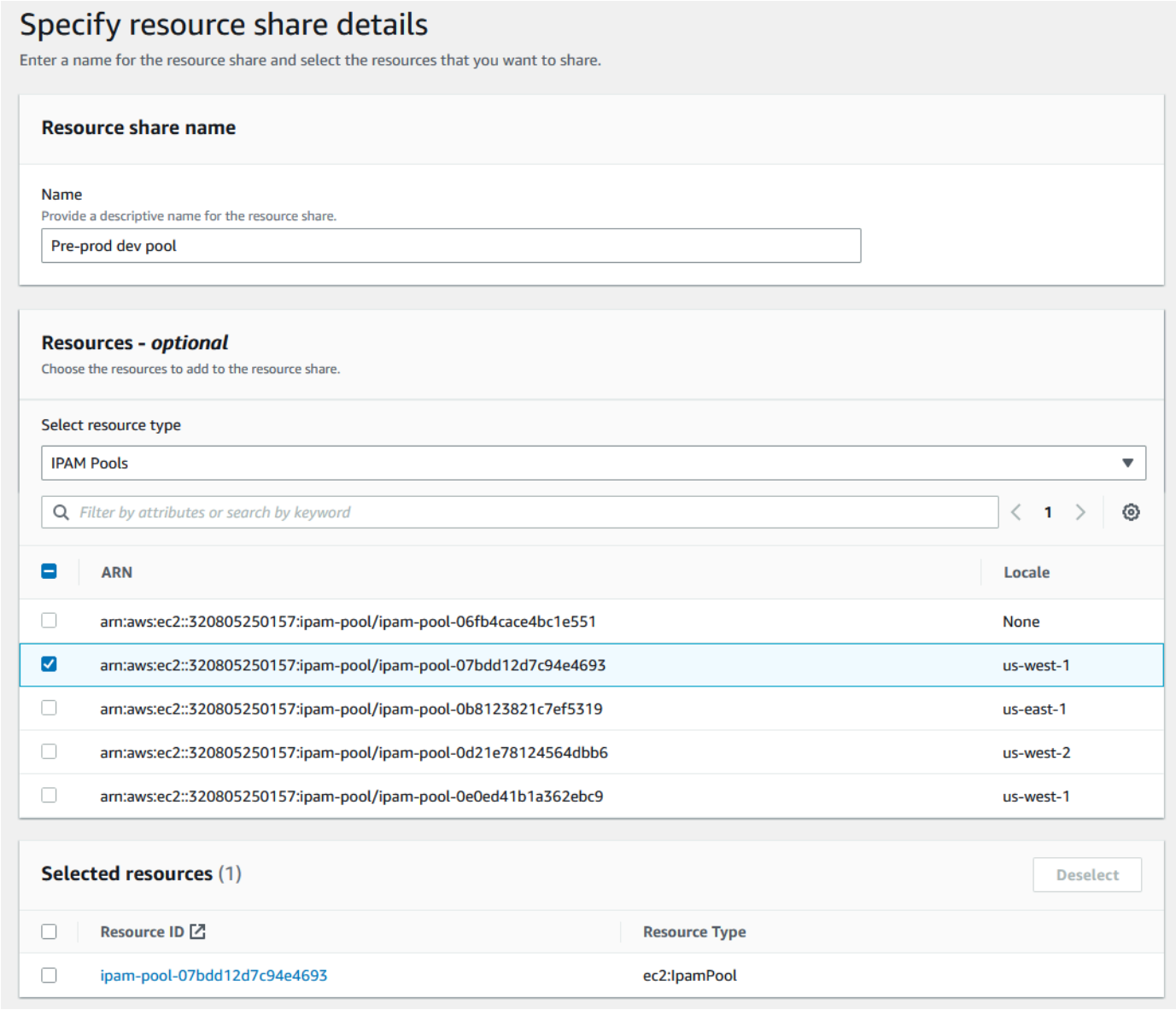
1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich und dann den IPAM-Pool für die Vorproduktion aus. Wählen Sie anschließend Aktionen > Details anzeigen aus.

4. Unter Resource sharing (Ressourcenfreigabe), wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus. Die AWS RAM-Konsole wird geöffnet. Sie geben den Pool mit AWS RAM frei.
5. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.

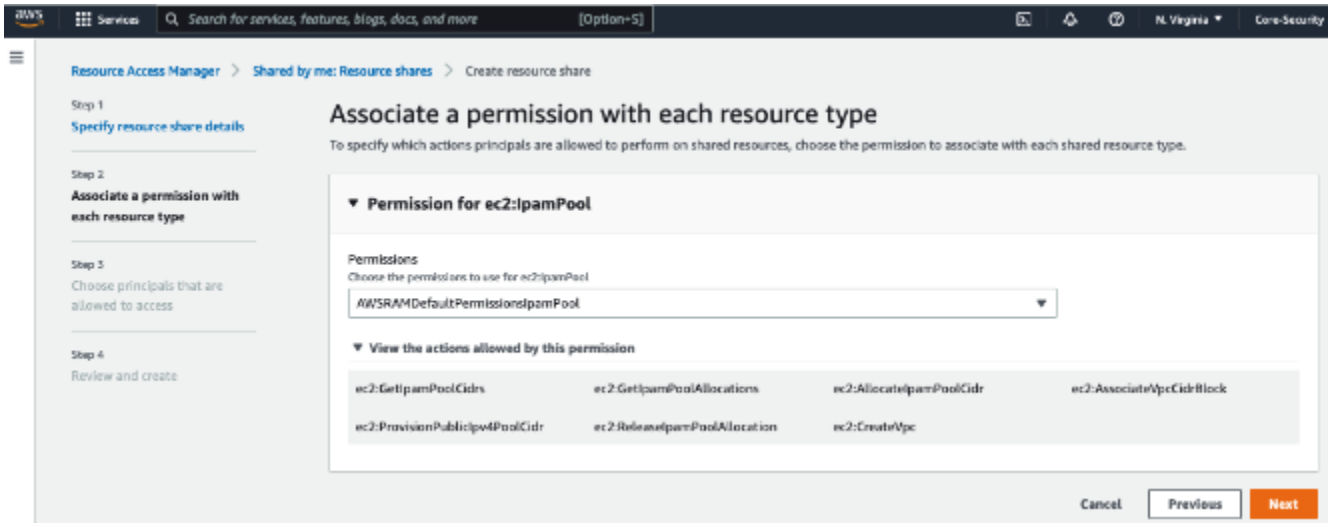


Die AWS RAM-Konsole wird geöffnet.

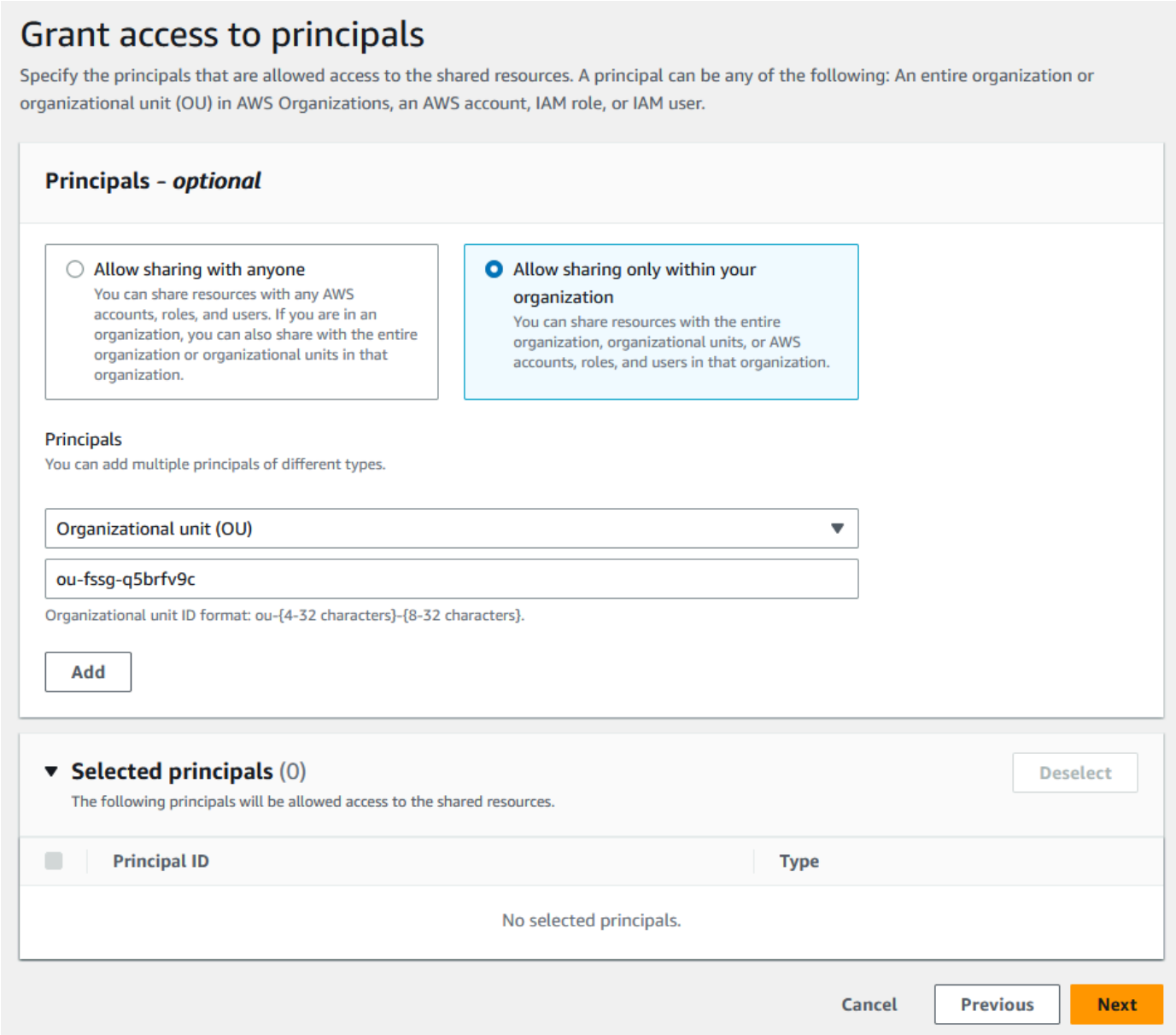
6. Wählen Sie in der AWS RAM-Konsole erneut Ressourcenfreigabe erstellen aus.
7. Fügen Sie einen Namen für den freigegebenen Pool hinzu.
8. Wählen Sie unter Ressourcentyp auswählen die Option IPAM-Pools und dann den ARN des Entwicklungspools für die Vorproduktion aus.



9. Wählen Sie Next (Weiter).
10. Lassen Sie die Standardberechtigung AWSRAMDefaultPermissionsIpamPool aktiviert. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mit AWS RAM können Sie jedoch mehr über diese Optionen erfahren.



11. Wählen Sie Next (Weiter).
12. Wählen Sie unter Prinzipale die Option Zulassen der Freigabe nur innerhalb der eigenen Organisation aus. Geben Sie die ID Ihrer Organisationseinheit von AWS Organizations ein (wie unter So lässt sich AWS Organizations in IPAM integrieren erwähnt). Wählen Sie dann Hinzufügen aus.



13. Wählen Sie Next (Weiter).
14. Überprüfen Sie die Optionen für die Ressourcenfreigabe und die Prinzipale, für die die Freigabe erfolgt. Wählen Sie dann Erstellen aus.

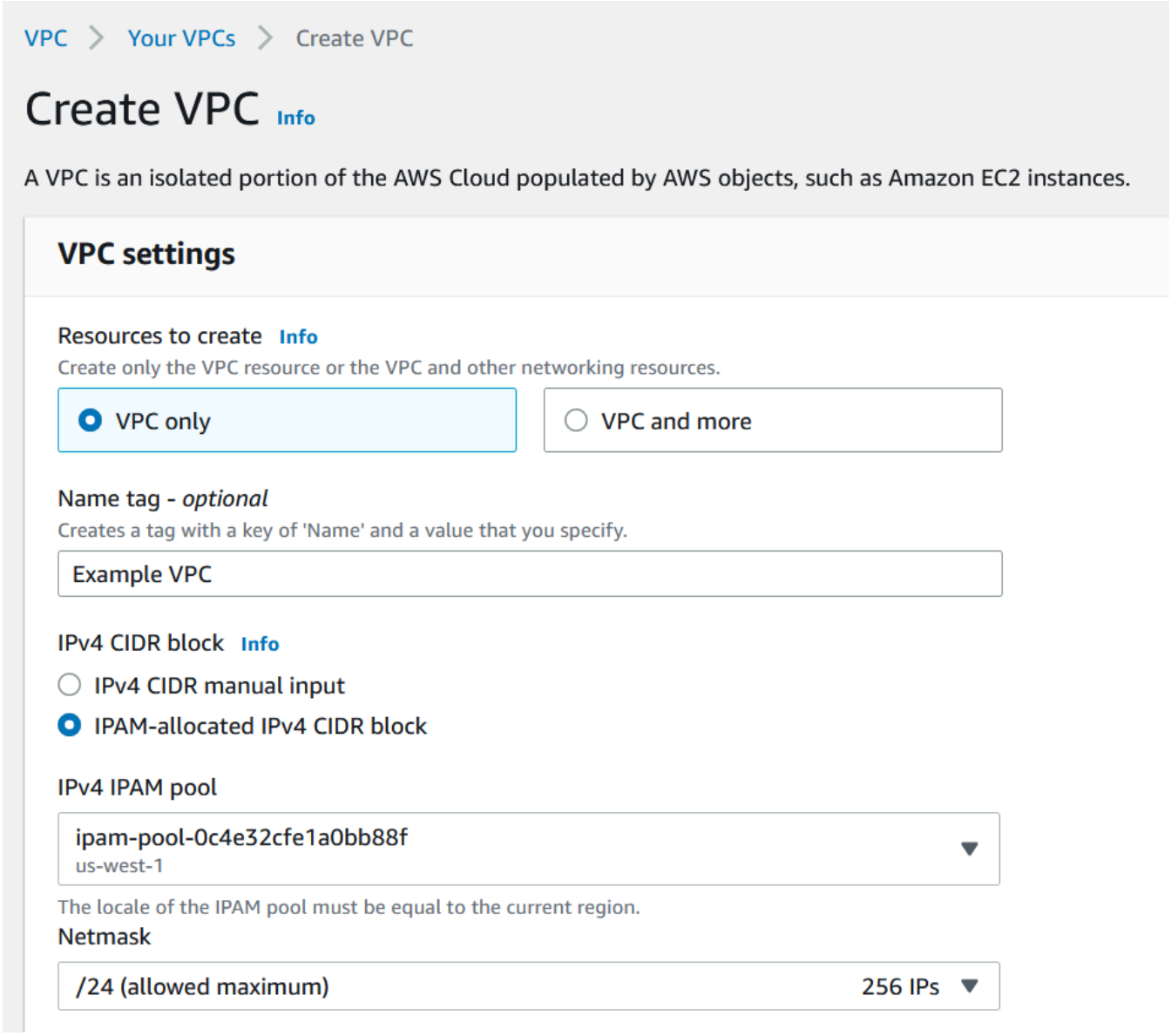
Nach der Freigabe des Pools fahren Sie mit dem nächsten Schritt fort, um eine VPC mit einem CIDR zu erstellen, das aus einem IPAM-Pool zugewiesen wird.

Schritt 7: Erstellen einer VPC mit einem CIDR, das aus einem IPAM-Pool zugewiesen wurde

Führen Sie die Schritte in diesem Abschnitt aus, um eine VPC mit einem CIDR zu erstellen, das aus dem Vorproduktionspool zugewiesen wird. Dieser Schritt sollte über das Mitgliedskonto in der Organisationseinheit durchgeführt werden, für das der IPAM-Pool im vorherigen Abschnitt freigegeben wurde (unter So lässt sich AWS Organizations in IPAM integrieren als example-member-account-2 bezeichnet). Weitere Informationen zu den IAM-Berechtigungen, die zum Erstellen von VPCs erforderlich sind, finden Sie unter Beispiele für Amazon-VPC-Richtlinien im Benutzerhandbuch von Amazon VPC.

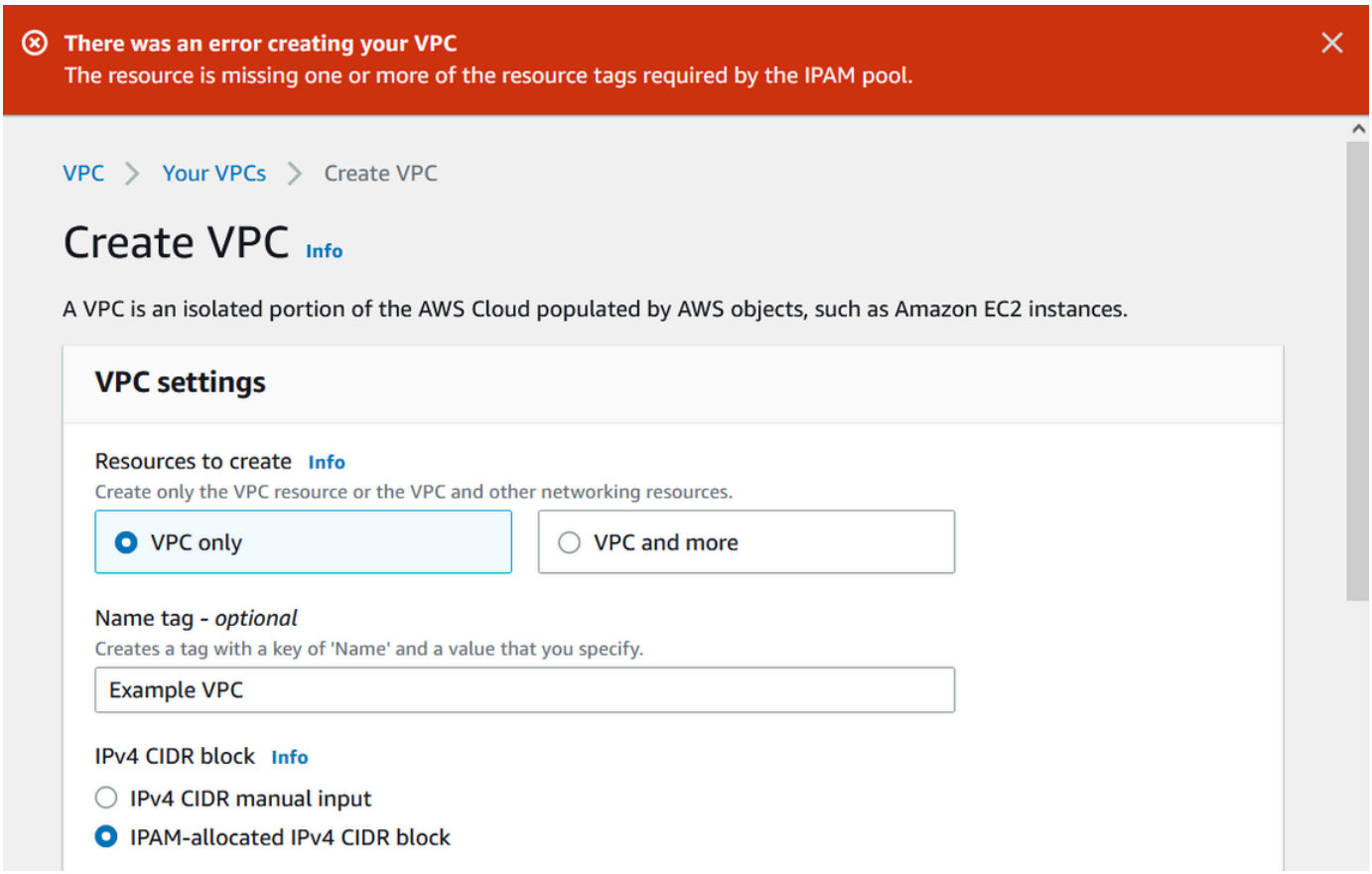
So erstellen Sie eine VPC mit einem CIDR, das aus einem IPAM-Pool zugewiesen wird

1. Öffnen Sie mit dem Mitgliedskonto die VPC-Konsole unter https://console.aws.amazon.com/vpc/ als Mitgliedskonto, das Sie als Entwicklerkonto verwenden möchten.
2. Wählen Sie VPC erstellen aus.
3. Gehen Sie wie folgt vor:
    1. Geben Sie einen Namen ein, wie etwa Beispiel-VPC.
    2. Wählen Sie Von IPAM zugewiesener IPv4-CIDR-Block aus.
    3. Wählen Sie unter IPv4-IPAM-Pool die ID des Vorproduktionspools aus.
    4. Wählen Sie eine Länge für die Netzmaske aus. Da Sie die verfügbare Netzmaskenlänge für diesen Pool auf /24 begrenzt haben (unter Schritt 5: Erstellen eines Entwicklungspools für die Vorproduktion), ist /24 die einzige verfügbare Netzmaskenoption.

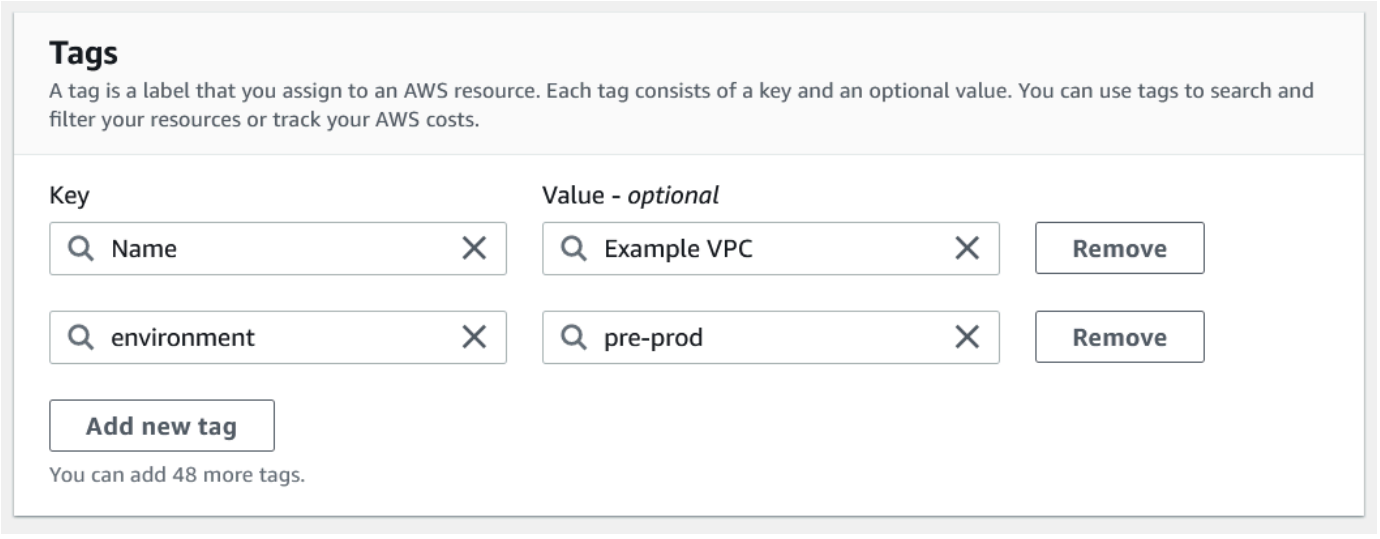


4. Fügen Sie – zu Demonstrationszwecken – unter Tags zum jetzigen Zeitpunkt keine zusätzlichen Tags hinzu. Bei der Erstellung des Vorproduktionspools (unter 5. Erstellen eines Entwicklungspools für die Vorproduktion) haben Sie eine Zuweisungsregel hinzugefügt, nach der VPCs, die mit CIDRs aus diesem Pool erstellt werden, über ein Umgebungs-/Vorproduktions-Tag verfügen müssen. Lassen Sie das Umgebungs-/Vorproduktions-Tag vorerst deaktiviert, damit eine Fehlermeldung mit dem Hinweis angezeigt wird, dass ein erforderliches Tag nicht hinzugefügt wurde.
5. Wählen Sie VPC erstellen aus.
6. Es wird eine Fehlermeldung mit dem Hinweis angezeigt, dass ein erforderliches Tag nicht hinzugefügt wurde. Der Fehler tritt auf, weil Sie beim Erstellen des Vorproduktionspools (unter Schritt 5: Erstellen eines Entwicklungspools für die Vorproduktion) eine Zuweisungsregel

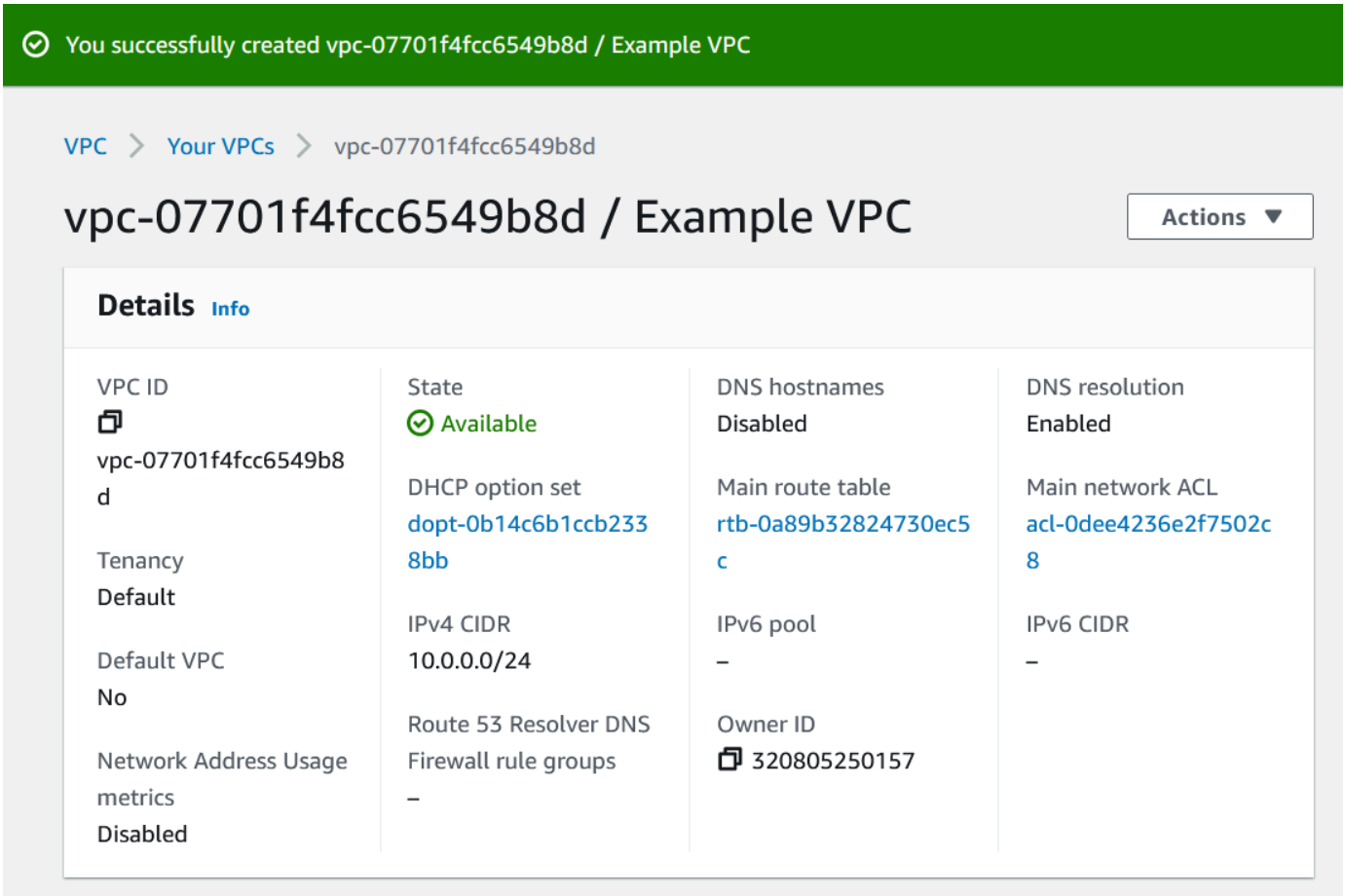
festgelegt haben. Nach der Zuweisungsregel müssen VPCs, die mit CIDRs aus diesem Pool erstellt werden, über ein Umgebungs-/Vorproduktions-Tag verfügen.



7. Fügen Sie nun unter Tags das Tag Umgebung/Vorproduktion hinzu und wählen Sie erneut VPC erstellen aus.



8. Die VPC wird erfolgreich erstellt und die VPC entspricht der Tag-Regel im Vorproduktionspool:



Im Bereich Ressourcen der IPAM-Konsole kann der IPAM-Administrator die VPC und das zugewiesene CIDR einsehen und verwalten. Hinweis: Es dauert etwas, bis die VPC im Bereich Ressourcen angezeigt wird.

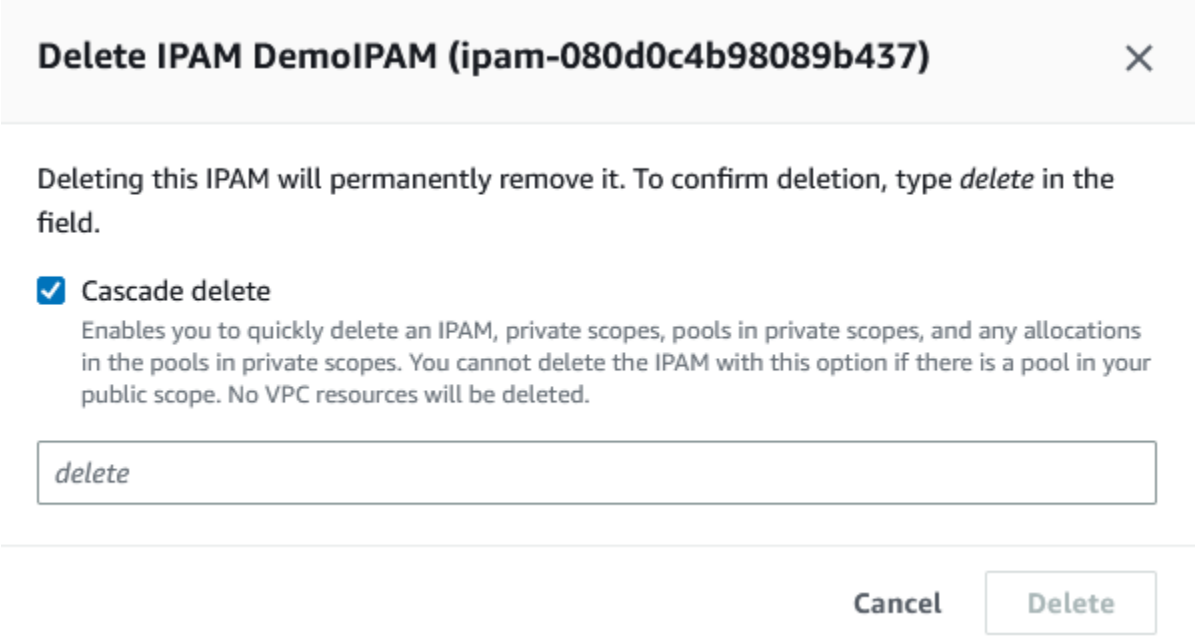
Schritt 8: Bereinigen

In diesem Tutorial haben Sie einen IPAM mit einem delegierten Administrator erstellt, mehrere Pools erstellt und ein Mitgliedskonto in Ihrer Organisation aktiviert, um ein VPC-CIDR aus einem Pool zuzuweisen.

Führen Sie die Schritte in diesem Abschnitt aus, um die Ressourcen zu bereinigen, die Sie in diesem Tutorial erstellt haben.

So bereinigen Sie die in diesem Tutorial erstellten Ressourcen

1. Löschen Sie die VPC mithilfe des Mitgliedskontos, über das die Beispiel-VPC erstellt wurde. Eine ausführliche Anleitung finden unter Löschen der VPC im Benutzerhandbuch von Amazon Virtual Private Cloud.
2. Löschen Sie mithilfe des IPAM-Administratorkontos die Beispielressourcenfreigabe in der AWS RAM-Konsole. Eine ausführliche Anleitung finden Sie unter Löschen einer Ressourcenfreigabe in AWSAWS RAM im Benutzerhandbuch von AWS Resource Access Manager.
3. Melden Sie sich mit dem IPAM-Administratorkonto bei der RAM-Konsole an und deaktivieren Sie die Freigabe für AWS Organizations, die Sie unter Schritt 6.1. Aktivieren der Ressourcenfreigabe in AWS RAM aktiviert haben.
4. Löschen Sie den Beispiel-IPAM mithilfe des IPAM-Administratorkontos, indem Sie den IPAM in der IPAM-Konsole auswählen und dann Aktionen > Löschen auswählen. Detaillierte Anweisungen finden Sie unter Löschen Sie ein IPAM.
5. Wenn Sie aufgefordert werden, den IPAM zu löschen, wählen Sie Als Kaskade löschen aus. Dadurch werden alle Bereiche und Pools im IPAM gelöscht, bevor er gelöscht wird.



6. Geben Sie delete ein und wählen Sie Löschen aus.
7. Melden Sie sich mit dem Verwaltungskonto von AWS Organizations bei der IPAM-Konsole an, wählen Sie Einstellungen aus und entfernen Sie das delegierte Administratorkonto.
8. (Optional) Wenn Sie IPAM in AWS Organizations integrieren, erstellt IPAM automatisch eine serviceverknüpfte Rolle in jedem Mitgliedskonto. Melden Sie sich mit jedem Mitgliedskonto

von AWS Organizations bei IAM an und löschen Sie jeweils die serviceverknüpfte Rolle AWSServiceRoleForIPAM darin.

9. Die Bereinigung ist abgeschlossen.

Tutorial: Erstellen eines IPAM und von Pools mit der AWS CLI

Führen Sie die Schritte in diesem Tutorial aus, um mit der AWS CLI einen IPAM zu erstellen, IP-Adresspools zu erstellen und eine VPC mit einem CIDR aus einem IPAM-Pool zuzuweisen.

Im Folgenden sehen Sie eine Beispielhierarchie der Poolstruktur, die Sie erstellen, indem Sie die Schritte in diesem Abschnitt ausführen:

- IPAM arbeitet in AWS-Region 1, AWS-Region 2
  - Privater Bereich
    - Pool auf oberster Ebene
      - Regionaler Pool in AWS-Region 2
        - Entwicklungs-Pool
          - Zuteilung für eine VPC

> **Note**
>
> In diesem Abschnitt erstellen Sie ein IPAM. Sie können standardmäßig nur ein IPAM erstellen. Weitere Informationen finden Sie unter Kontingente für Ihr IPAM. Wenn Sie bereits ein IPAM-Konto delegiert und ein IPAM erstellt haben, können Sie die Schritte 1 und 2 überspringen.

Inhalt

- Schritt 7. Erstellen Sie eine RAM-Freigabe zum Aktivieren von IP-Zuweisungen über Konten hinweg
- Schritt 8. Erstellen einer VPC
- Schritt 9. Bereinigen

Schritt 1: Aktivieren von IPAM in Ihrer Organisation

Dieser Schritt ist optional. Führen Sie diesen Schritt aus, um IPAM in Ihrer Organisation zu aktivieren und Ihr delegiertes IPAM mithilfe der AWS CLI zu konfigurieren. Weitere Informationen zur Rolle des IPAM-Kontos finden Sie unter Integrieren von IPAM mit Konten in einer - AWS Organisation.

Diese Anfrage muss von einem Managementkonto für AWS Organizations gemacht werden. Stellen Sie beim Ausführen des folgenden Befehls sicher, dass Sie eine Rolle mit einer IAM-Richtlinie verwenden, die die folgenden Aktionen zulässt:

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

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

Sie sollten die folgende Ausgabe sehen, die darauf hinweist, dass die Aktivierung erfolgreich war.

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

Schritt 2: Erstellen eines IPAMs

Führen Sie die Schritte in diesem Abschnitt aus, um ein IPAM zu erstellen und zusätzliche Informationen über die erstellten Bereiche anzuzeigen. Sie verwenden dieses IPAM, wenn Sie Pools erstellen und in späteren Schritten IP-Adressbereiche für diese Pools bereitstellen.

> **Note**
>
> Die Option „Betriebsregionen“ bestimmt, für welche AWS-Regionen die IPAM-Pools verwendet werden können. Weitere Informationen zum Betrieb von Regionen finden Sie unter Erstellen eines IPAM.

So erstellen Sie ein IPAM mithilfe der AWS CLI

1. Führen Sie den folgenden Befehl aus, um die IPAM-Instance zu erstellen.

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

Wenn Sie ein IPAM erstellen, führt AWS automatisch Folgendes aus:

- Gibt eine global eindeutige Ressourcen-ID (`IpamId`) für das IPAM zurück.
- Erstellt einen öffentlichen Standardbereich (`PublicDefaultScopeId`) und einen privaten Standardbereich (`PrivateDefaultScopeId`).


```
{

    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-0de83dba6694560a9",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
        "PublicDefaultScopeId": "ipam-scope-02a24107598e982c5",
        "PrivateDefaultScopeId": "ipam-scope-065e7dfe880df679c",
        "ScopeCount": 2,
        "Description": "my-ipam",
        "OperatingRegions": [
            {
                "RegionName": "us-west-2"
            },
            {
                "RegionName": "us-east-1"
            }
        ],
        "Tags": []
    }
```

```
}
```

2. Führen Sie den folgenden Befehl aus, um zusätzliche Informationen im Zusammenhang mit den Bereichen anzuzeigen. Der öffentliche Bereich ist für IP-Adressen vorgesehen, auf die über das öffentliche Internet zugegriffen werden soll. Der private Bereich ist für IP-Adressen gedacht, auf die nicht über das öffentliche Internet zugegriffen werden kann.

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

In der Ausgabe sehen Sie die verfügbaren Bereiche. Im nächsten Schritt verwenden Sie die ID des privaten Bereichs.

```
{
    "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
        }
    ]
}
```

Schritt 3: Erstellen eines IPv4-Adressenpools

Um einen IPv4-Adressenpool zu erstellen, führen Sie die Schritte in diesem Abschnitt aus.

> **Important**
>
> Sie werden die `--locale`-Option auf diesem Pool der obersten Ebene nicht verwenden. Sie legen das Gebietsschema im Regionalpool fest. Das Gebietsschema ist die AWS-Region, in der ein Pool für CIDR-Zuweisungen verfügbar sein soll. Da das Gebietsschema nicht im Pool der obersten Ebene festgelegt wird, ist das Gebietsschema standardmäßig `None`. Wenn ein Pool ein Gebietsschema von `None` hat, wird der Pool für VPC-Ressourcen in jeder AWS-Region nicht verfügbar sein. Sie können den IP-Adressraum im Pool nur manuell zuweisen, um Speicherplatz zu reservieren.

So erstellen Sie einen IPv4-Adresspool für alle Ihre AWS-Ressourcen mithilfe der AWS CLI

1. Führen Sie den folgenden Befehl aus, um einen IPv4-Adressenpool zu erstellen. Verwenden Sie die ID des privaten Bereichs des IPAM, den Sie im vorherigen Schritt erstellt haben.

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

   In der Ausgabe sehen Sie einen Status von `create-in-progress` für den Pool.

   ```
   {
       "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. Führen Sie den folgenden Befehl aus, bis Sie den Status von `create-complete` in der Ausgabe sehen.

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

Die folgende Beispielausgabe zeigt den korrekten Zustand.

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

Schritt 4: Stellen Sie ein CIDR für den Pool der obersten Ebene bereit

Führen Sie die Schritte in diesem Abschnitt aus, um einen CIDR für den Pool der obersten Ebene bereitzustellen, und überprüfen Sie dann, ob das CIDR bereitgestellt wurde. Weitere Informationen finden Sie unter Bereitstellen von CIDRs für einen Pool.

So stellen Sie einen CIDR-Block für den Pool mit der AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

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

In der Ausgabe können Sie den Status der Bereitstellung überprüfen.

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

2. Führen Sie den folgenden Befehl aus, bis Sie den Status von `provisioned` in der Ausgabe sehen.

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

Die folgende Beispielausgabe zeigt den korrekten Zustand.

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

Schritt 5. Erstellen Sie einen regionalen Pool mit CIDR aus dem Pool der obersten Ebene

Wenn Sie einen IPAM-Pool erstellen, gehört der Pool standardmäßig zur AWS-Region des IPAM. Wenn Sie eine VPC erstellen, muss sich der Pool, aus dem die VPC bezieht, in derselben Region befinden wie die VPC. Sie können die `--locale`-Option beim Erstellen eines Pools verwenden, um den Pool für Dienste in einer anderen Region als der IPAM-Region verfügbar zu machen. Um einen Regionalpool in einem anderen Gebietsschema zu erstellen, führen Sie die Schritte in diesem Abschnitt aus.

So erstellen Sie einen Pool mit einem CIDR aus dem vorherigen Pool unter Verwendung der AWS CLI

1. Führen Sie den folgenden Befehl aus, um den Pool zu erstellen und Leerzeichen mit einem bekannten verfügbaren CIDR aus dem vorherigen Pool einzufügen.

```
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
```

   In der Ausgabe sehen Sie die ID des Pools, den Sie erstellt haben. Sie benötigen diese ID im nächsten Schritt.

```
{
    "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. Führen Sie den folgenden Befehl aus, bis Sie den Status von `create-complete` in der Ausgabe sehen.

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

   In der Ausgabe sehen Sie die Pools, die Sie in Ihrem IPAM haben. In diesem Tutorial haben wir einen Pool auf oberster Ebene und einen regionalen Pool erstellt, sodass Sie beide sehen.

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

Schritt 6: Stellen Sie ein CIDR für den regionalen Pool bereit

Führen Sie die Schritte in diesem Abschnitt aus, um dem Pool einen CIDR-Block zuzuweisen und zu überprüfen, ob er erfolgreich bereitgestellt wurde.

So weisen Sie dem Regionalpool einen CIDR-Block zu, indem Sie die AWS CLI verwenden

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

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

   In der Ausgabe sehen Sie einen Status für den Pool.

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

2. Führen Sie den folgenden Befehl aus, bis Sie den Status von `provisioned` in der Ausgabe sehen.

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

   Die folgende Beispielausgabe zeigt den korrekten Zustand.

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

3. Führen Sie den folgenden Befehl aus, um den Pool der obersten Ebene abzufragen, um die Zuweisungen anzuzeigen. Der Regionalpool gilt als Zuweisung innerhalb des Pools der obersten Ebene.

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

In der Ausgabe sehen Sie den Regionalpool als Zuweisung im Pool der obersten Ebene.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "10.0.0.0/16",
            "IpamPoolAllocationId": "ipam-pool-alloc-
fbd525f6c2bf4e77a75690fc2d93479a",
            "ResourceId": "ipam-pool-0da89c821626f1e4b",
            "ResourceType": "ipam-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Schritt 7. Erstellen Sie eine RAM-Freigabe zum Aktivieren von IP-Zuweisungen über Konten hinweg

Dieser Schritt ist optional. Sie können diesen Schritt nur ausführen, wenn Sie Integrieren von IPAM mit Konten in einer - AWS Organisationabgeschlossen haben.

Wenn Sie einen IPAM-Pool erstellen, ermöglicht die AWS-RAM-Freigabe IP-Zuweisungen über Konten hinweg. RAM-Freigabe ist nur in Ihrer AWS-Heimatregion verfügbar. Beachten Sie, dass Sie diese Freigabe in derselben Region wie das IPAM erstellen, nicht in der lokalen Region für den Pool. Alle Verwaltungsoperationen für IPAM-Ressourcen werden über die Heimatregion Ihres IPAM durchgeführt. Das Beispiel in diesem Tutorial erstellt eine einzelne Freigabe für einen einzelnen Pool, Sie können jedoch mehrere Pools zu einer einzigen Freigabe hinzufügen. Weitere Informationen, einschließlich einer Erläuterung der Optionen, die Sie eingeben müssen, finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM.

Führen Sie den folgenden Befehl aus, um eine Ressourcenfreigabe zu erstellen.

```
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
```

Die Ausgabe zeigt, dass der Pool erstellt wurde.

```
{
    "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
    }
}
```

Schritt 8. Erstellen einer VPC

Führen Sie den folgenden Befehl aus, um eine VPC zu erstellen und der VPC aus dem Pool in Ihrem neu erstellten IPAM einen CIDR-Block zuzuweisen.

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

Die Ausgabe zeigt, dass die VPC erstellt wurde.

```
{
    "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
    }
}
```

Schritt 9. Bereinigen

Führen Sie die Schritte in diesem Abschnitt aus, um die IPAM-Ressourcen zu löschen, die Sie in diesem Tutorial erstellt haben.

1. Löschen der VPC.

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

2. Löschen Sie die RAM-Freigabe des IPAM-Pools.

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

3. Aufhebung des Pools-CIDRs aus dem Regionalpool.

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

4. Heben Sie die Bereitstellung von Pool-CIDR aus dem Pool der obersten Ebene auf.

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

5. Löschen Sie das IPAM

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

Tutorial: Anzeigen des IP-Adressverlaufs mithilfe von AWS CLI

Die Szenarien in diesem Abschnitt zeigen Ihnen, wie Sie die Prüfung von IP-Adressen mithilfe von AWS CLI. Allgemeine Informationen zur Verwendung von AWS CLI finden Sie unter Verwenden von AWS CLI im Benutzerhandbuch für die AWS-Befehlszeilenschnittstelle.

Inhalt

Übersicht

IPAM speichert Ihre Daten zur Überwachung der IP-Adresse automatisch für bis zu drei Jahre. Sie können die Verlaufsdaten verwenden, um Ihre Netzwerksicherheits- und Routing-Richtlinien zu analysieren und zu überprüfen. Sie können nach Verlaufserkenntnissen für die folgenden Ressourcentypen suchen:

- VPCs
- VPC-Subnetze
- Elastic-IP-Adressen
- EC2-Instances, die ausgeführt werden
- An Instances angefügte EC2-Netzwerkschnittstellen

Important

Obwohl IPAM keine Amazon-EC2-Instances oder an Instances angefügte EC2-Netzwerkschnittstellen überwacht, können Sie die Funktion Suche IP-Verläufe verwenden, um nach Verlaufsdaten zu EC2-Instance- und Netzwerkschnittstellen-CIDRs zu suchen.

Note

- Die Befehle in diesem Tutorial müssen mit dem Konto ausgeführt werden, dem das IPAM gehört, und der AWS-Region, die das IPAM hostet.
- Aufzeichnungen über Änderungen an CIDRs werden in regelmäßigen Snapshots erfasst, was bedeutet, dass es einige Zeit dauern kann, bis Aufzeichnungen angezeigt oder aktualisiert werden, und die Werte für SampledStartTime und SampledEndTime können von den tatsächlichen Zeiten abweichen, zu denen sie aufgetreten sind.

Szenarien

Die Szenarien in diesem Abschnitt zeigen Ihnen, wie Sie die Verwendung von IP-Adressen mithilfe von AWS CLI. Weitere Informationen zu den in diesem Tutorial erwähnten Werten wie z. B. Endzeit und Startzeit der Stichprobe finden Sie unter Verlauf der IP-Adresse anzeigen.

Szenario 1: Welche Ressourcen wurden am 27. Dezember 2021 (UTC) zwischen 1:00 Uhr und 21:00 Uhr mit **`10.2.1.155/32`** verknüpft?

1. Führen Sie den Befehl aus:

```
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. Sehen Sie sich die Ergebnisse der Analyse an. Im folgenden Beispiel wurde das CIDR im Laufe des Zeitraums einer Netzwerkschnittstelle und einer EC2-Instance zugewiesen. Beachten Sie, dass kein SampledEndTime-Wert bedeutet, dass die Akte noch aktiv ist. Weitere Informationen über die in der folgenden Ausgabe gezeigten Werten finden Sie unter Verlauf der IP-Adresse anzeigen.

```
{
    "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"
        }
    ]
```

```
}
```

Wenn die Besitzer-ID der Instance an die eine Netzwerkschnittstelle angehängt ist, von der Besitzer-ID der Netzwerkschnittstelle abweicht (wie es bei NAT-Gateways, Lambda-Netzwerkschnittstellen in VPCs und anderen AWS-Diensten der Fall ist), ist `ResourceOwnerId` eher `amazon-aws` als die Konto-ID des Besitzers der Netzwerkschnittstelle. Das folgende Beispiel zeigt die Akte für ein CIDR, das einem NAT-Gateway zugeordnet ist:

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

Szenario 2: Welche Ressourcen waren vom 1. Dezember 2021 bis zum 27. Dezember 2021 (UTC) mit **`10.2.1.0/24`** verbunden?

1. Führen Sie den Befehl aus:

```
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. Sehen Sie sich die Ergebnisse der Analyse an. Im folgenden Beispiel wurde das CIDR im Laufe des Zeitraums einem Subnetz und einer VPC zugewiesen. Beachten Sie, dass kein SampledEndTime-Wert bedeutet, dass der Datensatz noch aktiv ist. Weitere Informationen über die in der folgenden Ausgabe gezeigten Werten finden Sie unter Verlauf der IP-Adresse anzeigen.

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

Szenario 3: Welche Ressourcen waren vom 1. Dezember 2021 bis zum 27. Dezember 2021 (UTC) mit **2605:9cc0:409::/56** verbunden?

1. Führen Sie den folgenden Befehl aus, wobei --region die IPAM-Heimregion ist:

```
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. Sehen Sie sich die Ergebnisse der Analyse an. Im folgenden Beispiel wurde das CIDR im Laufe des Zeitraums zwei verschiedenen VPCs in einer Region außerhalb der IPAM-Heimatregion zugewiesen. Beachten Sie, dass kein SampledEndTime-Wert bedeutet, dass der Datensatz noch aktiv ist. Weitere Informationen über die in der folgenden Ausgabe gezeigten Werten finden Sie unter Verlauf der IP-Adresse anzeigen.


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


Szenario 4: Welche Ressourcen wurden in den letzten 24 Stunden (angenommen, die aktuelle Uhrzeit ist Mitternacht am 27. Dezember 2021 (UTC)) mit **`10.0.0.0/24`** verknüpft?

1. Führen Sie den Befehl aus:

```
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. Sehen Sie sich die Ergebnisse der Analyse an. Im folgenden Beispiel wurde das CIDR im Laufe des Zeitraums zahlreichen Subnetzen und VPCs zugewiesen. Beachten Sie, dass kein SampledEndTime-Wert bedeutet, dass der Datensatz noch aktiv ist. Weitere Informationen über die in der folgenden Ausgabe gezeigten Werten finden Sie unter Verlauf der IP-Adresse anzeigen.


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

Szenario 5: Welche Ressourcen sind derzeit mit **`10.2.1.155/32`** verbunden?

1. Führen Sie den Befehl aus:

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

2. Sehen Sie sich die Ergebnisse der Analyse an. Im folgenden Beispiel wurde das CIDR über den Zeitraum einer Netzwerkschnittstelle und einer EC2-Instance zugewiesen. Beachten Sie, dass kein SampledEndTime-Wert bedeutet, dass der Datensatz noch aktiv ist. Weitere Informationen über die in der folgenden Ausgabe gezeigten Werten finden Sie unter Verlauf der IP-Adresse anzeigen.

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

Szenario 6: Welche Ressourcen sind derzeit mit **`10.2.1.0/24`** verbunden?

1. Führen Sie den Befehl aus:

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

2. Sehen Sie sich die Ergebnisse der Analyse an. Im folgenden Beispiel wurde das CIDR über den Zeitraum einer VPC und einem Subnetz zugewiesen. Nur die Ergebnisse, die genau diesem `/24` CIDR entsprechen, werden zurückgegeben, nicht alle `/32` innerhalb des `/24`-CIDR. Beachten Sie, dass kein SampledEndTime-Wert bedeutet, dass der Datensatz noch aktiv ist. Weitere Informationen über die in der folgenden Ausgabe gezeigten Werten finden Sie unter Verlauf der IP-Adresse anzeigen.

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

Szenario 7: Welche Ressourcen sind derzeit mit **`54.0.0.9/32`** verbunden?

In diesem Beispiel wird `54.0.0.9/32` einer elastischen IP-Adresse zugewiesen, die nicht Teil der in Ihr IPAM integrierten AWS-Organisation ist.

1. Führen Sie den Befehl aus:

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

2. Da `54.0.0.9/32` einer elastischen IP-Adresse zugewiesen ist, die nicht Teil der AWS-Organisation ist, die in diesem Beispiel mit IPAM integriert ist, werden keine Datensätze zurückgegeben.

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

Tutorial: Einbinden Ihrer ASN in IPAM

Wenn Ihre Anwendungen vertrauenswürdige IP-Adressen und autonome Systemnummern (ASNs) verwenden, die Ihre Partner oder Kunden in ihrem Netzwerk zugelassen haben, können Sie diese Anwendungen ausführen, AWS ohne dass Ihre Partner oder Kunden ihre Zulassungslisten ändern müssen.

Eine autonome Systemnummer (ASN) ist eine weltweit eindeutige Nummer, die es ermöglicht, eine Gruppe von Netzwerken über das Internet zu identifizieren und mithilfe des Border Gateway Protocol Routing-Daten dynamisch mit anderen Netzwerken auszutauschen. Internetdienstanbieter (ISPs)

verwenden beispielsweise ASNs, um die Quelle des Netzwerkdatenverkehrs zu identifizieren. Nicht alle Organisationen kaufen ihre eigenen ASNs, aber Organisationen, die dies tun, können ihre ASN an andere weitergeben. AWS

Mit BYOASN (Bring Your Own Autonomous System Number) können Sie die IP-Adressen, an die Sie weiterleiten, AWS mit Ihrer eigenen öffentlichen ASN statt mit der ASN bewerben. AWS Wenn Sie BYOASN verwenden, überträgt der von Ihrer IP-Adresse ausgehende Datenverkehr Ihre ASN anstelle der ASN, und Ihre Workloads sind für Kunden oder Partner erreichbar, die den aufgelisteten Datenverkehr auf der Grundlage Ihrer IP-Adresse und AWS ASN zugelassen haben.

⚠ Important

- Schließen Sie dieses Tutorial mit dem IPAM-Administratorkonto in der Heimatregion Ihres IPAM ab.
- In diesem Tutorial wird davon ausgegangen, dass Sie Eigentümer der öffentlichen ASN sind, die Sie auf IPAM übertragen möchten, und dass Sie bereits eine BYOIP-CIDR installiert und für einen Pool in Ihrem öffentlichen Bereich bereitgestellt haben. AWS Sie können jederzeit eine ASN auf IPAM übertragen, aber um sie verwenden zu können, müssen Sie sie mit einer CIDR verknüpfen, die Sie Ihrem Konto hinzugefügt haben. AWS In diesem Tutorial wird davon ausgegangen, dass Sie dies bereits gemacht haben. Weitere Informationen finden Sie unter Tutorial: Mitbringen eigener IP-Adressen in IPAM.
- Sie können ohne Verzögerung zwischen Ihrer eigenen ASN und einer AWS ASN wechseln, sind jedoch darauf beschränkt, einmal pro Stunde von einer AWS ASN zu Ihrer eigenen ASN zu wechseln.
- Wenn Ihr BYOIP-CIDR derzeit beworben wird, müssen Sie ihn nicht aus der Werbung entfernen, um ihn mit Ihrer ASN zu verknüpfen.

Onboarding-Voraussetzungen für Ihre ASN

Für dieses Tutorial benötigen Sie Folgendes:

- Ihre öffentliche 2-Byte- oder 4-Byte-ASN.
- Wenn Sie bereits einen IP-Adressbereich mitgebracht habenTutorial: Mitbringen eigener IP-Adressen in IPAM, benötigen Sie den AWS CIDR-Bereich für IP-Adressen. Sie benötigen außerdem einen privaten Schlüssel. Sie können den privaten Schlüssel verwenden, den Sie erstellt haben, als Sie den IP-Adress-CIDR-Bereich hinzugefügt haben, AWS oder Sie können einen

neuen privaten Schlüssel erstellen, wie unter Erstellen eines privaten Schlüssels und Generieren eines X.509-Zertifikats im EC2-Benutzerhandbuch beschrieben.

- Wenn Sie einen IP-Adressbereich hinzufügenTutorial: Mitbringen eigener IP-Adressen in IPAM, erstellen Sie ein X.509-Zertifikat und laden das X.509-Zertifikat in den RDAP-Eintrag in Ihrem RIR hoch. AWS Sie müssen das gleiche Zertifikat, das Sie erstellt haben, in den RDAP-Eintrag in Ihrem RIR für die ASN hochladen. Achten Sie darauf, dass die `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----`-Zeichenfolgen vor und nach dem kodierten Teil enthalten sind. Der gesamte Inhalt muss sich in einer einzigen, langen Zeile befinden. Das Verfahren zum Aktualisieren des RDAP hängt von Ihrem RIR ab:
  - Verwenden Sie für ARIN das Accountmanager-Portal, um das Zertifikat im Abschnitt „Öffentliche Kommentare“ für das Objekt „Netzwerkinformationen“ hinzuzufügen, das Ihre ASN darstellt, indem Sie die Option „ASN ändern“ verwenden. Fügen Sie es nicht dem Kommentarbereich Ihrer Organisation hinzu.
  - Für RIPE fügen Sie das Zertifikat als neues Feld „descr“ zum Objekt „aut-num“ hinzu, das Ihre ASN darstellt. Diese finden Sie normalerweise im Bereich „Meine Ressourcen“ des

    RIPE-Datenbankportals. Fügen Sie sie nicht in den Kommentarbereich für Ihre Organisation oder in das Feld „Anmerkungen“ des Objekts „aut-num“ ein.
  - Senden Sie für APNIC das Zertifikat per E-Mail an helpdesk@apnic.net, um es manuell in das Feld „Anmerkungen“ für Ihre ASN aufzunehmen. Senden Sie die E-Mail über den autorisierten APNIC-Kontakt für die ASN.

Schritte des Tutorials

Führen Sie die folgenden Schritte mit der Konsole oder dem aus AWS . AWS CLI

AWS Management Console

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im linken Navigationsbereich die Option IPAMs.
3. Wählen Sie Ihren IPAM.
4. Wählen Sie die Registerkarte BYOASNS und dann BYOASNs bereitstellen.
5. Geben Sie die ASN ein. Infolgedessen wird das Nachrichtenfeld automatisch mit der Nachricht gefüllt, die Sie im nächsten Schritt signieren müssen.

- Die Nachricht hat das folgende Format: ACCOUNT ist Ihre AWS Kontonummer, ASN ist die ASN, die Sie an IPAM senden, und YYYYMMDD ist das Ablaufdatum der Nachricht (standardmäßig der letzte Tag des nächsten Monats). Beispiel:

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

6. Kopieren Sie die Nachricht und ersetzen Sie das Ablaufdatum ggf. durch Ihren eigenen Wert.
7. Signieren Sie die Nachricht mit dem privaten Schlüssel. Beispiel:

```
signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
 rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform
 PEM | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
```

8. Geben Sie unter Signatur die Signatur ein.
9. (Optional) Um eine weitere ASN bereitzustellen, wählen Sie Weitere ASN bereitstellen aus. Sie können bis zu 5 ASNs bereitstellen. Informationen zur Erhöhung dieses Kontingents finden Sie unter Kontingente für Ihr IPAM.
10. Wählen Sie Bereitstellung.
11. Sehen Sie sich den Bereitstellungsprozess auf der Registerkarte BYOASNs an. Warten Sie, bis der Status von Pending-provision zu Provisioned wechselt. BYOASNs mit dem Status Failed-provision werden nach 7 Tagen automatisch entfernt. Sobald die ASN erfolgreich bereitgestellt wurde, können Sie sie einem BYOIP-CIDR zuordnen.
12. Wählen Sie im linken Navigationsbereich Pools aus.
13. Wählen Sie Ihren öffentlichen Bereich. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
14. Wählen Sie einen regionalen Pool, für den ein BYOIP-CIDR bereitgestellt wurde. Für den Pool muss Service auf EC2 eingestellt sein und es muss ein Gebietsschema ausgewählt sein.
15. Wählen Sie die Registerkarte CIDRs und wählen Sie einen BYOIP-CIDR aus.
16. Wählen Sie Aktionen > BYOASN-Zuweisungen verwalten.
17. Wählen Sie unter Zugeordnet durch OASNs die ASN aus, zu der Sie weitergeleitet haben. AWS Wenn Sie mehrere ASNs haben, können Sie dem BYOIP-CIDR mehrere ASNs zuweisen. Sie können so viele ASNs zuweisen, wie Sie in IPAM einbinden können. Beachten Sie, dass Sie standardmäßig bis zu 5 ASNs in IPAM einbinden können. Weitere Informationen finden Sie unter Kontingente für Ihr IPAM.

18. Wählen Sie Associate aus.
19. Warten Sie, bis der ASN-Zuweisung abgeschlossen ist. Sobald die ASN erfolgreich mit dem BYOIP-CIDR verknüpft wurde, können Sie den BYOIP-CIDR erneut bewerben.
20. Wählen Sie die Registerkarte Pool-CIDRs.
21. Wählen Sie das BYOIP CIDR und Aktionen > Werben aus. Daraufhin werden Ihre ASN-Optionen angezeigt: die Amazon-ASN und alle ASNs, die Sie in IPAM eingebunden haben.
22. Wählen Sie die ASN aus, die Sie in IPAM eingebunden haben, und wählen Sie Werben Sie für CIDR. Als Ergebnis wird der BYOIP CIDR beworben und der Wert in der Spalte Werbung ändert sich von „Zurückgezogen“ auf „Beworben“. In der Spalte Autonome Systemnummer wird die dem CIDR zugeordnete ASN angezeigt.
23. (optional) Wenn Sie entscheiden, dass Sie die ASN-Zuweisung wieder zur Amazon-ASN ändern möchten, wählen Sie den BYOIP CIDR aus und wählen Sie erneut Aktionen > Werben. Wählen Sie dieses Mal die Amazon-ASN aus. Sie können jederzeit zur Amazon-ASN zurückkehren, aber Sie können nur einmal pro Stunde zu einer benutzerdefinierten ASN wechseln.

Das Tutorial ist abgeschlossen.

Bereinigen

1. Trennen der ASN vom BYOIP-CIDR
   - Um den BYOIP-CIDR aus der Werbung zurückzuziehen, wählen Sie in Ihrem Pool im öffentlichen Bereich den BYOIP-CIDR aus und wählen Sie Aktionen > Von der Werbung zurückziehen.
   - Um die ASN vom CIDR zu trennen, wählen Sie Aktionen > BYOASN-Zuweisungen verwalten.
2. Aufheben der Bereitstellung der ASN
   - Um die Bereitstellung der ASN aufzuheben, wählen Sie auf der Registerkarte „BYOASNs“ die ASN und anschließend die Option Bereitstellung der ASN aufheben. Infolgedessen wird die Bereitstellung der ASN aufgehoben. BYOASNs mit dem Status Deprovisioned werden nach 7 Tagen automatisch entfernt.

Die Bereinigung ist abgeschlossen.

Command line

1. Stellen Sie Ihre ASN bereit, indem Sie Ihre ASN und Ihre Autorisierungsnachricht angeben. Die Signatur ist die Nachricht, die mit Ihrem privaten Schlüssel signiert wurde.

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

2. Beschreiben Sie Ihre ASN, um den Bereitstellungsprozess nachzuverfolgen. Wenn die Anfrage erfolgreich ist, sollten Sie nach einigen Minuten sehen, dass sie auf bereitgestellt ProvisionStatusgesetzt ist.

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

3. Ordnen Sie Ihre ASN Ihrem BYOIP-CIDR zu. Jede benutzerdefinierte ASN, von der aus Sie Werbung schalten möchten, muss zunächst Ihrem CIDR zugewiesen werden.

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

4. Beschreiben Sie Ihren CIDR, um den Zuweisungsprozess nachzuverfolgen.

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

5. Werben Sie mit Ihrer ASN für Ihren CIDR. Wenn der CIDR bereits beworben wurde, wird dadurch die ursprüngliche ASN von Amazon auf Ihre übertragen.

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

6. Beschreiben Sie Ihren CIDR, um zu sehen, wie sich der ASN-Status von associated in advertised ändert.

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

Das Tutorial ist abgeschlossen.

Bereinigen

1. Führen Sie eine der folgenden Aktionen aus:

- Um nur Ihre ASN-Werbung zurückzuziehen und wieder die Amazon-ASNs zu verwenden und gleichzeitig die angekündigte CIDR beizubehalten, müssen Sie advertise-byoip-cidr mit dem speziellen AWS Wert für den ASN-Parameter aufrufen. Sie können jederzeit zur Amazon-ASN zurückkehren, aber Sie können nur einmal pro Stunde zu einer benutzerdefinierten ASN wechseln.

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

- Um Ihre CIDR- und ASN-Werbung gleichzeitig zurückzuziehen, können Sie anrufen. withdraw-byoip-cidr

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

2. Um Ihre ASN zu bereinigen, müssen Sie sie zunächst von Ihrem BYOIP-CIDR trennen.

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

3. Sobald Ihre ASN von allen BYOIP-CIDRs, denen Sie sie zugewiesen haben, getrennt wurde, können Sie die Bereitstellung aufheben.

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

4. Die Bereitstellung des BYOIP-CIDR kann auch aufgehoben werden, sobald alle ASN-Zuweisungen entfernt wurden.

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

5. Bestätigen Sie das Aufheben der Bereitstellung.

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

Die Bereinigung ist abgeschlossen.

Tutorial: Mitbringen eigener IP-Adressen in IPAM

Die Tutorials in diesem Abschnitt führen Sie durch den Prozess, öffentlichen IP-Adressraum in IPAM zu integrieren AWS und ihn zu verwalten.

Die Verwaltung des öffentlichen IP-Adressraums mit IPAM hat folgende Vorteile:

- Verbessert die Auslastung öffentlicher IP-Adressen in Ihrer Organisation: Sie können IPAM verwenden, um den IP-Adressraum über AWS -Konten freizugeben. Ohne IPAM zu verwenden, können Sie Ihren öffentlichen IP-Bereich nicht über AWS -Konten von Organizations freigeben.
- Vereinfacht den Prozess der Bereitstellung von öffentlichem IP-Raum für AWS: Sie können IPAM verwenden, um den öffentlichen IP-Adressraum einmal zu integrieren, und dann IPAM verwenden, um Ihre öffentlichen IPs über Regionen zu verteilen. Ohne IPAM müssen Sie Ihre öffentlichen IPs für jede Region einbinden. AWS

⚠ Important

- Bevor Sie mit diesem Tutorial beginnen, führen Sie die Schritte unter Onboarding-Voraussetzungen für Ihren BYOIP-Adressbereich im Amazon EC2 EC2-Benutzerhandbuch durch.

  Wenn Sie die ROAs erstellen, müssen Sie für IPv4-CIDRs die maximale Länge eines IP-Adresspräfixes auf `/24` festlegen. Wenn Sie IPv6-CIDRs zu einem werbefähigen Pool hinzufügen, darf die maximale Länge eines IP-Adresspräfixes `/48` sein. Dadurch wird gewährleistet, dass Sie die volle Flexibilität haben, Ihre öffentliche IP-Adresse auf verschiedene Regionen aufzuteilen. AWS IPAM erzwingt die von Ihnen festgelegte maximale Länge. Die maximale Länge ist die kleinste Ankündigung der Präfixlänge, die Sie für diese Route zulassen werden. Wenn Sie zum Beispiel einen `/20`-CIDR-Block auf AWS bringen, indem Sie die maximale Länge auf `/24` setzen, können Sie den größeren Block beliebig teilen (z. B. mit `/21`, `/22` oder `/24`) und diese kleineren CIDR-Blöcke auf eine beliebige Region verteilen. Wenn Sie die maximale Länge auf `/23` festlegen würden, könnten Sie kein `/24` aus dem größeren Block teilen und bewerben. Beachten Sie außerdem, dass `/24` der kleinste IPv4-Block und `/48` der kleinste IPv6-Block ist, den Sie von einer Region im Internet ankündigen können.

- Sobald Sie einen IPv4-Adressbereich AWS eingerichtet haben, können Sie alle IP-Adressen in diesem Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Inhalt

Bringen Sie Ihr eigenes öffentliches IPv4-CIDR mit der AWS Management Console und der CLI auf IPAM AWS

Gehen Sie wie folgt vor, um ein IPv4- oder IPv6-CIDR sowohl mit der AWS Management Console als auch mit der CLI auf IPAM zu übertragen. AWS

⚠ Important

- Bevor Sie mit diesem Tutorial beginnen, führen Sie die Schritte unter Onboarding-Voraussetzungen für Ihren BYOIP-Adressbereich im Amazon EC2 EC2-Benutzerhandbuch durch.

  Wenn Sie die ROAs erstellen, müssen Sie für IPv4-CIDRs die maximale Länge eines IP-Adresspräfixes auf `/24` festlegen. Wenn Sie IPv6-CIDRs zu einem werbefähigen Pool hinzufügen, darf die maximale Länge eines IP-Adresspräfixes `/48` sein. Dadurch wird gewährleistet, dass Sie die volle Flexibilität haben, Ihre öffentliche IP-Adresse auf verschiedene Regionen aufzuteilen. AWS IPAM erzwingt die von Ihnen festgelegte maximale Länge. Die maximale Länge ist die kleinste Ankündigung der Präfixlänge, die Sie für diese Route zulassen werden. Wenn Sie zum Beispiel einen `/20`-CIDR-Block auf AWS bringen, indem Sie die maximale Länge auf `/24` setzen, können Sie den größeren Block beliebig teilen (z. B. mit `/21`, `/22` oder `/24`) und diese kleineren CIDR-Blöcke auf eine beliebige Region verteilen. Wenn Sie die maximale Länge auf `/23` festlegen würden, könnten Sie kein `/24` aus dem größeren Block teilen und bewerben. Beachten Sie außerdem, dass `/24` der kleinste IPv4-Block und `/48` der kleinste IPv6-Block ist, den Sie von einer Region im Internet ankündigen können.

- Sobald Sie einen IPv4-Adressbereich AWS eingerichtet haben, können Sie alle IP-Adressen in diesem Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Inhalt

Bringen Sie Ihr eigenes IPv4-CIDR mit der AWS Management Console und der CLI auf IPAM AWS

Gehen Sie wie folgt vor, um ein IPv4-CIDR auf IPAM zu übertragen und eine Elastic IP-Adresse (EIP) sowohl über die AWS Management Console als auch über die CLI zuzuweisen. AWS

Important

- Sie können derzeit keine BYOIP-Adressbereiche in Local Zones bereitstellen oder bewerben.
- In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
  - Integrieren von IPAM mit Konten in einer - AWS Organisation.
  - Erstellen eines IPAM.
- Jeder Schritt dieses Tutorials muss von einem der drei Unternehmenskonten AWS Organizations werden:
  - Das Verwaltungskonto.
  - Das als Ihr IPAM-Administrator konfigurierte Mitgliedskonto in Integrieren von IPAM mit Konten in einer - AWS Organisation. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zuweist. In diesem Tutorial wird dieses Konto als Mitgliedskonto bezeichnet.

Inhalt

Schritt 1: Erstellen Sie AWS CLI benannte Profile und IAM-Rollen

Um dieses Tutorial als AWS Einzelbenutzer abzuschließen, können Sie AWS CLI benannte Profile verwenden, um von einer IAM-Rolle zu einer anderen zu wechseln. Benannte Profile sind Sammlungen von Einstellungen und Anmeldeinformationen, auf die Sie verweisen, wenn Sie die Option `--profile` mit der AWS CLI verwenden. Weitere Informationen zum Erstellen von IAM-Rollen und benannten Profilen für AWS Konten finden Sie unter Verwenden einer IAM-Rolle in der AWS CLI im AWS Identity and Access Management-Benutzerhandbuch.

Erstellen Sie eine Rolle und ein benanntes Profil für jedes der drei AWS Konten, die Sie in diesem Tutorial verwenden werden:

- Ein Profil, das `management-account` für das Verwaltungskonto der AWS Organizations aufgerufen wurde.
- Ein Profil, das `ipam-account` für das Mitgliedskonto der AWS Organizations aufgerufen wird und als Ihr IPAM-Administrator konfiguriert ist.
- Ein Profil, das `member-account` für das Mitgliedskonto der AWS Organizations in Ihrer Organisation aufgerufen wird und CIDRs aus einem IPAM-Pool zuweist.

Nachdem Sie die IAM-Rollen und benannten Profile erstellt haben, kehren Sie zu dieser Seite zurück und fahren Sie mit dem nächsten Schritt fort. Im weiteren Verlauf dieses Tutorials werden Sie feststellen, dass die AWS CLI Beispielbefehle die `--profile` Option mit einem der genannten Profile verwenden, um anzugeben, welches Konto den Befehl ausführen muss.

Schritt 2: Erstellen Sie einen IPAM-Pool der obersten Ebene

Führen Sie die Schritte in diesem Abschnitt durch, um einen IPAM-Pool der obersten Ebene zu erstellen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

So erstellen Sie einen Pool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wählen Sie den Bereich Öffentlich. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie Pool erstellen.
5. (Optional) Fügen Sie ein Namens-Tag für den Pool und eine Beschreibung für den Pool hinzu.
6. Wählen Sie unter Quelle die Option IPAM-Bereich aus.
7. Wählen Sie unter Adressfamilie IPv4 aus.
8. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
9. Wählen Sie unter Gebietsschema die Option Keines aus.

   Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden.

   Die IPAM-Integration mit BYOIP setzt voraus, dass das Gebietsschema für den Pool festgelegt ist, der für das BYOIP CIDR verwendet wird. Da wir einen IPAM-Pool der obersten Ebene mit einem darin enthaltenen regionalen Pool erstellen und einer elastischen IP-Adresse aus dem regionalen Pool Speicherplatz zuweisen werden, legen Sie das Gebietsschema für den

regionalen Pool und nicht für den Pool der obersten Ebene fest. Sie fügen das Gebietsschema zum Regionalpool hinzu, wenn Sie den Regionalpool in einem späteren Schritt erstellen.

> **Note**
>
> Wenn Sie nur einen einzelnen Pool und keinen Pool auf der obersten Ebene mit regionalen Pools erstellen, möchten Sie ein Gebietsschema für diesen Pool auswählen, damit der Pool für Zuweisungen verfügbar ist.

10. Wählen Sie unter Öffentliche IP-Quelle eine der folgenden Optionen aus:

    - BYOIP: Sie bringen Ihren eigenen IPv4- oder IPv6-Adressbereich (BYOIP) in diesen Pool ein.
    - Im Besitz von Amazon: Sie möchten, dass Amazon einen IPv6-Adressbereich für diesen Pool bereitstellt.

11. Führen Sie eine der folgenden Aktionen aus:

    - Wenn Sie im vorherigen Schritt BYOIP ausgewählt haben, wählen Sie unter CIDRs für die Bereitstellung ein CIDR aus, das für den Pool bereitgestellt werden soll. Beachten Sie, dass bei der Bereitstellung eines IPv4-CIDR für einen Pool innerhalb des Pools der obersten Ebene das minimale IPv4-CIDR, das Sie bereitstellen können, `/24` beträgt; spezifischere CIDRs (wie `/25`) sind nicht zulässig. Sie müssen das CIDR und die BYOIP-Nachricht und die Zertifikatssignatur in die Anfrage aufnehmen, damit wir überprüfen können, ob Sie den öffentlichen Raum besitzen. Eine Liste der BYOIP-Voraussetzungen, einschließlich Informationen zum Abrufen dieser BYOIP-Nachricht und der Zertifikatssignatur, finden Sie unter Bringen Sie Ihr eigenes öffentliches IPv4-CIDR mit der AWS Management Console und der CLI auf IPAM AWS.

      > **Important**
      >
      > Während die meisten Bereitstellungen innerhalb von zwei Stunden abgeschlossen sein werden, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich beworbene Bereiche abgeschlossen ist.

    - Wenn Sie sich für Eigentum von Amazon entschieden haben, wählen Sie unter Netzmaskenlänge eine Netzmaskenlänge von `/40` bis `/52` aus. Der Standardwert ist `/52`.

12. Lassen Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren deaktiviert.
13. (Optional) Wählen Sie Tags für den Pool.

14. Wählen Sie Pool erstellen.

Stellen Sie sicher, dass dieses CIDR bereitgestellt wurde, bevor Sie fortfahren. Sie können den Bereitstellungsstatus auf der Registerkarte CIDRs auf der Seite Pool-Details sehen.

Schritt 3. Erstellen Sie einen regionalen Pool im Pool der obersten Ebene

Erstellen Sie einen regionalen Pool im Pool der obersten Ebene. Die IPAM-Integration mit BYOIP setzt voraus, dass das Gebietsschema für den Pool festgelegt ist, der für das BYOIP CIDR verwendet wird. Sie fügen das Gebietsschema dem regionalen Pool hinzu, wenn Sie den regionalen Pool in diesem Abschnitt erstellen. Das `Locale` muss eine der Betriebsregionen sein, die Sie beim Erstellen des IPAM konfiguriert haben.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Erstellen eines regionalen Pools im Pool der obersten Ebene

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wenn Sie den privaten Standardbereich nicht verwenden möchten, wählen Sie im Dropdown-Menü oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie Pool erstellen.
5. (Optional) Fügen Sie ein Namens-Tag für den Pool und eine Beschreibung für den Pool hinzu.
6. Unter Quelle wählen Sie den Pool der obersten Ebene aus, den Sie im vorherigen Abschnitt erstellt haben.
7. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
8. Wählen Sie unter Gebietsschema das Gebietsschema für den Pool aus. In diesem Tutorial verwenden wir `us-east-2` als Gebietsschema für den regionalen Pool. Die verfügbaren Optionen stammen aus den Betriebsregionen, die Sie beim Erstellen Ihres IPAM ausgewählt haben.

Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden. Die Auswahl eines Gebietsschemas stellt sicher, dass es keine regionsübergreifenden Abhängigkeiten zwischen Ihrem Pool und den daraus zugewiesenen Ressourcen gibt.

9. Wählen Sie unter Dienst EC2 (EIP/VPC) aus. Der Dienst, den Sie auswählen, bestimmt den AWS Dienst, bei dem der CIDR beworben wird. Derzeit ist die einzige Option EC2 (EIP/VPC), was bedeutet, dass die aus diesem Pool zugewiesenen CIDRs für den Amazon-EC2-Service (für elastische IP-Adressen) und den Amazon-VPC-Service (für CIDRs, die mit VPCs verknüpft sind) beworben werden können.
10. Wählen Sie unter CIDRs für die Bereitstellung ein CIDR aus, das für den Pool bereitgestellt werden soll. Beachten Sie, dass bei der Bereitstellung eines CIDR für einen Pool innerhalb des Pools der obersten Ebene das minimale IPv4-CIDR, das Sie bereitstellen können, beträgt `/24`; spezifischere CIDRs (wie `/25`) sind nicht zulässig. Nachdem Sie den ersten regionalen Pool erstellt haben, können Sie kleinere Pools (z. B.`/25`) innerhalb des regionalen Pools erstellen.
11. Aktivieren Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren. Sie haben hier dieselben Zuweisungsregeloptionen wie beim Erstellen des Pools der obersten Ebene. Für eine Erläuterung der Optionen, die beim Erstellen von Pools verfügbar sind, siehe Erstellen eines IPv4-Pools der obersten Ebene. Die Zuordnungsregeln für den Regionalpool werden nicht vom Pool der obersten Ebene geerbt. Wenn Sie hier keine Regeln anwenden, werden keine Zuteilungsregeln für den Pool festgelegt.
12. (Optional) Wählen Sie Tags für den Pool.
13. Wenn Sie mit der Konfiguration Ihres Pools fertig sind, wählen Sie Create pool (Pool erstellen) aus.

Stellen Sie sicher, dass dieses CIDR bereitgestellt wurde, bevor Sie fortfahren. Sie können den Bereitstellungsstatus auf der Registerkarte CIDRs auf der Seite Pool-Details sehen.

Schritt 4. Regionalen Pool teilen

Folgen Sie den Schritten in diesem Abschnitt, um den IPAM-Pool mithilfe von AWS Resource Access Manager (RAM) gemeinsam zu nutzen.

Aktivieren der Ressourcenfreigabe in AWS RAM

Nachdem Sie Ihren IPAM erstellt haben, sollten Sie den regionalen Pool mit anderen Konten in Ihrer Organisation teilen. Bevor Sie einen IPAM-Pool gemeinsam nutzen, führen Sie die Schritte in diesem Abschnitt aus, um die gemeinsame Nutzung von Ressourcen mit zu aktivieren. AWS RAM Wenn Sie das verwenden, AWS CLI um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`management-account`** Option.

So aktivieren Sie die Ressourcenfreigabe

1. Öffnen Sie mit dem AWS Organizations Verwaltungskonto die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie im linken Navigationsbereich Einstellungen, dann Teilen mit AWS Organizations aktivieren und anschließend Einstellungen speichern aus.

Nun können Sie einen IPAM-Pool für andere Mitglieder der Organisation freigeben.

Teilen Sie einen IPAM-Pool mit AWS RAM

In diesem Abschnitt teilen Sie den regionalen Pool mit einem anderen AWS Organizations Mitgliedskonto. Vollständige Anweisungen zur Freigabe von IPAM-Pools, einschließlich Informationen zu den erforderlichen IAM-Berechtigungen, finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM. Wenn Sie das verwenden AWS CLI , um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`ipam-account`** Option.

Um einen IPAM-Pool gemeinsam zu nutzen, verwenden Sie AWS RAM

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich, wählen Sie den IPAM-Pool aus und wählen Sie Aktionen > Details anzeigen aus.

4. Unter Resource sharing (Ressourcenfreigabe), wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus. Die AWS RAM Konsole wird geöffnet. Sie teilen sich den Pool mit AWS RAM.
5. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.
6. Wählen Sie in der AWS RAM Konsole erneut Create a resource share aus.
7. Fügen Sie einen Namen für den freigegebenen Pool hinzu.
8. Wählen Sie unter Ressourcentyp auswählen die Option IPAM-Pools und dann den ARN des Pools aus, den Sie teilen möchten.
9. Wählen Sie Weiter aus.
10. Wählen Sie die AWSRAMPermissionIpamPoolByoipCidrImportBerechtigung aus. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mit AWS RAM können Sie jedoch mehr über diese Optionen erfahren.
11. Wählen Sie Weiter aus.
12. Wählen Sie unter Prinzipale > Prinzipaltyp auswählen die Option AWS -Konto und geben Sie die Konto-ID des Kontos ein, das IPAM einen IP-Adressbereich hinzufügen soll, und wählen Sie Hinzufügen.
13. Wählen Sie Weiter aus.
14. Überprüfen Sie die Optionen für die Ressourcenfreigabe und die Prinzipale, für die die Freigabe erfolgt. Wählen Sie dann Erstellen aus.
15. Damit das **`member-account`**-Konto IP-Adressen-CIDRS aus dem IPAM-Pool zuweisen kann, erstellen Sie eine zweite Ressourcenfreigabe mit `AWSRAMDefaultPermissionsIpamPool`. Der Wert für `--resource-arns` ist der ARN des IPAM-Pools, den Sie im vorherigen Abschnitt erstellt haben. Der Wert für `--principals` ist die Konto-ID von**`member-account`**. Der Wert für `--permission-arns` ist der ARN der `AWSRAMDefaultPermissionsIpamPool`-Berechtigung.

Schritt 5: Erstellen eines öffentlichen IPv4-Pools

Das Erstellen eines öffentlichen IPv4-Pools ist ein notwendiger Schritt, damit eine öffentliche IPv4-Adresse auf AWS mit IPAM verwaltet wird. Dieser Schritt sollte von dem Mitgliedskonto durchgeführt werden, das eine elastische IP-Adresse bereitstellt.

Important

- Dieser Schritt muss vom Mitgliedskonto mit der AWS CLI durchgeführt werden.
- Öffentliche IPv4-Pools und IPAM-Pools werden von unterschiedlichen Ressourcen in verwaltet. AWSÖffentliche IPv4-Pools sind Einzelkonto-Ressourcen, mit denen Sie Ihre öffentlichen CIDRs in elastische IP-Adressen konvertieren können. IPAM-Pools können verwendet werden, um Ihren öffentlichen Raum öffentlichen IPv4-Pools zuzuweisen.

Um einen öffentlichen IPv4-Pool mit dem zu erstellen AWS CLI

- Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `Locale`-Option entsprechen, die Sie gewählt haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird.

  ```
  aws ec2 create-public-ipv4-pool --region us-east-2 --profile member-account
  ```

  In der Ausgabe sehen Sie die öffentliche IPv4-Pool-ID. Sie benötigen diese ID im nächsten Schritt.

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

Schritt 6: Bereitstellen eines öffentlichen IPv4-CIDR für Ihren öffentlichen IPv4-Pool

Stellen Sie das öffentliche IPv4-CIDR für Ihren öffentlichen IPv4-Pool bereit. Der Wert für `--region` muss mit dem Wert `Locale` übereinstimmen, den Sie beim Erstellen des Pools ausgewählt haben, der für das BYOIP CIDR verwendet wird. Der `--netmask-length` ist die Menge an Speicherplatz aus dem IPAM-Pool, den Sie in Ihren öffentlichen Pool bringen möchten. Der Wert darf nicht größer als die Netzmaskenlänge des IPAM-Pools sein. Das spezifischste IPv4-Präfix, das Sie aufnehmen können, ist `/24`.

Note

Wenn Sie einen `/24`-CIDR-Bereich für IPAM bereitstellen, um ihn in einer AWS -Organisation gemeinsam zu nutzen, können Sie kleinere Präfixe für mehrere IPAM-Pools bereitstellen,

beispielsweise /27 (mit `-- netmask-length 27`), anstatt das gesamte /24-CIDR (unter Verwendung von `-- netmask-length 24`) bereitzustellen, wie in diesem Tutorial gezeigt.

Important

Dieser Schritt muss vom Mitgliedskonto mit der AWS CLI durchgeführt werden.

Um einen öffentlichen IPv4-Pool mit dem zu erstellen AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

```
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
```

   In der Ausgabe sehen Sie das bereitgestellte CIDR.

```
{
    "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. Führen Sie den folgenden Befehl aus, um das im öffentlichen IPv4-Pool bereitgestellte CIDR anzuzeigen.

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --max-results 10 --
profile member-account
```

   In der Ausgabe sehen Sie das bereitgestellte CIDR. Standardmäßig wird das CIDR nicht beworben, was bedeutet, dass es über das Internet nicht öffentlich zugänglich ist. Sie haben die Möglichkeit, dieses CIDR im letzten Schritt dieses Tutorials als beworben zu setzen.

```
{
```

```
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 255
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 255,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

Öffnen Sie nach dem Erstellen des öffentlichen IPv4-Pools die IPAM-Konsole, um den im regionalen IPAM-Pool zugewiesenen öffentlichen IPv4-Pool anzuzeigen, und zeigen Sie die Zuweisung im regionalen Pool unter Zuweisungen oder Ressourcen an.

Schritt 7: Erstellen einer elastischen IP-Adresse aus dem öffentlichen IPv4-Pool

Führen Sie die Schritte unter Zuweisen einer Elastic IP-Adresse im Amazon EC2 EC2-Benutzerhandbuch aus, um eine Elastic IP-Adresse (EIP) aus dem öffentlichen IPv4-Pool zu erstellen. Wenn Sie EC2 in der AWS Management-Konsole öffnen, muss die AWS Region, der Sie die EIP zuweisen, der `Locale` Option entsprechen, die Sie bei der Erstellung des Pools ausgewählt haben, der für die BYOIP CIDR verwendet werden soll.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden. Wenn Sie die verwenden, verwenden Sie die Option. AWS CLI`--profile` **`member-account`**

Schritt 8: Verknüpfen Sie die elastische IP-Adresse mit einer EC2-Instance

Führen Sie die Schritte unter Zuordnen einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle im Amazon EC2 EC2-Benutzerhandbuch aus, um die EIP einer EC2-Instance zuzuordnen. Wenn Sie EC2 in der AWS Management-Konsole öffnen, muss die AWS Region, der Sie die EIP zuordnen, der `Locale` Option entsprechen, die Sie bei der Erstellung des Pools

ausgewählt haben, der für die BYOIP CIDR verwendet werden soll. In diesem Tutorial ist dieser Pool der regionale Pool.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden. Wenn Sie die verwenden, verwenden Sie die AWS CLI Option. `--profile` **`member-account`**

Schritt 9: Werben Sie für das CIDR

Die Schritte in diesem Abschnitt müssen vom IPAM-Konto ausgeführt werden. Sobald Sie die Elastic IP-Adresse (EIP) einer Instance oder einem Elastic Load Balancer zugeordnet haben, können Sie damit beginnen, den CIDR, zu dem Sie gebracht haben, zu bewerben, der sich in einem Pool befindet AWS , in dem der Service EC2 (EIP/VPC) konfiguriert ist. In diesem Tutorial ist das Ihr regionaler Pool. Standardmäßig wird das CIDR nicht beworben, was bedeutet, dass es über das Internet nicht öffentlich zugänglich ist.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Werbung für das CIDR

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wählen Sie den Bereich Öffentlich. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie den regionalen Pool aus, den Sie in diesem Tutorial erstellt haben.
5. Wählen Sie die Registerkarte CIDRs.
6. Wählen Sie das BYOIP CIDR und Aktionen > Werben aus.
7. Wählen Sie Für CIDR werben aus.

Als Ergebnis wird das BYOIP CIDR beworben und der Wert in der Spalte Werbung ändert sich von Zurückgezogen auf Beworben.

Schritt 10: Bereinigen

Führen Sie die Schritte in diesem Abschnitt aus, um die Ressourcen zu bereinigen, die Sie in diesem Tutorial bereitgestellt und erstellt haben.

Schritt 1: Das CIDR aus der Werbung zurückziehen

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wählen Sie den Bereich Öffentlich.
4. Wählen Sie den regionalen Pool aus, den Sie in diesem Tutorial erstellt haben.
5. Wählen Sie die Registerkarte CIDRs.
6. Wählen Sie das BYOIP CIDR aus und wählen Sie Aktionen > Werbung zurückziehen.
7. Wählen Sie CIDR zurückziehen aus.

Infolgedessen wird das BYOIP CIDR nicht mehr beworben und der Wert in der Spalte Werbung ändert sich von Beworben in Zurückgezogen.

Schritt 2: Trennen der Zuweisung der elastischen IP-Adresse

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden. Wenn Sie das verwenden, verwenden Sie die Option. AWS CLI`--profile` **`member-account`**

- Führen Sie die Schritte unter Trennen einer Elastic IP-Adresse im Amazon EC2 EC2-Benutzerhandbuch aus, um die EIP zu trennen. Wenn Sie EC2 in der AWS Management-Konsole öffnen, muss die AWS Region, in der Sie die EIP trennen, mit der `Locale` Option übereinstimmen, die Sie bei der Erstellung des Pools ausgewählt haben, der für den BYOIP-CIDR verwendet werden soll. In diesem Tutorial ist dieser Pool der regionale Pool.

Schritt 3: Geben Sie die elastische IP-Adresse frei

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden. Wenn Sie die verwenden, verwenden Sie die Option. AWS CLI`--profile` **`member-account`**

- Führen Sie die Schritte unter Elastic IP Address veröffentlichen im Amazon EC2 EC2-Benutzerhandbuch aus, um eine Elastic IP-Adresse (EIP) aus dem öffentlichen IPv4-Pool freizugeben. Wenn Sie EC2 in der AWS Management-Konsole öffnen, muss die AWS Region, der Sie die EIP zuweisen, mit der `Locale` Option übereinstimmen, die Sie bei der Erstellung des Pools ausgewählt haben, der für die BYOIP CIDR verwendet werden soll.

Schritt 4: Heben Sie die Bereitstellung des öffentlichen IPv4-CIDR aus Ihrem öffentlichen IPv4-Pool auf

> **Important**
>
> Dieser Schritt muss vom Mitgliedskonto mit der AWS CLI durchgeführt werden.

1. Zeigen Sie Ihre BYOIP CIDRs an.

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

   In der Ausgabe sehen Sie die IP-Adressen in Ihrem BYOIP CIDR.

```
{
    "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. Führen Sie den folgenden Befehl aus, um die letzte IP-Adresse im CIDR aus dem öffentlichen IPv4-Pool freizugeben. Geben Sie die IP-Adresse mit einer Netzmaske von `/32` ein.

```
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
```

In der Ausgabe sehen Sie die Aufhebung der Bereitstellung des CIDR.

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

> **Important**
>
> Sie müssen diesen Befehl für jede IP-Adresse im CIDR-Bereich erneut ausführen. Wenn Ihr CIDR ein `/24` ist, müssen Sie diesen Befehl ausführen, um die Bereitstellung jeder der 256 IP-Adressen im `/24`-CIDR aufzuheben.

3. Zeigen Sie Ihre BYOIP-CIDRs erneut an und stellen Sie sicher, dass keine bereitgestellten Adressen mehr vorhanden sind. Wenn Sie den Befehl in diesem Abschnitt ausführen, muss der Wert für `--region` mit der Region Ihres IPAMs übereinstimmen.

```
aws ec2 describe-public-ipv4-pools --region us-east-2 --profile member-account
```

In der Ausgabe sehen Sie die Anzahl der IP-Adressen in Ihrem öffentlichen IPv4-Pool.

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
```

```
}
```

> **Note**
>
> Es kann einige Zeit dauern, bis IPAM erkennt, dass Zuweisungen öffentlicher IPv4-Pools entfernt wurden. Sie können das IPAM-Pool-CIDR nicht weiter bereinigen und die Bereitstellung aufheben, bis Sie feststellen, dass die Zuweisung aus IPAM entfernt wurde.

Schritt 5: Löschen des öffentlichen IPv4-Pool

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

- Führen Sie den folgenden Befehl aus, um den öffentlichen IPv4-Pool CIDR zu löschen. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `Locale`-Option entsprechen, die Sie gewählt haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird. In diesem Tutorial ist dieser Pool der regionale Pool. Dieser Schritt muss mit der AWS CLI ausgeführt werden.

  ```
  aws ec2 delete-public-ipv4-pool --region us-east-2 --pool-id ipv4pool-
  ec2-09037ce61cf068f9a --profile member-account
  ```

  In der Ausgabe sehen Sie den Rückgabewert true.

  ```
  {
  "ReturnValue": true
  }
  ```

  Öffnen Sie nach dem Löschen des Pools die IPAM-Konsole, um die nicht von IPAM verwaltete Zuweisung anzuzeigen, und zeigen Sie die Details des regionalen Pools unter Zuweisungen an.

Schritt 6: Löschen der RAM-Freigaben und Deaktivieren der RAM-Integration mit AWS - Organizations

Dieser Schritt muss vom IPAM-Konto bzw. vom Verwaltungskonto ausgeführt werden. Wenn Sie die AWS CLI RAM-Shares löschen und die RAM-Integration deaktivieren möchten, verwenden Sie die `--profile` **`management-account`** Optionen `--profile` **`ipam-account`** und.

- Führen Sie die Schritte unter Löschen einer Ressourcenfreigabe im AWS RAM und Deaktivieren der gemeinsamen Nutzung von Ressourcen mit AWS Organizations im AWS RAM-Benutzerhandbuch in dieser Reihenfolge aus, um die RAM-Shares zu löschen und die RAM-Integration mit AWS Organizations zu deaktivieren.

Schritt 7: Heben Sie die Bereitstellung der CIDRs aus dem regionalen Pool und dem Pool der obersten Ebene auf

Dieser Schritt muss vom IPAM-Konto ausgeführt werden. Wenn Sie den AWS CLI zur gemeinsamen Nutzung des Pools verwenden, verwenden Sie die `--profile` **`ipam-account`** Option.

- Führen Sie die Schritte in Deprovisionierung von CIDRs aus einem Pool aus, um die Bereitstellung der CIDRs aus dem regionalen Pool und dann aus dem Pool der obersten Ebene in dieser Reihenfolge aufzuheben.

Schritt 8: Löschen Sie den regionalen Pool und den Pool der obersten Ebene

Dieser Schritt muss vom IPAM-Konto ausgeführt werden. Wenn Sie den AWS CLI zur gemeinsamen Nutzung des Pools verwenden, verwenden Sie die `--profile` **`ipam-account`** Option.

- Führen Sie die Schritte in Einen Pool löschen aus, um den regionalen Pool und dann den Pool der obersten Ebene in dieser Reihenfolge zu löschen.

Bringen Sie mithilfe der AWS -Managementkonsole Ihr eigenes IPv6-CIDR zu IPAM

Folgen Sie den Schritten in diesem Tutorial, um ein IPv6-CIDR auf IPAM zu übertragen und dem CIDR eine VPC zuzuweisen, indem Sie sowohl die Managementkonsole als auch die verwenden. AWS AWS CLI

Important

- Sie können derzeit keine BYOIP-Adressbereiche in Local Zones bereitstellen oder bewerben.
- In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
  - Integrieren von IPAM mit Konten in einer - AWS Organisation.
  - Erstellen eines IPAM.

- Jeder Schritt dieses Tutorials muss von einem der drei Unternehmenskonten AWS Organizations werden:
  - Das Verwaltungskonto.
  - Das als Ihr IPAM-Administrator konfigurierte Mitgliedskonto in Integrieren von IPAM mit Konten in einer - AWS Organisation. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zuweist. In diesem Tutorial wird dieses Konto als Mitgliedskonto bezeichnet.

Inhalt

Schritt 1: Erstellen Sie einen IPAM-Pool der obersten Ebene

Da Sie einen IPAM-Pool der obersten Ebene mit einem regionalen Pool erstellen und wir einer Ressource aus dem regionalen Pool Speicherplatz zuweisen werden, legen Sie das Gebietsschema für den regionalen Pool und nicht für den Pool der obersten Ebene fest. Sie fügen das Gebietsschema zum Regionalpool hinzu, wenn Sie den Regionalpool in einem späteren Schritt erstellen. Die IPAM-Integration mit BYOIP setzt voraus, dass das Gebietsschema für den Pool festgelegt ist, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

So erstellen Sie einen Pool

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.

3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wählen Sie den Bereich Öffentlich. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie Pool erstellen.
5. (Optional) Fügen Sie ein Namens-Tag für den Pool und eine Beschreibung für den Pool hinzu.
6. Wählen Sie unter Quelle die Option IPAM-Bereich aus.
7. Wählen Sie unter Adressfamilie IPv6 aus.

   Wenn Sie IPv6 wählen, wird eine Umschaltoption angezeigt, mit der Sie steuern können, ob die CIDRs in diesem Pool öffentlich bekannt AWS gegeben werden können. Lassen Sie diese Option aktiviert.
8. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
9. Stellen Sie sicher, dass Erlauben Sie CIDRs in diesem Pool öffentlich beworben zu werden ausgewählt ist.
10. Wählen Sie unter Gebietsschema die Option Keines aus. Sie legen das Gebietsschema im Regionalpool fest.

    Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden.

    > **Note**
    >
    > Wenn Sie nur einen einzelnen Pool und keinen Pool auf der obersten Ebene mit regionalen Pools erstellen, möchten Sie ein Gebietsschema für diesen Pool auswählen, damit der Pool für Zuweisungen verfügbar ist.
11. Unter Öffentliche IP-Quelle ist BYOIP standardmäßig ausgewählt.

12. Wählen Sie unter CIDRs für die Bereitstellung ein CIDR aus, das für den Pool bereitgestellt werden soll. Beachten Sie, dass bei der Bereitstellung eines IPv6-CIDRs für einen Pool innerhalb des Pools der obersten Ebene der spezifischste IPv6-Adressbereich, den Sie verwenden können, /48 für CIDRs, die öffentlich beworben werden können, und /60 für CIDRs, die nicht öffentlich beworben werden können, ist. Sie müssen das CIDR und die BYOIP-Nachricht und die Zertifikatssignatur in die Anfrage aufnehmen, damit wir überprüfen können, ob Sie den öffentlichen Raum besitzen. Eine Liste der BYOIP-Voraussetzungen, einschließlich Informationen zum Abrufen dieser BYOIP-Nachricht und der Zertifikatssignatur, finden Sie unter Bringen Sie Ihr eigenes öffentliches IPv4-CIDR mit der AWS Management Console und der CLI auf IPAM AWS.

    > **Important**
    >
    > Während die meisten Bereitstellungen innerhalb von zwei Stunden abgeschlossen sein werden, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich beworbene Bereiche abgeschlossen ist.

13. Lassen Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren deaktiviert.
14. (Optional) Wählen Sie Tags für den Pool.
15. Wählen Sie Pool erstellen.

Stellen Sie sicher, dass dieses CIDR bereitgestellt wurde, bevor Sie fortfahren. Sie können den Bereitstellungsstatus auf der Registerkarte CIDRs auf der Seite Pool-Details sehen.

Schritt 2. Erstellen Sie einen regionalen Pool im Pool der obersten Ebene

Erstellen Sie einen regionalen Pool im Pool der obersten Ebene. Für den Pool ist ein Gebietsschema erforderlich, und es muss sich um eine der Betriebsregionen handeln, die Sie beim Erstellen des IPAM konfiguriert haben.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Erstellen eines regionalen Pools im Pool der obersten Ebene

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wenn Sie den privaten Standardbereich nicht verwenden möchten, wählen Sie im Dropdown-Menü

oben im Inhaltsbereich den Bereich aus, den Sie verwenden möchten. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.

4. Wählen Sie Pool erstellen.
5. (Optional) Fügen Sie Name tag (Namenstag) für den Pool und eine Beschreibung für den Pool ein.
6. Unter Quelle wählen Sie den Pool der obersten Ebene aus, den Sie im vorherigen Abschnitt erstellt haben.
7. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
8. Wählen Sie das Gebietsschema für den Pool aus. Die Auswahl eines Gebietsschemas stellt sicher, dass es keine regionsübergreifenden Abhängigkeiten zwischen Ihrem Pool und den daraus zugewiesenen Ressourcen gibt. Die verfügbaren Optionen stammen aus den Betriebsregionen, die Sie beim Erstellen Ihres IPAM ausgewählt haben. In diesem Tutorial verwenden wir `us-east-2` als Gebietsschema für den regionalen Pool.

   Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden.
9. Wählen Sie unter Dienst EC2 (EIP/VPC) aus. Der Dienst, den Sie auswählen, bestimmt den AWS Dienst, bei dem der CIDR beworben wird. Derzeit ist die einzige Option EC2 (EIP/VPC), was bedeutet, dass die aus diesem Pool zugewiesenen CIDRs für den Amazon EC2-Service und den Amazon VPC-Service (für CIDRs, die mit VPCs verknüpft sind) beworben werden können.
10. Wählen Sie unter CIDRs für die Bereitstellung ein CIDR aus, das für den Pool bereitgestellt werden soll. Beachten Sie, dass bei der Bereitstellung eines IPv6-CIDR für einen Pool innerhalb des Top-Level-Pool der spezifischste IPv6-Adressbereich, den Sie verwenden können, /48 für CIDRs, die öffentlich beworben werden können, und /60 für CIDRs, die nicht öffentlich beworben werden können, ist.
11. Aktivieren Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren und wählen Sie optionale Zuweisungsregeln für diesen Pool:

- Automatically import discovered resources (Entdeckte Ressourcen automatisch importieren): Diese Option ist nicht verfügbar, wenn Locale (Gebietsschema) auf None (Keine) gesetzt wird. Wenn diese Option ausgewählt ist, sucht IPAM kontinuierlich nach Ressourcen im CIDR-Bereich dieses Pools und importiert diese automatisch als Zuweisungen in Ihr IPAM. Beachten Sie Folgendes:
  - Die CIDRs, die für diese Ressourcen zugewiesen werden, dürfen nicht bereits anderen Ressourcen zugeordnet sein, damit der Import erfolgreich ist.
  - IPAM importiert ein CIDR unabhängig von seiner Compliance der Zuordnungsregeln des Pools, sodass eine Ressource importiert und anschließend als nicht konform gekennzeichnet wird.
  - Wenn IPAM mehrere sich überlappende CIDRs entdeckt, importiert IPAM nur das größte CIDR.
  - Wenn IPAM mehrere CIDRs mit übereinstimmenden CIDRs entdeckt, importiert IPAM zufällig nur einen von ihnen.
- Minimum netmask lenght (Minimale Netzmaskenlänge): Die minimale Netzmaskenlänge, die erforderlich ist, damit CIDR-Zuweisungen in diesem IPAM-Pool konform sind, und der CIDR-Block der größten Größe, der aus dem Pool zugewiesen werden kann. Die minimale Netzmaskenlänge muss kleiner als die maximale Netzmaskenlänge sein. Mögliche Netzmaskenlängen für IPv4-Adressen sind `0` - `32`. Mögliche Netzmaskenlängen für IPv6-Adressen sind `0` - `128`.
- Default netmask lenght (Standardlänge für Netzmasken): Eine standardmäßige Netzmaskenlänge für Zuweisungen, die diesem Pool hinzugefügt wurden.
- Maximum netmask lenght (Maximale Netzmaskellänge): Die maximale Netzmaskenlänge, die für CIDR-Zuweisungen in diesem Pool erforderlich ist. Dieser Wert gibt den CIDR-Block der kleinsten Größe vor, der aus dem Pool zugewiesen werden kann. Stellen Sie sicher, dass dieser Wert mindestens **`/48`** ist.
- Tagging (Markierung): Die Tags, die benötigt werden, damit Ressourcen Speicherplatz aus dem Pool zuweisen können. Wenn die Ressourcen ihre Tags geändert haben, nachdem sie Speicherplatz zugewiesen haben oder wenn die Zuordnungskennzeichnungsregeln im Pool geändert werden, wird die Ressource möglicherweise als nicht konform gekennzeichnet.
- Locale (Gebietsschema): Das Gebietsschema, das für Ressourcen benötigt wird, die CIDRs aus diesem Pool verwenden. Automatisch importierte Ressourcen, die dieses Gebietsschema nicht haben, werden als nicht konform gekennzeichnet. Ressourcen, die nicht automatisch in

den Pool importiert werden, dürfen keinen Speicherplatz aus dem Pool zuweisen, es sei denn, sie befinden sich in diesem Gebietsschema.

12. (Optional) Wählen Sie Tags für den Pool.
13. Wenn Sie mit der Konfiguration Ihres Pools fertig sind, wählen Sie Create pool (Pool erstellen) aus.

Stellen Sie sicher, dass dieses CIDR bereitgestellt wurde, bevor Sie fortfahren. Sie können den Bereitstellungsstatus auf der Registerkarte CIDRs auf der Seite Pool-Details sehen.

Schritt 3. Regionalen Pool teilen

Folgen Sie den Schritten in diesem Abschnitt, um den IPAM-Pool mithilfe von (RAM) gemeinsam zu nutzen. AWS Resource Access Manager

Aktivieren der Ressourcenfreigabe in AWS RAM

Nachdem Sie Ihren IPAM erstellt haben, sollten Sie den regionalen Pool mit anderen Konten in Ihrer Organisation teilen. Bevor Sie einen IPAM-Pool gemeinsam nutzen, führen Sie die Schritte in diesem Abschnitt aus, um die gemeinsame Nutzung von Ressourcen mit zu aktivieren. AWS RAM Wenn Sie das verwenden, AWS CLI um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`management-account`** Option.

So aktivieren Sie die Ressourcenfreigabe

1. Öffnen Sie mit dem AWS Organizations Verwaltungskonto die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie im linken Navigationsbereich Einstellungen, dann Teilen mit AWS Organizations aktivieren und anschließend Einstellungen speichern aus.

Nun können Sie einen IPAM-Pool für andere Mitglieder der Organisation freigeben.

Teilen Sie einen IPAM-Pool mit AWS RAM

In diesem Abschnitt teilen Sie den regionalen Pool mit einem anderen AWS Organizations Mitgliedskonto. Vollständige Anweisungen zur Freigabe von IPAM-Pools, einschließlich Informationen zu den erforderlichen IAM-Berechtigungen, finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM. Wenn Sie das verwenden AWS CLI , um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`ipam-account`** Option.

Um einen IPAM-Pool gemeinsam zu nutzen AWS RAM

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich, wählen Sie den IPAM-Pool aus und wählen Sie Aktionen > Details anzeigen aus.
4. Unter Resource sharing (Ressourcenfreigabe), wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus. Die AWS RAM Konsole wird geöffnet. Sie teilen sich den Pool mit AWS RAM.
5. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.
6. Wählen Sie in der AWS RAM Konsole erneut Create a resource share aus.
7. Fügen Sie einen Namen für den freigegebenen Pool hinzu.
8. Wählen Sie unter Ressourcentyp auswählen die Option IPAM-Pools und dann den ARN des Pools aus, den Sie teilen möchten.
9. Wählen Sie Weiter aus.
10. Wählen Sie die AWSRAMPermissionIpamPoolByoipCidrImportBerechtigung aus. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mit AWS RAM können Sie jedoch mehr über diese Optionen erfahren.
11. Wählen Sie Weiter aus.
12. Wählen Sie unter Prinzipale > Prinzipaltyp auswählen die Option AWS -Konto und geben Sie die Konto-ID des Kontos ein, das IPAM einen IP-Adressbereich hinzufügen soll, und wählen Sie Hinzufügen.
13. Wählen Sie Weiter aus.
14. Überprüfen Sie die Optionen für die Ressourcenfreigabe und die Prinzipale, für die die Freigabe erfolgt. Wählen Sie dann Erstellen aus.
15. Damit das **`member-account`**-Konto IP-Adressen-CIDRS aus dem IPAM-Pool zuweisen kann, erstellen Sie eine zweite Ressourcenfreigabe mit `AWSRAMDefaultPermissionsIpamPool`. Der Wert für `--resource-arns` ist der ARN des IPAM-Pools, den Sie im vorherigen Abschnitt erstellt haben. Der Wert für `--principals` ist die Konto-ID von**`member-account`**. Der Wert für `--permission-arns` ist der ARN der `AWSRAMDefaultPermissionsIpamPool`-Berechtigung.

Schritt 4: Erstellen einer VPC

Führen Sie die Schritte unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch aus.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

> **Note**
>
> - Wenn Sie VPC in der AWS Managementkonsole öffnen, muss die AWS Region, in der Sie die VPC erstellen, mit der `Locale` Option übereinstimmen, die Sie bei der Erstellung des Pools ausgewählt haben, der für die BYOIP CIDR verwendet werden soll.
> - Wenn Sie den Schritt zur Auswahl eines CIDR für die VPC erreichen, haben Sie die Möglichkeit, ein CIDR aus einem IPAM-Pool zu verwenden. Wählen Sie den regionalen Pool aus, den Sie in diesem Tutorial erstellt haben.

Wenn Sie die VPC erstellen, AWS weist sie der VPC einen CIDR im IPAM-Pool zu. Sie können die Zuweisung in IPAM anzeigen, indem Sie im Inhaltsbereich der IPAM-Konsole einen Pool auswählen und die Registerkarte Zuweisungen für den Pool anzeigen.

Schritt 5: Werben für den CIDR

Die Schritte in diesem Abschnitt müssen vom IPAM-Konto ausgeführt werden. Sobald Sie die VPC erstellt haben, können Sie damit beginnen, das CIDR, zu dem Sie es gebracht haben, bekannt zu geben AWS , das sich in dem Pool befindet, in dem der Service EC2 (EIP/VPC) konfiguriert ist. In diesem Tutorial ist das Ihr regionaler Pool. Standardmäßig wird das CIDR nicht beworben, was bedeutet, dass es über das Internet nicht öffentlich zugänglich ist.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Werbung für das CIDR

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wählen Sie den Bereich Öffentlich. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
4. Wählen Sie den regionalen Pool aus, den Sie in diesem Tutorial erstellt haben.

5. Wählen Sie die Registerkarte CIDRs.
6. Wählen Sie das BYOIP CIDR und Aktionen > Werben aus.
7. Wählen Sie Für CIDR werben aus.

Als Ergebnis wird das BYOIP CIDR beworben und der Wert in der Spalte Werbung ändert sich von Zurückgezogen auf Beworben.

Schritt 6: Bereinigen

Führen Sie die Schritte in diesem Abschnitt aus, um die Ressourcen zu bereinigen, die Sie in diesem Tutorial bereitgestellt und erstellt haben.

Schritt 1: Das CIDR aus der Werbung zurückziehen

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt. Wählen Sie den Bereich Öffentlich.
4. Wählen Sie den regionalen Pool aus, den Sie in diesem Tutorial erstellt haben.
5. Wählen Sie die Registerkarte CIDRs.
6. Wählen Sie das BYOIP CIDR aus und wählen Sie Aktionen > Werbung zurückziehen.
7. Wählen Sie CIDR zurückziehen aus.

Infolgedessen wird das BYOIP CIDR nicht mehr beworben und der Wert in der Spalte Werbung ändert sich von Beworben in Zurückgezogen.

Schritt 2: Löschen der VPC

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

- Führen Sie die Schritte unter Löschen einer VPC im Amazon-VPC-Benutzerhandbuch aus, um die VPC zu löschen. Wenn Sie VPC in der AWS Managementkonsole öffnen, muss die AWS Region, aus der die VPC gelöscht wird, mit der `Locale` Option übereinstimmen, die Sie bei der Erstellung des Pools ausgewählt haben, der für die BYOIP-CIDR verwendet werden soll. In diesem Tutorial ist dieser Pool der regionale Pool.

Wenn Sie die VPC löschen, dauert es einige Zeit, bis IPAM erkennt, dass die Ressource gelöscht wurde, und das der VPC zugewiesene CIDR freigibt. Sie können nicht mit dem nächsten Schritt in der Bereinigung fortfahren, bis Sie sehen, dass IPAM die Zuweisung aus dem Pool auf der Registerkarte Zuweisungen der Pooldetails entfernt hat.

Schritt 3: Löschen Sie die RAM-Shares und deaktivieren Sie die RAM-Integration mit AWS Organizations

Dieser Schritt muss vom IPAM-Konto bzw. vom Verwaltungskonto ausgeführt werden.

- Führen Sie die Schritte unter Löschen einer Ressourcenfreigabe im AWS RAM und Deaktivieren der gemeinsamen Nutzung von Ressourcen mit AWS Organizations im AWS RAM-Benutzerhandbuch in dieser Reihenfolge aus, um die RAM-Shares zu löschen und die RAM-Integration mit AWS Organizations zu deaktivieren.

Schritt 4: Heben Sie die Bereitstellung der CIDRs aus dem regionalen Pool und dem Pool der obersten Ebene auf

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

- Führen Sie die Schritte in Deprovisionierung von CIDRs aus einem Pool aus, um die Bereitstellung der CIDRs aus dem regionalen Pool und dann aus dem Pool der obersten Ebene in dieser Reihenfolge aufzuheben.

Schritt 5: Löschen Sie den Regionalen Pool und den Pool der obersten Ebene

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

- Führen Sie die Schritte in Einen Pool löschen aus, um den regionalen Pool und dann den Pool der obersten Ebene in dieser Reihenfolge zu löschen.

Bringen Sie Ihr eigenes öffentliches IPv4-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS

Gehen Sie wie folgt vor, um ein IPv4- oder IPv6-CIDR nur mit der CLI auf IPAM zu übertragen. AWS

Important

- Bevor Sie mit diesem Tutorial beginnen, führen Sie die Schritte unter Onboarding-Voraussetzungen für Ihren BYOIP-Adressbereich im Amazon EC2 EC2-Benutzerhandbuch durch.

  Wenn Sie die ROAs erstellen, müssen Sie für IPv4-CIDRs die maximale Länge eines IP-Adresspräfixes auf `/24` festlegen. Wenn Sie IPv6-CIDRs zu einem werbefähigen Pool hinzufügen, darf die maximale Länge eines IP-Adresspräfixes `/48` sein. Dadurch wird gewährleistet, dass Sie die volle Flexibilität haben, Ihre öffentliche IP-Adresse auf verschiedene Regionen aufzuteilen. AWS IPAM erzwingt die von Ihnen festgelegte maximale Länge. Die maximale Länge ist die kleinste Ankündigung der Präfixlänge, die Sie für diese Route zulassen werden. Wenn Sie zum Beispiel einen `/20`-CIDR-Block auf AWS bringen, indem Sie die maximale Länge auf `/24` setzen, können Sie den größeren Block beliebig teilen (z. B. mit `/21`, `/22` oder `/24`) und diese kleineren CIDR-Blöcke auf eine beliebige Region verteilen. Wenn Sie die maximale Länge auf `/23` festlegen würden, könnten Sie kein `/24` aus dem größeren Block teilen und bewerben. Beachten Sie außerdem, dass `/24` der kleinste IPv4-Block und `/48` der kleinste IPv6-Block ist, den Sie von einer Region im Internet ankündigen können.
- Sobald Sie einen IPv4-Adressbereich AWS eingerichtet haben, können Sie alle IP-Adressen in diesem Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Inhalt

Bringen Sie Ihr eigenes öffentliches IPv4-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS

Befolgen Sie diese Schritte, um ein IPv4-CIDR zu IPAM zu bringen und dem CIDR eine Elastic-IP-Adresse (EIP) zuzuweisen, indem Sie nur die AWS CLI verwenden.

Important

- Sie können derzeit keine BYOIP-Adressbereiche in Local Zones bereitstellen oder bewerben.
- In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
  - Integrieren von IPAM mit Konten in einer - AWS Organisation.
  - Erstellen eines IPAM.
- Jeder Schritt dieses Tutorials muss von einem der drei Unternehmenskonten AWS Organizations werden:
  - Das Verwaltungskonto.
  - Das als Ihr IPAM-Administrator konfigurierte Mitgliedskonto in Integrieren von IPAM mit Konten in einer - AWS Organisation. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zuweist. In diesem Tutorial wird dieses Konto als Mitgliedskonto bezeichnet.

Inhalt

Schritt 1: Erstellen Sie AWS CLI benannte Profile und IAM-Rollen

Um dieses Tutorial als AWS Einzelbenutzer abzuschließen, können Sie AWS CLI benannte Profile verwenden, um von einer IAM-Rolle zu einer anderen zu wechseln. Benannte Profile sind Sammlungen von Einstellungen und Anmeldeinformationen, auf die Sie verweisen, wenn Sie die Option `--profile` mit der AWS CLI verwenden. Weitere Informationen zum Erstellen von IAM-Rollen und benannten Profilen für AWS Konten finden Sie unter Verwenden einer IAM-Rolle in der AWS CLI im AWS Identity and Access Management-Benutzerhandbuch.

Erstellen Sie eine Rolle und ein benanntes Profil für jedes der drei AWS Konten, die Sie in diesem Tutorial verwenden werden:

- Ein Profil, das `management-account` für das Verwaltungskonto der AWS Organizations aufgerufen wurde.
- Ein Profil, das `ipam-account` für das Mitgliedskonto der AWS Organizations aufgerufen wird und als Ihr IPAM-Administrator konfiguriert ist.
- Ein Profil, das `member-account` für das Mitgliedskonto der AWS Organizations in Ihrer Organisation aufgerufen wird und CIDRs aus einem IPAM-Pool zuweist.

Nachdem Sie die IAM-Rollen und benannten Profile erstellt haben, kehren Sie zu dieser Seite zurück und fahren Sie mit dem nächsten Schritt fort. Im weiteren Verlauf dieses Tutorials werden Sie feststellen, dass die AWS CLI Beispielbefehle die `--profile` Option mit einem der genannten Profile verwenden, um anzugeben, welches Konto den Befehl ausführen muss.

Schritt 2: Erstellen eines IPAMs

Dieser Schritt ist optional. Wenn Sie bereits ein IPAM mit erstellten Betriebsregionen von `us-east-1` und `us-west-2` erstellt haben, können Sie diesen Schritt überspringen. Erstellen Sie ein IPAM und geben Sie eine Betriebsregion von `us-east-1` und `us-west-2` an. Sie müssen eine Betriebsregion auswählen, damit Sie die Gebietsschemaoption verwenden können, wenn Sie Ihren IPAM-Pool erstellen. Die IPAM-Integration mit BYOIP setzt voraus, dass das Gebietsschema für den Pool festgelegt ist, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Führen Sie den folgenden Befehl aus:

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

In der Ausgabe sehen Sie das von Ihnen erstellte IPAM. Notieren Sie den Wert für `PublicDefaultScopeId`. Im nächsten Schritt benötigen Sie Ihre ID für den öffentlichen Bereich. Sie verwenden den öffentlichen Bereich, da BYOIP-CIDRs öffentliche IP-Adressen sind, wofür der öffentliche Bereich bestimmt ist.


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


Schritt 3: Erstellen Sie einen IPAM-Pool der obersten Ebene

Führen Sie die Schritte in diesem Abschnitt durch, um einen IPAM-Pool der obersten Ebene zu erstellen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Um einen IPv4-Adresspool für all Ihre AWS Ressourcen zu erstellen, verwenden Sie den AWS CLI

1. Führen Sie den folgenden Befehl aus, um einen IPAM-Pool zu erstellen. Verwenden Sie die ID des öffentlichen Bereichs des IPAM, den Sie im vorherigen Schritt erstellt haben.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
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
```

In der Ausgabe sehen Sie `create-in-progress`, was darauf hinweist, dass die Poolerstellung im Gange ist.

```
{
    "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. Führen Sie den folgenden Befehl aus, bis Sie den Status von `create-complete` in der Ausgabe sehen.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Das folgende Beispiel zeigt den Status des Pools.

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

Schritt 4: Stellen Sie ein CIDR für den Pool der obersten Ebene bereit

Stellen Sie einen CIDR-Block für den Pool der obersten Ebene bereit. Beachten Sie, dass bei der Bereitstellung eines IPv4-CIDR für einen Pool innerhalb des Pools der obersten Ebene das minimale IPv4-CIDR, das Sie bereitstellen können, `/24` beträgt; spezifischere CIDRs (wie `/25`) sind nicht zulässig. Sie müssen das CIDR und die BYOIP-Nachricht und die Zertifikatssignatur in die Anfrage aufnehmen, damit wir überprüfen können, ob Sie den öffentlichen Raum besitzen. Eine Liste der BYOIP-Voraussetzungen, einschließlich Informationen zum Abrufen dieser BYOIP-Nachricht und der Zertifikatssignatur, finden Sie unter Bringen Sie Ihr eigenes öffentliches IPv4-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

> **Important**
>
> Sie müssen nur `--cidr-authorization-context` hinzufügen, wenn Sie das BYOIP CIDR für den Pool der obersten Ebene bereitstellen. Für den Regionalpool im Pool der obersten Ebene können Sie die `--cidr-authorization-context`-Option auslassen. Sobald Sie Ihre BYOIP an IPAM integriert haben, müssen Sie keine Eigentumsvalidierung durchführen, wenn Sie das BYOIP auf Regionen und Konten aufteilen.

Um einen CIDR-Block für den Pool bereitzustellen, verwenden Sie AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

```
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~KCIsMaU0P7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRYOdRaNx8yt-uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

   In der Ausgabe sehen Sie die CIDR-Bereitstellung.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Stellen Sie sicher, dass dieses CIDR bereitgestellt wurde, bevor Sie fortfahren.

> **Important**
>
> Während die meisten Bereitstellungen innerhalb von zwei Stunden abgeschlossen sein werden, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich beworbene Bereiche abgeschlossen ist.

   Führen Sie den folgenden Befehl aus, bis Sie den Status von `provisioned` in der Ausgabe sehen.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Die folgende Beispielausgabe zeigt den Zustand.

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

Schritt 5: Erstellen Sie einen regionalen Pool im Pool der obersten Ebene

Erstellen Sie einen regionalen Pool im Pool der obersten Ebene. `--locale` ist für den Pool erforderlich und es muss eine der Betriebsregionen sein, die Sie beim Erstellen des IPAM konfiguriert haben. Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Sie können beispielsweise nur ein CIDR für eine VPC aus einem IPAM-Pool zuweisen, der ein Gebietsschema mit der Region der VPC teilt. Beachten Sie, dass Sie es nicht ändern können, wenn Sie ein Gebietsschema für einen Pool ausgewählt haben. Wenn die Heimatregion des IPAM aufgrund eines Ausfalls nicht verfügbar ist und der Pool einen anderen Standort hat als die Heimatregion des IPAM, kann der Pool weiterhin zur Zuweisung von IP-Adressen verwendet werden.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Die Auswahl eines Gebietsschemas stellt sicher, dass es keine regionsübergreifenden Abhängigkeiten zwischen Ihrem Pool und den daraus zugewiesenen Ressourcen gibt. Die verfügbaren Optionen stammen aus den Betriebsregionen, die Sie beim Erstellen Ihres IPAM ausgewählt haben. In diesem Tutorial verwenden wir `us-west-2` als Gebietsschema für den regionalen Pool.

> **Important**
>
> Wenn Sie den Pool erstellen, müssen Sie `--aws-service ec2` einschließen. Der Dienst, den Sie auswählen, bestimmt den AWS Dienst, bei dem der CIDR beworben wird. Derzeit ist die einzige Option `ec2`, was bedeutet, dass die aus diesem Pool zugewiesenen CIDRs für den Amazon-EC2-Service (für elastische IP-Adressen) und den Amazon-VPC-Service (für CIDRs, die mit VPCs verknüpft sind) beworben werden können.

So erstellen Sie einen regionalen Pool mit der AWS CLI

1. Führen Sie den folgenden Befehl aus, um den Pool zu erstellen.

```
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
```

   In der Ausgabe sehen Sie, wie IPAM den Pool erstellt.

```
{
     "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. Führen Sie den folgenden Befehl aus, bis Sie den Status von `create-complete` in der Konsolenausgabe sehen.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

   In der Ausgabe sehen Sie die Pools, die Sie in Ihrem IPAM haben. In diesem Tutorial haben wir einen Pool auf oberster Ebene und einen regionalen Pool erstellt, sodass Sie beide sehen.

Schritt 6: Stellen Sie ein CIDR für den regionalen Pool bereit

Stellen Sie einen CIDR-Block für den regionalen Pool bereit. Beachten Sie, dass bei der Bereitstellung eines CIDR für einen Pool innerhalb des Pools der obersten Ebene das minimale IPv4-CIDR, das Sie bereitstellen können, `/24` beträgt; spezifischere CIDRs (wie `/25`) sind nicht zulässig. Nachdem Sie den ersten regionalen Pool erstellt haben, können Sie kleinere Pools (z. B.`/25`) innerhalb des regionalen Pools erstellen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Um dem regionalen Pool einen CIDR-Block zuzuweisen, verwenden Sie AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

```
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
```

   In der Ausgabe sehen Sie die CIDR-Bereitstellung.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Führen Sie den folgenden Befehl aus, bis Sie den Status von `provisioned` in der Ausgabe sehen.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   Die folgende Beispielausgabe zeigt den korrekten Zustand.

```
{
    "IpamPoolCidrs": [
        {
```

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

Schritt 7. Regionalen Pool teilen

Folgen Sie den Schritten in diesem Abschnitt, um den IPAM-Pool mithilfe von AWS Resource Access Manager (RAM) gemeinsam zu nutzen.

Aktivieren der Ressourcenfreigabe in AWS RAM

Nachdem Sie Ihren IPAM erstellt haben, sollten Sie den regionalen Pool mit anderen Konten in Ihrer Organisation teilen. Bevor Sie einen IPAM-Pool gemeinsam nutzen, führen Sie die Schritte in diesem Abschnitt aus, um die gemeinsame Nutzung von Ressourcen mit zu aktivieren. AWS RAM Wenn Sie das verwenden, AWS CLI um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`management-account`** Option.

So aktivieren Sie die Ressourcenfreigabe

1. Öffnen Sie mit dem AWS Organizations Verwaltungskonto die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie im linken Navigationsbereich Einstellungen, dann Teilen aktivieren mit AWS Organizations und klicken Sie dann auf Einstellungen speichern.

Nun können Sie einen IPAM-Pool für andere Mitglieder der Organisation freigeben.

Teilen Sie einen IPAM-Pool mit AWS RAM

In diesem Abschnitt teilen Sie den regionalen Pool mit einem anderen AWS Organizations Mitgliedskonto. Vollständige Anweisungen zur Freigabe von IPAM-Pools, einschließlich Informationen zu den erforderlichen IAM-Berechtigungen, finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM. Wenn Sie das verwenden AWS CLI , um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`ipam-account`** Option.

Um einen IPAM-Pool gemeinsam zu nutzen, verwenden Sie AWS RAM

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.

2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich, wählen Sie den IPAM-Pool aus und wählen Sie Aktionen > Details anzeigen aus.
4. Unter Resource sharing (Ressourcenfreigabe), wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus. Die AWS RAM Konsole wird geöffnet. Sie teilen sich den Pool mit AWS RAM.
5. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.
6. Wählen Sie in der AWS RAM Konsole erneut Create a resource share aus.
7. Fügen Sie einen Namen für den freigegebenen Pool hinzu.
8. Wählen Sie unter Ressourcentyp auswählen die Option IPAM-Pools und dann den ARN des Pools aus, den Sie teilen möchten.
9. Wählen Sie Weiter aus.
10. Wählen Sie die AWSRAMPermissionIpamPoolByoipCidrImportBerechtigung aus. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mit AWS RAM können Sie jedoch mehr über diese Optionen erfahren.
11. Wählen Sie Weiter aus.
12. Wählen Sie unter Prinzipale > Prinzipaltyp auswählen die Option AWS -Konto und geben Sie die Konto-ID des Kontos ein, das IPAM einen IP-Adressbereich hinzufügen soll, und wählen Sie Hinzufügen.
13. Wählen Sie Weiter aus.
14. Überprüfen Sie die Optionen für die Ressourcenfreigabe und die Prinzipale, für die die Freigabe erfolgt. Wählen Sie dann Erstellen aus.
15. Damit das **`member-account`**-Konto IP-Adressen-CIDRS aus dem IPAM-Pool zuweisen kann, erstellen Sie eine zweite Ressourcenfreigabe mit `AWSRAMDefaultPermissionsIpamPool`. Der Wert für `--resource-arns` ist der ARN des IPAM-Pools, den Sie im vorherigen Abschnitt erstellt haben. Der Wert für `--principals` ist die Konto-ID von**`member-account`**. Der Wert für `--permission-arns` ist der ARN der `AWSRAMDefaultPermissionsIpamPool`-Berechtigung.

Schritt 8: Erstellen eines öffentlichen IPv4-Pools

Das Erstellen eines öffentlichen IPv4-Pools ist ein notwendiger Schritt, damit eine öffentliche IPv4-Adresse auf AWS mit IPAM verwaltet wird. Dieser Schritt wird normalerweise von einem anderen AWS Konto ausgeführt, das eine Elastic IP-Adresse bereitstellen möchte.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

> **Important**
>
> Öffentliche IPv4-Pools und IPAM-Pools werden von unterschiedlichen Ressourcen in verwaltet. AWSÖffentliche IPv4-Pools sind Einzelkonto-Ressourcen, mit denen Sie Ihre öffentlichen CIDRs in elastische IP-Adressen konvertieren können. IPAM-Pools können verwendet werden, um Ihren öffentlichen Raum öffentlichen IPv4-Pools zuzuweisen.

Um einen öffentlichen IPv4-Pool mit dem zu erstellen AWS CLI

- Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird.

  ```
  aws ec2 create-public-ipv4-pool --region us-west-2 --profile member-account
  ```

  In der Ausgabe sehen Sie die öffentliche IPv4-Pool-ID. Sie benötigen diese ID im nächsten Schritt.

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

Schritt 9: Bereitstellen eines öffentlichen IPv4-CIDR für Ihren öffentlichen IPv4-Pool

Stellen Sie das öffentliche IPv4-CIDR für Ihren öffentlichen IPv4-Pool bereit. Der Wert für `--region` muss dem `--locale`-Wert entsprechen den Sie bei der Erstellung des Pools eingegeben haben, der für das BYOIP-CIDR verwendet wird.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

Um einen öffentlichen IPv4-Pool mit dem zu erstellen AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

```
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
```

In der Ausgabe sehen Sie das bereitgestellte CIDR.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. Führen Sie den folgenden Befehl aus, um das im öffentlichen IPv4-Pool bereitgestellte CIDR anzuzeigen.

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-
account
```

In der Ausgabe sehen Sie das bereitgestellte CIDR. Standardmäßig wird das CIDR nicht beworben, was bedeutet, dass es über das Internet nicht öffentlich zugänglich ist. Sie haben die Möglichkeit, dieses CIDR im letzten Schritt dieses Tutorials als beworben zu setzen.

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

Schritt 10: Erstellen einer elastischen IP-Adresse aus dem öffentlichen IPv4-Pool

Erstellen Sie eine elastische IP-Adresse (EIP) aus dem öffentlichen IPv4-Pool. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

Um eine EIP aus dem öffentlichen IPv4-Pool zu erstellen, verwenden Sie AWS CLI

1. Führen Sie den folgenden Befehl aus, um ein EIP zu erstellen.

```
aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
ec2-0019eed22a684e0b2 --profile member-account
```

   In der Ausgabe sehen Sie die Zuweisung.

```
{
    "PublicIp": "130.137.245.100",
    "AllocationId": "eipalloc-0db3405026756dbf6",
    "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

2. Führen Sie den folgenden Befehl aus, um die in IPAM verwaltete EIP-Zuweisung anzuzeigen.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   Die Ausgabe zeigt die Zuweisung in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
```

```
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Schritt 11: Werben für den CIDR

Die Schritte in diesem Abschnitt müssen vom IPAM-Konto ausgeführt werden. Sobald Sie die Elastic IP-Adresse (EIP) mit einer Instance oder einem Elastic Load Balancer verknüpft haben, können Sie damit beginnen, den CIDR zu bewerben, zu dem Sie weitergeleitet haben und der AWS sich im definierten Pool befindet. `--aws-service ec2` In diesem Tutorial ist das Ihr regionaler Pool. Standardmäßig wird das CIDR nicht beworben, was bedeutet, dass es über das Internet nicht öffentlich zugänglich ist. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Beginnen Sie mit der Werbung für den CIDR mithilfe von AWS CLI

- Führen Sie den folgenden Befehl aus, um das CIDR anzukündigen.

  ```
  aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
  profile ipam-account
  ```

  In der Ausgabe sehen Sie, dass das CIDR beworben wird.

  ```
  {
      "ByoipCidr": {
          "Cidr": "130.137.245.0/24",
          "State": "advertised"
      }
  }
  ```

Schritt 12: Bereinigen

Führen Sie die Schritte in diesem Abschnitt aus, um die Ressourcen zu bereinigen, die Sie in diesem Tutorial bereitgestellt und erstellt haben. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss

der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird.

Reinigen Sie mit dem AWS CLI

1. Zeigen Sie die in IPAM verwaltete EIP-Zuweisung an.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   Die Ausgabe zeigt die Zuweisung in IPAM.

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "130.137.245.0/24",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
               "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
               "ResourceType": "ec2-public-ipv4-pool",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

2. Beenden Sie die Werbung für das IPv4-CIDR.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
   profile ipam-account
   ```

   In der Ausgabe sehen Sie, dass sich der CIDR-Status von advertised (beworben) zu provisioned (bereitgestellt) geändert hat.

   ```
   {
       "ByoipCidr": {
           "Cidr": "130.137.245.0/24",
           "State": "provisioned"
   ```

```
    }
}
```

3. Geben Sie die elastische IP-Adresse frei.

   Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

   ```
   aws ec2 release-address --region us-west-2 --allocation-
   id eipalloc-0db3405026756dbf6 --profile member-account
   ```

   Sie werden keine Ausgabe sehen, wenn Sie diesen Befehl ausführen.

4. Zeigen Sie Ihre BYOIP CIDRs an.

   Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

   ```
   aws ec2 describe-public-ipv4-pools --region us-west-2 --profile member-account
   ```

   In der Ausgabe sehen Sie die IP-Adressen in Ihrem BYOIP CIDR.

   ```
   {
       "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. Geben Sie die letzte IP-Adresse im CIDR aus dem öffentlichen IPv4-Pool frei. Geben Sie die IP-Adresse mit einer Netzmaske von /32 ein. Sie müssen diesen Befehl für jede IP-Adresse im CIDR-Bereich erneut ausführen. Wenn Ihr CIDR ein `/24` ist, müssen Sie diesen Befehl ausführen, um die Bereitstellung jeder der 256 IP-Adressen im `/24`-CIDR aufzuheben. Wenn Sie den Befehl in diesem Abschnitt ausführen, muss der Wert für `--region` mit der Region Ihres IPAMs übereinstimmen.

   Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

   ```
   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
   ```

   In der Ausgabe sehen Sie die Aufhebung der Bereitstellung des CIDR.

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

       "DeprovisionedAddresses": [

           "130.137.245.255"

       ]

   }
   ```

6. Zeigen Sie Ihre BYOIP-CIDRs erneut an und stellen Sie sicher, dass keine bereitgestellten Adressen mehr vorhanden sind. Wenn Sie den Befehl in diesem Abschnitt ausführen, muss der Wert für `--region` mit der Region Ihres IPAMs übereinstimmen.

   Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
   ```

   In der Ausgabe sehen Sie die Anzahl der IP-Adressen in Ihrem öffentlichen IPv4-Pool.

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
               "Description": "",
   ```

```
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

7. Anzeigen der EIP-Zuweisung wird nicht mehr in IPAM verwaltet. Es kann einige Zeit dauern, bis IPAM feststellt, dass die elastische IP-Adresse entfernt wurde. Sie können das IPAM-Pool-CIDR nicht weiter bereinigen und die Bereitstellung aufheben, bis Sie feststellen, dass die Zuweisung aus IPAM entfernt wurde. Wenn Sie den Befehl in diesem Abschnitt ausführen, muss der Wert für `--region` mit der Option -- locale übereinstimmen, die Sie beim Erstellen des Pools eingegeben haben, der für das BYOIP-CIDR verwendet wird.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   Die Ausgabe zeigt die Zuweisung in IPAM.

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

8. Heben Sie die Bereitstellung des regionalen Pool-CIDR auf. Wenn Sie die Befehle in diesem Schritt ausführen, muss der Wert für `--region` mit der Region Ihres IPAM übereinstimmen.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   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
   ```

   In der Ausgabe sehen Sie die Aufhebung der Bereitstellung von CIDR.

   ```
   {
       "IpamPoolCidr": {
   ```

```
        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }

}
```

Die Aufhebung der Bereitstellung dauert etwas. Überprüfen Sie den Status der Aufhebung der Bereitstellung.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Warten Sie, bis deprovisioned (Bereitstellung aufgehoben) angezeigt wird, bevor Sie mit dem nächsten Schritt fortfahren.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. Löschen Sie die RAM-Freigaben und deaktivieren Sie die RAM-Integration mit AWS Organizations. Führen Sie die Schritte unter Löschen einer Ressourcenfreigabe im AWS RAM und Deaktivieren der gemeinsamen Nutzung von Ressourcen mit AWS Organizations im AWS RAM-Benutzerhandbuch in dieser Reihenfolge aus, um die RAM-Shares zu löschen und die RAM-Integration mit AWS Organizations zu deaktivieren.

   Dieser Schritt muss vom IPAM-Konto bzw. vom Verwaltungskonto ausgeführt werden. Wenn Sie das verwenden AWS CLI , um die RAM-Shares zu löschen und die RAM-Integration zu deaktivieren, verwenden Sie die `--profile` **`management-account`** Optionen `--profile` **`ipam-account`** und.

10. Löschen des regionalen Pools. Wenn Sie den Befehl in diesem Schritt ausführen, muss der Wert für `--region` mit der Region Ihres IPAM übereinstimmen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

In der Ausgabe sehen Sie den Löschstatus.

```
{
   "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. Heben Sie die Bereitstellung des Pool-CIDR der obersten Ebene auf. Wenn Sie die Befehle in diesem Schritt ausführen, muss der Wert für `--region` mit der Region Ihres IPAM übereinstimmen.

    Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

    ```
    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
    ```

    In der Ausgabe sehen Sie die Aufhebung der Bereitstellung von CIDR.

    ```
    {
    ```

```
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }

}
```

Die Aufhebung der Bereitstellung dauert etwas. Führen Sie den folgenden Befehl aus, um den Status der Aufhebung der Bereitstellung zu überprüfen.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Warten Sie, bis deprovisioned (Bereitstellung aufgehoben) angezeigt wird, bevor Sie mit dem nächsten Schritt fortfahren.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

12. Löschen des Pools der obersten Ebene. Wenn Sie den Befehl in diesem Schritt ausführen, muss der Wert für `--region` mit der Region Ihres IPAM übereinstimmen.

    Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

    ```
    aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
    pool-0a03d430ca3f5c035 --profile ipam-account
    ```

    In der Ausgabe sehen Sie den Löschstatus.

```
{
  "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. Löschen Sie das IPAM. Wenn Sie den Befehl in diesem Schritt ausführen, muss der Wert für `--region` mit der Region Ihres IPAM übereinstimmen.

    Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    In der Ausgabe sehen Sie die IPAM-Antwort. Das bedeutet, dass das IPAM gelöscht wurde.

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

Bringen Sie Ihr eigenes IPv6-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS

Befolgen Sie diese Schritte, um ein IPv6-CIDR zu IPAM zu bringen und eine VPC nur mit dem AWS CLI.

Important

- Sie können derzeit keine BYOIP-Adressbereiche in Local Zones bereitstellen oder bewerben.
- In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
  - Integrieren von IPAM mit Konten in einer - AWS Organisation.
  - Erstellen eines IPAM.
- Jeder Schritt dieses Tutorials muss von einem der drei Unternehmenskonten AWS Organizations werden:
  - Das Verwaltungskonto.
  - Das als Ihr IPAM-Administrator konfigurierte Mitgliedskonto in Integrieren von IPAM mit Konten in einer - AWS Organisation. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.

- Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zuweist. In diesem Tutorial wird dieses Konto als Mitgliedskonto bezeichnet.

Inhalt

Schritt 1: Erstellen Sie AWS CLI benannte Profile und IAM-Rollen

Um dieses Tutorial als AWS Einzelbenutzer abzuschließen, können Sie AWS CLI benannte Profile verwenden, um von einer IAM-Rolle zu einer anderen zu wechseln. Benannte Profile sind Sammlungen von Einstellungen und Anmeldeinformationen, auf die Sie verweisen, wenn Sie die Option `--profile` mit der AWS CLI verwenden. Weitere Informationen zum Erstellen von IAM-Rollen und benannten Profilen für AWS Konten finden Sie unter Verwenden einer IAM-Rolle in der AWS CLI im AWS Identity and Access Management-Benutzerhandbuch.

Erstellen Sie eine Rolle und ein benanntes Profil für jedes der drei AWS Konten, die Sie in diesem Tutorial verwenden werden:

- Ein Profil, das `management-account` für das Verwaltungskonto der AWS Organizations aufgerufen wurde.
- Ein Profil, das `ipam-account` für das Mitgliedskonto der AWS Organizations aufgerufen wird und als Ihr IPAM-Administrator konfiguriert ist.
- Ein Profil, das `member-account` für das Mitgliedskonto der AWS Organizations in Ihrer Organisation aufgerufen wird und CIDRs aus einem IPAM-Pool zuweist.

Nachdem Sie die IAM-Rollen und benannten Profile erstellt haben, kehren Sie zu dieser Seite zurück und fahren Sie mit dem nächsten Schritt fort. Im weiteren Verlauf dieses Tutorials werden Sie feststellen, dass die AWS CLI Beispielbefehle die `--profile` Option mit einem der genannten Profile verwenden, um anzugeben, welches Konto den Befehl ausführen muss.

Schritt 2: Erstellen eines IPAMs

Dieser Schritt ist optional. Wenn Sie bereits ein IPAM mit erstellten Betriebsregionen von `us-east-1` und `us-west-2` erstellt haben, können Sie diesen Schritt überspringen. Erstellen Sie ein IPAM und geben Sie eine Betriebsregion von `us-east-1` und `us-west-2` an. Sie müssen eine Betriebsregion auswählen, damit Sie die Gebietsschemaoption verwenden können, wenn Sie Ihren IPAM-Pool erstellen. Die IPAM-Integration mit BYOIP setzt voraus, dass das Gebietsschema für den Pool festgelegt ist, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Führen Sie den folgenden Befehl aus:

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

In der Ausgabe sehen Sie das von Ihnen erstellte IPAM. Notieren Sie den Wert für `PublicDefaultScopeId`. Im nächsten Schritt benötigen Sie Ihre ID für den öffentlichen Bereich.

```
{
 "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": []
```

```
    }
}
```

Schritt 3: Erstellen eines IPAM-Pools

Da Sie einen IPAM-Pool der obersten Ebene mit einem darin enthaltenen regionalen Pool erstellen und einer Ressource (einer VPC) aus dem regionalen Pool Speicherplatz zuweisen, legen Sie das Gebietsschema für den regionalen Pool fest und nicht der Pool der obersten Ebene. Sie fügen das Gebietsschema zum Regionalpool hinzu, wenn Sie den Regionalpool in einem späteren Schritt erstellen. Die IPAM-Integration mit BYOIP setzt voraus, dass das Gebietsschema für den Pool festgelegt ist, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Wählen Sie aus, ob dieser IPAM-Pool-CIDR AWS über das öffentliche Internet (oder) beworben werden soll. `--publicly-advertisable` `--no-publicly-advertisable`

> **Note**
>
> Beachten Sie, dass die Bereichs-ID die ID für den öffentlichen Bereich sein muss und die Adressfamilie `ipv6` sein muss.

Um einen IPv6-Adresspool für all Ihre Ressourcen zu erstellen, verwenden Sie AWSAWS CLI

1. Führen Sie den folgenden Befehl aus, um einen IPAM-Pool zu erstellen. Verwenden Sie die ID des öffentlichen Bereichs des IPAM, den Sie im vorherigen Schritt erstellt haben.

   ```
   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
   ```

   In der Ausgabe sehen Sie `create-in-progress`, was darauf hinweist, dass die Poolerstellung im Gange ist.

   ```
   {
       "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. Führen Sie den folgenden Befehl aus, bis Sie den Status von `create-complete` in der Ausgabe sehen.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Das folgende Beispiel zeigt den Status des Pools.

```
{
    "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": []

    }

}
```

Schritt 4: Stellen Sie ein CIDR für den Pool der obersten Ebene bereit

Stellen Sie einen CIDR-Block für den Pool der obersten Ebene bereit. Beachten Sie, dass bei der Bereitstellung eines IPv6-CIDR für einen Pool innerhalb des Pools der obersten Ebene der spezifischste IPv6-Adressbereich, den Sie verwenden können, /48 für CIDRs, die öffentlich beworben werden können, und /60 für CIDRs, die nicht öffentlich beworben werden können, ist. Sie müssen das CIDR und die BYOIP-Nachricht und die Zertifikatssignatur in die Anfrage aufnehmen, damit wir überprüfen können, ob Sie den öffentlichen Raum besitzen. Eine Liste der BYOIP-Voraussetzungen, einschließlich Informationen zum Abrufen dieser BYOIP-Nachricht und der Zertifikatssignatur, finden Sie unter Bringen Sie Ihr eigenes öffentliches IPv4-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS.

Sie müssen nur `--cidr-authorization-context` hinzufügen, wenn Sie das BYOIP CIDR für den Pool der obersten Ebene bereitstellen. Für den Regionalpool im Pool der obersten Ebene können Sie die `--cidr-authorization-context`-Option auslassen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Um einen CIDR-Block für den Pool bereitzustellen, verwenden Sie AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --cidr-authorization-
context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|
SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

   In der Ausgabe sehen Sie die CIDR-Bereitstellung.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "pending-provision"

    }

}
```

2. Stellen Sie sicher, dass dieses CIDR bereitgestellt wurde, bevor Sie fortfahren.

> **Important**
>
> Während die meisten Bereitstellungen innerhalb von zwei Stunden abgeschlossen sein werden, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich beworbene Bereiche abgeschlossen ist.

Führen Sie den folgenden Befehl aus, bis Sie den Status von `provisioned` in der Ausgabe sehen.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Die folgende Beispielausgabe zeigt den Zustand.

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

Schritt 5: Erstellen Sie einen regionalen Pool im Pool der obersten Ebene

Erstellen Sie einen regionalen Pool im Pool der obersten Ebene. `--locale` ist für den Pool erforderlich und es muss eine der Betriebsregionen sein, die Sie beim Erstellen des IPAM konfiguriert haben.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

> **Important**
>
> Wenn Sie den Pool erstellen, müssen Sie `--aws-service ec2` einschließen. Der von Ihnen gewählte Dienst bestimmt, für welchen AWS Dienst der CIDR beworben wird. Derzeit besteht die einzige Option darin`ec2`, dass die aus diesem Pool zugewiesenen CIDRs für den Amazon EC2-Service und den Amazon VPC-Service (für CIDRs, die mit VPCs verknüpft sind) beworben werden.

So erstellen Sie einen regionalen Pool mit der AWS CLI

1. Führen Sie den folgenden Befehl aus, um den Pool zu erstellen.

```
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
```

In der Ausgabe sehen Sie, wie IPAM den Pool erstellt.

```
{
    "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. Führen Sie den folgenden Befehl aus, bis Sie den Status von `create-complete` in der Konsolenausgabe sehen.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

In der Ausgabe sehen Sie die Pools, die Sie in Ihrem IPAM haben. In diesem Tutorial haben wir einen Pool auf oberster Ebene und einen regionalen Pool erstellt, sodass Sie beide sehen.

Schritt 6: Stellen Sie ein CIDR für den regionalen Pool bereit

Stellen Sie einen CIDR-Block für den regionalen Pool bereit. Beachten Sie, dass bei der Bereitstellung des CIDR für einen Pool innerhalb des Top-Level-Pool der spezifischste IPv6-Adressbereich, den Sie verwenden können, /48 für CIDRs, die öffentlich beworben werden können, und /60 für CIDRs, die nicht öffentlich beworben werden können, ist.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Um dem regionalen Pool einen CIDR-Block zuzuweisen, verwenden Sie AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   In der Ausgabe sehen Sie die CIDR-Bereitstellung.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
}
```

2. Führen Sie den folgenden Befehl aus, bis Sie den Status von `provisioned` in der Ausgabe sehen.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   Die folgende Beispielausgabe zeigt den korrekten Zustand.

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

Schritt 7. Regionalen Pool teilen

Folgen Sie den Schritten in diesem Abschnitt, um den IPAM-Pool mithilfe von AWS Resource Access Manager (RAM) gemeinsam zu nutzen.

Aktivieren der Ressourcenfreigabe in AWS RAM

Nachdem Sie Ihren IPAM erstellt haben, sollten Sie den regionalen Pool mit anderen Konten in Ihrer Organisation teilen. Bevor Sie einen IPAM-Pool gemeinsam nutzen, führen Sie die Schritte in diesem Abschnitt aus, um die gemeinsame Nutzung von Ressourcen mit zu aktivieren. AWS RAM Wenn Sie das verwenden, AWS CLI um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`management-account`** Option.

So aktivieren Sie die Ressourcenfreigabe

1. Öffnen Sie mit dem AWS Organizations Verwaltungskonto die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie im linken Navigationsbereich Einstellungen, dann Teilen mit AWS Organizations aktivieren und anschließend Einstellungen speichern aus.

Nun können Sie einen IPAM-Pool für andere Mitglieder der Organisation freigeben.

Teilen Sie einen IPAM-Pool mit AWS RAM

In diesem Abschnitt teilen Sie den regionalen Pool mit einem anderen AWS Organizations Mitgliedskonto. Vollständige Anweisungen zur Freigabe von IPAM-Pools, einschließlich Informationen zu den erforderlichen IAM-Berechtigungen, finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM. Wenn Sie das verwenden AWS CLI , um die gemeinsame Nutzung von Ressourcen zu aktivieren, verwenden Sie die `--profile` **`ipam-account`** Option.

Um einen IPAM-Pool gemeinsam zu nutzen, verwenden Sie AWS RAM

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich, wählen Sie den IPAM-Pool aus und wählen Sie Aktionen > Details anzeigen aus.

4. Unter Resource sharing (Ressourcenfreigabe), wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus. Die AWS RAM Konsole wird geöffnet. Sie teilen sich den Pool mit AWS RAM.
5. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.
6. Wählen Sie in der AWS RAM Konsole erneut Create a resource share aus.
7. Fügen Sie einen Namen für den freigegebenen Pool hinzu.
8. Wählen Sie unter Ressourcentyp auswählen die Option IPAM-Pools und dann den ARN des Pools aus, den Sie teilen möchten.
9. Wählen Sie Weiter aus.
10. Wählen Sie die AWSRAMPermissionIpamPoolByoipCidrImportBerechtigung aus. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mit AWS RAM können Sie jedoch mehr über diese Optionen erfahren.
11. Wählen Sie Weiter aus.
12. Wählen Sie unter Prinzipale > Prinzipaltyp auswählen die Option AWS -Konto und geben Sie die Konto-ID des Kontos ein, das IPAM einen IP-Adressbereich hinzufügen soll, und wählen Sie Hinzufügen.
13. Wählen Sie Weiter aus.
14. Überprüfen Sie die Optionen für die Ressourcenfreigabe und die Prinzipale, für die die Freigabe erfolgt. Wählen Sie dann Erstellen aus.
15. Damit das **`member-account`**-Konto IP-Adressen-CIDRS aus dem IPAM-Pool zuweisen kann, erstellen Sie eine zweite Ressourcenfreigabe mit `AWSRAMDefaultPermissionsIpamPool`. Der Wert für `--resource-arns` ist der ARN des IPAM-Pools, den Sie im vorherigen Abschnitt erstellt haben. Der Wert für `--principals` ist die Konto-ID von**`member-account`**. Der Wert für `--permission-arns` ist der ARN der `AWSRAMDefaultPermissionsIpamPool`-Berechtigung.

Schritt 8: Erstellen einer VPC mit dem IPv6-CIDR

Erstellen Sie eine VPC mithilfe der IPAM-Pool-ID. Sie müssen der VPC auch einen IPv4-CIDR-Block mit der `--cidr-block`-Option zuordnen, sonst schlägt die Anfrage fehl. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

Um eine VPC mit dem IPv6 CIDR zu erstellen, verwenden Sie den AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR bereitzustellen.

```
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
```

   In der Ausgabe sehen Sie, dass die VPC erstellt wird.

```
{
    "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. Zeigen Sie die VPC-Zuweisung in IPAM an.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

In der Ausgabe sehen Sie die Zuweisung in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Schritt 9: Werben Sie für das CIDR

Sobald Sie die VPC mit dem in IPAM zugewiesenen CIDR erstellt haben, können Sie damit beginnen, den CIDR, zu dem Sie gebracht haben und der sich im definierten Pool befindet AWS , bekannt zu geben. `--aws-service ec2` In diesem Tutorial ist das Ihr regionaler Pool. Standardmäßig wird das CIDR nicht beworben, was bedeutet, dass es über das Internet nicht öffentlich zugänglich ist. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Regionalpool erstellt haben, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Beginnen Sie mit der Werbung für CIDR mithilfe der AWS CLI

- Führen Sie den folgenden Befehl aus, um das CIDR anzukündigen.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

In der Ausgabe sehen Sie, dass das CIDR beworben wird.

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "advertised"
    }
}
```

Schritt 10: Bereinigen

Führen Sie die Schritte in diesem Abschnitt aus, um die Ressourcen zu bereinigen, die Sie in diesem Tutorial bereitgestellt und erstellt haben. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Regionalpool erstellt haben, der für das BYOIP CIDR verwendet wird.

Reinigen Sie mit dem AWS CLI

1. Führen Sie den folgenden Befehl aus, um die in IPAM verwaltete VPC-Zuweisung anzuzeigen.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   Die Ausgabe zeigt die Zuweisung in IPAM.

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "2605:9cc0:409::/56",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
               "ResourceId": "vpc-00b5573ffc3b31a29",
               "ResourceType": "vpc",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

2. Führen Sie den folgenden Befehl aus, um die Werbung für das CIDR zu beenden. Wenn Sie den Befehl in diesem Schritt ausführen, muss der Wert für `--region` mit der Option `--locale`

übereinstimmen, die Sie beim Erstellen des regionalen Pools eingegeben haben, der für das BYOIP CIDR verwendet wird.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

In der Ausgabe sehen Sie, dass sich der CIDR-Status von advertised (beworben) zu provisioned (bereitgestellt) geändert hat.

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "provisioned"
    }
}
```

3. Führen Sie den folgenden Befehl aus, um die VPC zu löschen. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Regionalpool erstellt haben, der für das BYOIP CIDR verwendet wird.

   Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

   ```
   aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
   profile member-account
   ```

   Sie werden keine Ausgabe sehen, wenn Sie diesen Befehl ausführen.

4. Führen Sie den folgenden Befehl aus, um die VPC-Zuweisung in IPAM anzuzeigen. Es kann einige Zeit dauern, bis IPAM feststellt, dass die VPC gelöscht wurde, und diese Zuweisung entfernt. Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` der `--locale`-Option entsprechen, die Sie eingegeben haben, als Sie den Regionalpool erstellt haben, der für das BYOIP CIDR verwendet wird.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

Die Ausgabe zeigt die Zuweisung in IPAM.

```
{
   "IpamPoolAllocations": [

        {

            "Cidr": "2605:9cc0:409::/56",

            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",

            "ResourceType": "vpc",

            "ResourceOwner": "123456789012"

        }

    ]

}
```

Führen Sie den Befehl erneut aus und suchen Sie nach der zu entfernenden Zuweisung. Sie können das IPAM-Pool-CIDR nicht weiter bereinigen und die Bereitstellung aufheben, bis Sie feststellen, dass die Zuweisung aus IPAM entfernt wurde.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Die Ausgabe zeigt die aus IPAM entfernte Zuweisung.

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

5. Löschen Sie die RAM-Freigaben und deaktivieren Sie die RAM-Integration mit AWS - Organizations. Führen Sie die Schritte unter Löschen einer Ressourcenfreigabe im AWS RAM und Deaktivieren der gemeinsamen Nutzung von Ressourcen mit AWS Organizations im AWS

RAM-Benutzerhandbuch in dieser Reihenfolge aus, um die RAM-Shares zu löschen und die RAM-Integration mit AWS Organizations zu deaktivieren.

Dieser Schritt muss vom IPAM-Konto bzw. vom Verwaltungskonto ausgeführt werden. Wenn Sie die AWS CLI RAM-Shares löschen und die RAM-Integration deaktivieren möchten, verwenden Sie die `--profile management-account` Optionen `--profile ipam-account` und.

6. Führen Sie den folgenden Befehl aus, um die Bereitstellung des regionalen Pool-CIDR aufzuheben.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
   ```

   In der Ausgabe sehen Sie die Aufhebung der Bereitstellung von CIDR.

   ```
   {
       "IpamPoolCidr": {
           "Cidr": "2605:9cc0:409::/48",
           "State": "pending-deprovision"
       }
   }
   ```

   Die Aufhebung der Bereitstellung dauert etwas. Führen Sie den Befehl weiter aus, bis der CIDR-Status Bereitstellung aufgehoben angezeigt wird.

   ```
   aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
   ```

   In der Ausgabe sehen Sie die Aufhebung der Bereitstellung von CIDR.

   ```
   {
       "IpamPoolCidr": {
           "Cidr": "2605:9cc0:409::/48",
           "State": "deprovisioned"
       }
   }
   ```

7. Führen Sie den folgenden Befehl aus, um den regionalen Pool zu löschen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

In der Ausgabe sehen Sie den Löschstatus.

```
{
    "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. Führen Sie den folgenden Befehl aus, um die Bereitstellung des Pool-CIDR der obersten Ebene aufzuheben.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

   ```
   aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
   pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
   ```

   In der Ausgabe sehen Sie die Aufhebung der Bereitstellung von CIDR.

   ```
   {
       "IpamPoolCidr": {
           "Cidr": "2605:9cc0:409::/48",
   ```

```
        "State": "pending-deprovision"
    }
}
```

Die Aufhebung der Bereitstellung dauert etwas. Führen Sie den folgenden Befehl aus, um den Status der Aufhebung der Bereitstellung zu überprüfen.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Warten Sie, bis deprovisioned (Bereitstellung aufgehoben) angezeigt wird, bevor Sie mit dem nächsten Schritt fortfahren.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. Führen Sie den folgenden Befehl aus, um den Pool der obersten Ebene zu löschen.

   Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

   In der Ausgabe sehen Sie den Löschstatus.

```
{
    "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. Führen Sie den folgenden Befehl aus, um den IPAM zu löschen.

    Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    In der Ausgabe sehen Sie die IPAM-Antwort. Das bedeutet, dass das IPAM gelöscht wurde.

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

```
}
```

Tutorial: Übertragen eines vorhandenen BYOIP-IPv4-CIDR an IPAM

Führen Sie diese Schritte aus, um ein vorhandenes IPv4-CIDR auf IPAM zu übertragen. Wenn Sie bereits ein IPv4-BYOIP-CIDR mit haben AWS, können Sie das CIDR von einem öffentlichen IPv4-Pool auf IPAM verschieben. Sie können ein IPv6 CIDR nicht an IPAM übertragen.

In diesem Tutorial wird davon ausgegangen, dass Sie bereits erfolgreich einen IP-Adressbereich AWS mithilfe des unter Bring Your Own IP Addresses (BYOIP) in Amazon EC2 beschriebenen Prozesses hinzugefügt haben und diesen IP-Adressbereich nun an IPAM übertragen möchten. Wenn Sie zum ersten Mal eine neue IP-Adresse verwenden, AWS führen Sie die Schritte unter aus. Tutorial: Mitbringen eigener IP-Adressen in IPAM

Wenn Sie einen öffentlichen IPv4-Pool an IPAM übertragen, hat dies keine Auswirkungen auf bestehende Zuordnungen. Sobald Sie einen öffentlichen IPv4-Pool an IPAM übertragen haben, können Sie je nach Ressourcentyp möglicherweise die vorhandenen Zuordnungen überwachen. Weitere Informationen finden Sie unter Überwachen Sie die CIDR-Nutzung nach Ressourcen.

Important

- Dieses Tutorial geht davon aus, dass Sie die Schritte in Erstellen eines IPAM bereits abgeschlossen haben.
- Jeder Schritt dieses Tutorials muss von einem von zwei AWS Konten ausgeführt werden:
  - Das Konto für den IPAM-Administrator. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Konto in Ihrer Organisation, dem das BYOIP CIDR gehört. In diesem Tutorial wird dieses Konto als BYOIP-CIDR-Besitzerkonto bezeichnet.

Inhalt

Schritt 1: Erstellen Sie AWS CLI benannte Profile und IAM-Rollen

Um dieses Tutorial als AWS Einzelbenutzer abzuschließen, können Sie AWS CLI benannte Profile verwenden, um von einer IAM-Rolle zu einer anderen zu wechseln. Benannte Profile sind Sammlungen von Einstellungen und Anmeldeinformationen, auf die Sie verweisen, wenn Sie die Option `--profile` mit der AWS CLI verwenden. Weitere Informationen zum Erstellen von IAM-Rollen und benannten Profilen für AWS Konten finden Sie unter Verwenden einer IAM-Rolle in der AWS CLI im AWS Identity and Access Management-Benutzerhandbuch.

Erstellen Sie eine Rolle und ein benanntes Profil für jedes der drei AWS Konten, die Sie in diesem Tutorial verwenden werden:

- Ein Profil, das `ipam-account` für das AWS Konto aufgerufen wird, das der IPAM-Administrator ist.
- Ein Profil, das `byoip-owner-account` für das AWS Konto in Ihrer Organisation aufgerufen wird, dem die BYOIP CIDR gehört.

Nachdem Sie die IAM-Rollen und benannten Profile erstellt haben, kehren Sie zu dieser Seite zurück und fahren Sie mit dem nächsten Schritt fort. Im weiteren Verlauf dieses Tutorials werden Sie feststellen, dass die AWS CLI Beispielbefehle die `--profile` Option mit einem der genannten Profile verwenden, um anzugeben, welches Konto den Befehl ausführen muss.

Schritt 2: Abrufen der ID Ihres IPAM für den öffentlichen Bereich

Führen Sie die Schritte in diesem Abschnitt aus, um die ID Ihres IPAMs für den öffentlichen Bereich abzurufen. Dieser Schritt sollte vom **`ipam-account`**-Konto ausgeführt werden.

Führen Sie den folgenden Befehl aus, um Ihre ID für den öffentlichen Bereich abzurufen.

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

In der Ausgabe sehen Sie Ihre ID für den öffentlichen Bereich. Notieren Sie die Werte für `PublicDefaultScopeId`. Sie benötigen ihn im nächsten Schritt.

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


Schritt 3: Erstellen eines IPAM-Pools

Um einen IPAM-Pool zu erstellen, führen Sie die Schritte in diesem Abschnitt aus. Dieser Schritt sollte vom **`ipam-account`**-Konto ausgeführt werden. Der von Ihnen erstellte IPAM-Pool muss ein Pool der obersten Ebene mit der `--locale`-Option sein, die der BYOIP-CIDR-Region AWS entspricht. Sie können ein BYOIP nur in einen IPAM-Pool der obersten Ebene übertragen.

> **Important**
>
> Wenn Sie den Pool erstellen, müssen Sie `--aws-service ec2` einschließen. Der Dienst, den Sie auswählen, bestimmt den AWS Dienst, bei dem der CIDR beworben wird. Derzeit ist die einzige Option `ec2`, was bedeutet, dass die aus diesem Pool zugewiesenen CIDRs für den Amazon-EC2-Service (für elastische IP-Adressen) und den Amazon-VPC-Service (für CIDRs, die mit VPCs verknüpft sind) beworben werden können.

So erstellen Sie einen IPv4-Adresspool für das übertragene BYOIP CIDR mit dem AWS CLI

1. Führen Sie den folgenden Befehl aus, um einen IPAM-Pool zu erstellen. Verwenden Sie die ID des öffentlichen Bereichs des IPAM, die Sie im vorherigen Schritt abgerufen haben.

```
aws ec2 create-ipam-pool --region us-east-1 --profile ipam-account --ipam-scope-
id ipam-scope-0087d83896280b594 --description "top-level-pool" --locale us-west-2
 --aws-service ec2 --address-family ipv4
```

   In der Ausgabe sehen Sie `create-in-progress`, was darauf hinweist, dass die Poolerstellung im Gange ist.

```
{
    "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. Führen Sie den folgenden Befehl aus, bis Sie den Status von `create-complete` in der Ausgabe sehen.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

   Das folgende Beispiel zeigt den Status des Pools. Sie benötigen den OwnerIdim nächsten Schritt.

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

Schritt 4: Teilen Sie den IPAM-Pool mit AWS RAM

Folgen Sie den Schritten in diesem Abschnitt, um einen IPAM-Pool gemeinsam zu nutzen, AWS RAM sodass ein anderes AWS Konto ein vorhandenes BYOIP-IPV4-CIDR in den IPAM-Pool übertragen und den IPAM-Pool verwenden kann. Dieser Schritt sollte vom **`ipam-account`**-Konto ausgeführt werden.

So geben Sie einen IPv4-Adresspool mit der AWS CLI frei

1. Sehen Sie sich die für IPAM-Pools verfügbaren Berechtigungen an. AWS RAM Sie benötigen beide ARNs, um die Schritte in diesem Abschnitt durchführen zu können.

```
aws ram list-permissions --region us-east-1 --profile ipam-account --resource-type
 ec2:IpamPool
```

```
{
```

```
    "permissions": [
        {
           "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool",
           "version": "1",
           "defaultVersion": true,
           "name": "AWSRAMDefaultPermissionsIpamPool",
           "resourceType": "ec2:IpamPool",
           "status": "ATTACHABLE",
           "creationTime": "2022-06-30T13:04:29.335000-07:00",
           "lastUpdatedTime": "2022-06-30T13:04:29.335000-07:00",
           "isResourceTypeDefault": true
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionIpamPoolByoipCidrImport",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMPermissionIpamPoolByoipCidrImport",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:55.032000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:55.032000-07:00",
            "isResourceTypeDefault": false
        }
    ]
}
```

2. Erstellen Sie eine Ressourcenfreigabe, damit das Konto **`byoip-owner-account`** BYOIP-CIDRs in IPAM importieren kann. Der Wert für `--resource-arns` ist der ARN des IPAM-Pools, den Sie im vorherigen Abschnitt erstellt haben. Beim Wert für `--principals` handelt es sich um die ID des BYOIP-CIDR-Eigentümerkontos. Der Wert für `--permission-arns` ist der ARN der `AWSRAMPermissionIpamPoolByoipCidrImport`-Berechtigung.

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare2 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMPermissionIpamPoolByoipCidrImport
```

```
{

    "resourceShare": {
```

```
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7993758c-a4ea-43ad-be12-b3abaffe361a",
        "name": "PoolShare2",

        "owningAccountId": "123456789012",

        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:32:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:32:25.536000-07:00"

        }

}
```

3. (Optional) Wenn Sie nach Abschluss der Übertragung dem Konto **byoip-owner-account** erlauben möchten, IP-Adress-CIDRs aus dem IPAM-Pool öffentlichen IPv4-Pools zuzuweisen, kopieren Sie den ARN für `AWSRAMDefaultPermissionsIpamPool` und erstellen Sie eine zweite Ressourcenfreigabe. Der Wert für `--resource-arns` ist der ARN des IPAM-Pools, den Sie im vorherigen Abschnitt erstellt haben. Beim Wert für `--principals` handelt es sich um die ID des BYOIP-CIDR-Eigentümerkontos. Der Wert für `--permission-arns` ist der ARN der `AWSRAMDefaultPermissionsIpamPool`-Berechtigung.

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare1 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool
```

```
{

    "resourceShare": {

        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f",
        "name": "PoolShare1",

        "owningAccountId": "123456789012",
```

```
        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:31:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:31:25.536000-07:00"

        }

}
```

Durch die Erstellung der Ressourcenfreigabe im RAM kann das byoip-owner-account Konto nun CIDRs nach IPAM verschieben.

Schritt 5: Übertragen eines vorhandenen BYOIP-IPV4-CIDR an IPAM

Führen Sie die Schritte in diesem Abschnitt aus, um ein vorhandenes BYOIP-IPV4-CIDR an IPAM zu übertragen. Dieser Schritt sollte vom **`byoip-owner-account`**-Konto ausgeführt werden.

> **Important**
>
> Sobald Sie einen IPv4-Adressbereich eingerichtet haben AWS, können Sie alle IP-Adressen in diesem Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Um das BYOIP CIDR an IPAM zu übertragen, muss der BYOIP-CIDR-Besitzer die folgenden Berechtigungen in seiner IAM-Richtlinie haben:

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> Sie können AWS CLI für diesen Schritt entweder das AWS Management Console oder das verwenden.

AWS Management Console

So übertragen Sie einen BYOIP CIDR in den IPAM-Pool:

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/ als das **`byoip-owner-account`**-Konto.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den Pool der obersten Ebene, der in diesem Tutorial erstellt und geteilt wurde.
4. Wählen Sie Aktionen **>** BYOIP CIDR übertragen.
5. Wählen Sie BYOIP CIDR übertragen.
6. Wählen Sie Ihren BYOIP CIDR.
7. Wählen Sie Bereitstellung.

Command line

Verwenden Sie die folgenden AWS CLI Befehle, um eine BYOIP-CIDR mithilfe von an den IPAM-Pool zu übertragen: AWS CLI

1. Führen Sie den folgenden Befehl aus, um das CIDR zu übertragen. Stellen Sie sicher, dass der `--region` Wert der AWS Region des BYOIP-CIDR entspricht.

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

In der Ausgabe sehen Sie die CIDR-Bereitstellung.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "pending-transfer"

    }

}
```

2. Stellen Sie sicher, dass das CIDR übertragen wurde. Führen Sie den folgenden Befehl aus, bis Sie den Status von `complete-transfer` in der Ausgabe sehen.

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

Die folgende Beispielausgabe zeigt den Zustand.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

Schritt 6: Anzeigen des CIDR in IPAM

Führen Sie die Schritte in diesem Abschnitt aus, um den CIDR in IPAM anzuzeigen. Dieser Schritt sollte vom **`ipam-account`**-Konto ausgeführt werden.

Um das übertragene BYOIP-CIDR im IPAM-Pool mit dem AWS CLI

- Führen Sie den folgenden Befehl aus, um die in IPAM verwaltete Zuweisung anzuzeigen. Stellen Sie sicher, dass der `--region` Wert der AWS Region des BYOIP-CIDR entspricht.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

Die Ausgabe zeigt die Zuweisung in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
```

```
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

Schritt 7: Bereinigen

Führen Sie die Schritte in diesem Abschnitt aus, um die Ressourcen zu entfernen, die Sie in diesem Tutorial erstellt haben. Dieser Schritt sollte vom **`ipam-account`**-Konto ausgeführt werden.

Um die in diesem Tutorial erstellten Ressourcen zu bereinigen, verwenden Sie den AWS CLI

1. Zum Löschen der freigegebenen Ressourcen des IPAM-Pools führen Sie den folgenden Befehl aus, um den ARN der ersten Ressourcenfreigabe abzurufen:

```
aws ram get-resource-shares --region us-east-1 --profile ipam-account --
name PoolShare1 --resource-owner SELF
```

```
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f",
            "name": "PoolShare1",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2023-04-28T07:31:25.536000-07:00",
            "lastUpdatedTime": "2023-04-28T07:31:25.536000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

2. Kopieren Sie den ARN der Ressourcenfreigabe und löschen Sie damit die Ressourcenfreigabe des IPAM-Pools.

```
aws ram delete-resource-share --region us-east-1 --profile ipam-account
 --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f
```

```
{
    "returnValue": true
}
```

3. Wenn Sie unter Schritt 4: Teilen Sie den IPAM-Pool mit AWS RAM eine zusätzliche Ressourcenfreigabe erstellt haben, wiederholen Sie die beiden vorherigen Schritte, um den ARN der zweiten Ressourcenfreigabe für `PoolShare2` abzurufen und die zweite Ressourcenfreigabe zu löschen.
4. Führen Sie den folgenden Befehl aus, um die Zuordnungs-ID für den BYOIP CIDR abzurufen. Stellen Sie sicher, dass der `--region` Wert mit der AWS Region des BYOIP-CIDR übereinstimmt.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

Die Ausgabe zeigt die Zuweisung in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

5. Geben Sie die letzte IP-Adresse im CIDR aus dem öffentlichen IPv4-Pool frei. Geben Sie die IP-Adresse mit einer Netzmaske von /32 ein. Sie müssen diesen Befehl für jede IP-Adresse im CIDR-Bereich erneut ausführen. Wenn Ihr CIDR ein `/24` ist, müssen Sie diesen Befehl ausführen, um die Bereitstellung jeder der 256 IP-Adressen im `/24`-CIDR aufzuheben. Wenn Sie

den Befehl in diesem Abschnitt ausführen, muss der Wert für `--region` mit der Region Ihres IPAMs übereinstimmen.

Dieser Schritt muss vom **`byoip-owner-account`**-Konto ausgeführt werden.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1  --profile byoip-owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.255/32
```

In der Ausgabe sehen Sie die Aufhebung der Bereitstellung des CIDR.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",

    "DeprovisionedAddresses": [

        "130.137.249.255"

    ]

}
```

6. Zeigen Sie Ihre BYOIP-CIDRs erneut an und stellen Sie sicher, dass keine bereitgestellten Adressen mehr vorhanden sind. Wenn Sie den Befehl in diesem Abschnitt ausführen, muss der Wert für `--region` mit der Region Ihres IPAMs übereinstimmen.

   Dieser Schritt muss vom **`byoip-owner-account`**-Konto ausgeführt werden.

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
   ```

   In der Ausgabe sehen Sie die Anzahl der IP-Adressen in Ihrem öffentlichen IPv4-Pool.

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
               "Description": "",
               "PoolAddressRanges": [],
               "TotalAddressCount": 0,
               "TotalAvailableAddressCount": 0,
               "NetworkBorderGroup": "us-east-1",
               "Tags": []
   ```

```
        }
    ]
}
```

7. Führen Sie den folgenden Befehl aus, um den Pool der obersten Ebene zu löschen.

```
aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
id ipam-pool-0a03d430ca3f5c035
```

In der Ausgabe sehen Sie den Löschstatus.

```
{
    "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"
    }
}
```

Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen

Schließen Sie dieses Tutorial ab, um den VPC-IP-Adressraum für die Zuweisung von IP-Adressen zu VPC-Subnetzen zu planen und IP-Adressmetriken auf Subnetz- und VPC-Ebene zu überwachen.

> **Note**
>
> Dieses Tutorial behandelt die Zuweisung von privatem IPv4-Adressraum in einem privaten IPAM-Bereich zu VPCs und Subnetzen. Sie können dieses Tutorial auch mit dem öffentlichen Bereich und einem IPv6-CIDR-Bereich abschließen, indem Sie die VPC mit der von Amazon bereitgestellten IPv6-CIDR-Blockoption auf der VPC-Konsole erstellen.

Wenn Sie den VPC-IP-Adressraum für Subnetze planen, können Sie Folgendes tun:

- Planen und organisieren Sie die IP-Adressen Ihrer VPC für die Zuweisung zu Subnetzen: Sie können den VPC-IP-Adressraum in kleinere CIDR-Blöcke aufteilen und diese CIDR-Blöcke für Subnetze mit unterschiedlichen Geschäftsanforderungen bereitstellen, z. B. wenn Sie Workloads in Entwicklungs- oder Produktionssubnetzen ausführen.
- Vereinfachen Sie die Zuweisung von IP-Adressen für VPC-Subnetze: Sobald der Adressraum Ihrer VPC geplant und organisiert ist, können Sie eine Netzmaskenlänge wählen, anstatt manuell ein CIDR einzugeben. Wenn ein Entwickler beispielsweise ein Subnetz für das Hosten von Entwicklungs-Workloads erstellt, muss er einen Pool und eine Netzmaskenlänge für das Subnetz auswählen. IPAM weist den CIDR-Block dann automatisch Ihrem Subnetz zu.

Das folgende Beispiel zeigt die Hierarchie der Pool- und Ressourcenstruktur, die Sie mit diesem Tutorial erstellen werden:

- Privater Bereich
  - Ressourcenplanungspool (10.0.0.0/20)
    - Subnetzpool für Entwickler (10.0.0.0/24)
      - Subnetz für Entwickler (10.0.0.0/28)
    - Subnetzpool für die Produktion (10.0.0.1/24)
      - Subnetz für die Produktion (10.0.0.16/28)

> **Important**
>
> - Der Ressourcenplanungspool kann verwendet werden, um CIDRs Subnetzen zuzuweisen, oder er kann als Quellpool verwendet werden, in dem Sie andere Pools erstellen können.

In diesem Tutorial verwenden wir den Ressourcenplanungspool als Quellpool für Subnetzpools.

- Sie können mehrere Ressourcenplanungspools mit derselben VPC erstellen, wenn der VPC mehr als ein CIDR bereitgestellt wurde. Wenn einer VPC beispielsweise zwei CIDRs zugewiesen sind, können Sie zwei Ressourcenplanungspools erstellen, einen aus jedem CIDR. Jeder CIDR kann jeweils einem Pool zugewiesen werden.

Schritt 1: Erstellen einer VPC

Führen Sie die Schritte in diesem Abschnitt durch, um eine VPC zu erstellen, die für die Planung von Subnetz-IP-Adressen verwendet werden soll. Weitere Informationen zu den IAM-Berechtigungen, die zum Erstellen von VPCs erforderlich sind, finden Sie unter Beispiele für Amazon-VPC-Richtlinien im Benutzerhandbuch von Amazon VPC.

> **Note**
>
> Sie können eine vorhandene VPC verwenden, anstatt eine neue zu erstellen. Dieses Tutorial konzentriert sich jedoch auf das Szenario, in dem die VPC mit einem manuell zugewiesenen CIDR-Block konfiguriert ist, nicht mit einem IPAM-automatisch zugewiesenen CIDR-Block.

So erstellen Sie eine VPC

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC erstellen aus.
3. Geben Sie einen Namen für die VPC ein, z. B. tutorial-vpc.
4. Wählen Sie Manuelle IPv4-CIDR-Eingabe und geben Sie einen IPv4-CIDR-Block ein. In diesem Tutorial verwenden wir 10.0.0.0/20.
5. Überspringen Sie die Option zum Hinzufügen eines IPv6-CIDR-Blocks.
6. Wählen Sie VPC erstellen aus.
7. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
8. Klicken Sie im linken Navigationsbereich auf Ressourcen.

9. Warten Sie, bis die erstellte VPC angezeigt wird. Dies dauert einige Zeit und Sie müssen möglicherweise das Fenster aktualisieren, damit sie angezeigt wird. Die VPC muss von IPAM erkannt werden, bevor Sie mit dem nächsten Schritt fortfahren können.

Schritt 2: Erstellen eines Ressourcenplanungspools

Führen Sie die Schritte in diesem Abschnitt durch, um einen Ressourcenplanungspool zu erstellen.

So erstellen Sie einen Ressourcenplanungspool

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich aus.
4. Wählen Sie Pool erstellen.
5. Lassen Sie unter IPAM-Bereich den privaten Bereich ausgewählt.
6. (Optional) Fügen Sie ein Namens-Tag hinzu, z. B. „Resource-Planning-Pool“.
7. Wählen Sie unter Quelle die Option IPAM-Bereich aus.
8. Wählen Sie unter Ressourcenplanung die Option IP-Raum innerhalb einer VPC planen und wählen Sie die VPC aus, die Sie im vorherigen Schritt erstellt haben. Die VPC ist die Ressource, die zur Bereitstellung von CIDRs für den Ressourcenplanungspool verwendet wird.
9. Wählen Sie unter CIDRs für die Bereitstellung ein VPC-CIDR aus, das für den Ressourcenpool bereitgestellt werden soll. Das CIDR, das Sie für den Ressourcenplanungspool bereitstellen, muss mit dem für die VPC bereitgestellten CIDR übereinstimmen. In diesem Tutorial verwenden wir 10.0.0.0/20.
10. Wählen Sie Pool erstellen.
11. Sobald der Pool erstellt ist, wählen Sie die Registerkarte CIDR, um den Status des bereitgestellten CIDR zu sehen. Aktualisieren Sie die Seite und warten Sie, bis sich der CIDR-Status von Pending-provision zu Provisioned ändert, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 3: Erstellen von Subnetz-Pools

Führen Sie die Schritte in diesem Abschnitt durch, um zwei Subnetzpools zu erstellen, die für die Zuweisung von IP-Speicherplatz zu Subnetzen verwendet werden.

So erstellen Sie Subnetz-Pools

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich aus.
4. Wählen Sie Pool erstellen.
5. Lassen Sie unter IPAM-Bereich den privaten Bereich ausgewählt.
6. (Optional) Fügen Sie ein Namens-Tag hinzu, z. B. „dev-subnet-pool“.
7. Wählen Sie unter Quelle die Option IPAM-Pool und dann den Ressourcenplanungspool aus, den Sie in Schritt 3 erstellt haben. Die Adressfamilie, die Konfiguration für die Ressourcenplanung und das Gebietsschema werden automatisch aus dem Quellpool übernommen.
8. Wählen Sie unter CIDRs für die Bereitstellung ein CIDR aus, das für den Subnetzpool bereitgestellt werden soll. In diesem Tutorial verwenden wir 10.0.0.0/24.
9. Wählen Sie Pool erstellen.
10. Sobald der Pool erstellt ist, wählen Sie die Registerkarte CIDR, um den Status des bereitgestellten CIDR zu sehen. Aktualisieren Sie die Seite und warten Sie, bis sich der CIDR-Status von Pending-provision zu Provisioned ändert, bevor Sie mit dem nächsten Schritt fortfahren.
11. Wiederholen Sie diesen Vorgang, um ein weiteres Subnetz mit dem Namen „prod-subnet-pool“ zu erstellen.

Wenn Sie diesen Subnetzpool nun für andere AWS-Konten verfügbar machen möchten, können Sie den Subnetzpool teilen. Anweisungen dazu finden Sie unter Teilen Sie einen IPAM-Pool mit AWS RAM. Kehren Sie dann hierher zurück, um das Tutorial abzuschließen.

Schritt 4: Erstellen von Subnetzen

Führen Sie diese Schritte durch, um zwei Subnetze zu erstellen.

So erstellen Sie Subnetze

1. Öffnen Sie mithilfe des entsprechenden Kontos die VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie Subnetze > Subnetz erstellen.

3. Wählen Sie die VPC aus, die Sie zu Beginn dieses Tutorials erstellt haben.
4. Geben Sie einen Namen für das Subnetz ein, z. B. „tutorial-subnet“.
5. (Optional) Wählen Sie eine Availability Zone aus.
6. Wählen Sie unter IPv4-CIDR-Block die Option IPAM-zugewiesener IPV4-CIDR-Block und wählen Sie den Dev-Subnetzpool und eine /28-Netzmaske aus.
7. Wählen Sie Subnetz erstellen.
8. Wiederholen Sie diesen Vorgang, um ein weiteres Subnetz zu erstellen. Wählen Sie diesmal den Prod-Subnetzpool und eine /28-Netzmaske.
9. Kehren Sie zur IPAM-Konsole zurück und wählen Sie im linken Navigationsbereich die Option Ressourcen.
10. Suchen Sie nach den Subnetzpools, die Sie erstellt haben, und warten Sie, bis die von Ihnen erstellten Subnetze darunter angezeigt werden. Dies dauert einige Zeit und Sie müssen möglicherweise das Fenster aktualisieren, damit sie angezeigt wird.

Das Tutorial ist abgeschlossen. Sie können nach Bedarf zusätzliche Subnetzpools erstellen oder eine EC2-Instance in einem der Subnetze starten.

IPAM veröffentlicht Metriken zur Nutzung von IP-Adressen in Subnetzen. Sie können CloudWatch-Alarme für die SubnetIPUsage-Metrik einrichten, sodass Sie Maßnahmen ergreifen können, wenn die IP-Nutzungsgrenzwerte überschritten werden. Wenn Sie beispielsweise einem Subnetz ein /24 CIDR (256 IP-Adressen) zugewiesen haben und Sie benachrichtigt werden möchten, wenn 80 % der IPs genutzt wurden, können Sie einen CloudWatch-Alarm einrichten, der Sie benachrichtigt, wenn dieser Schwellenwert erreicht ist. Weitere Informationen zum Erstellen eines Alarms für die Subnetz-IP-Nutzung finden Sie unter Kurzer Tipp zum Erstellen von Alarmen.

Schritt 5: Bereinigen

Führen Sie diese Schritte durch, um die Ressourcen zu löschen, die Sie mit diesem Tutorial erstellt haben.

So bereinigen Sie die Ressourcen

1. Öffnen Sie mithilfe des IPAM-Administratorkontos die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich aus.

4. Wählen Sie den Ressourcenplanungspool aus und wählen Sie Aktion > Löschen.
5. Wählen Sie Als Kaskade löschen aus. Der Ressourcenplanungspool und die Subnetzpools werden gelöscht. Dadurch werden die Subnetze selbst nicht gelöscht. Sie bleiben bei den für sie bereitgestellten CIDRs, obwohl die CIDRs nicht mehr aus einem IPAM-Pool stammen.
6. Wählen Sie Löschen.
7. Löschen Sie die Subnetze.
8. Löschen Sie die VPC.

Die Bereinigung ist abgeschlossen.

Identity and Access Management in IPAM

AWS verwendet Sicherheitsanmeldeinformationen, um Sie zu identifizieren und Ihnen Zugriff auf Ihre AWS-Ressourcen zu gewähren. Sie können Funktionen von AWS Identity and Access Management (IAM) verwenden, um anderen Benutzern, Services und Anwendungen die uneingeschränkte oder eingeschränkte Nutzung Ihrer AWS-Ressourcen zu erlauben, ohne Ihre Sicherheitsanmeldeinformationen zu teilen.

In diesem Abschnitt werden die AWS-serviceverknüpften Rollen beschrieben, die speziell für IPAM erstellt werden, und die verwalteten Richtlinien, die an die serviceverknüpften IPAM-Rollen angehängt sind. Weitere Informationen zu AWS-IAM-Rollen und -Richtlinien finden Sie unter Rollenbegriffe und -Konzepte im IAM-Benutzerhandbuch.

Weitere Informationen zu Identity and Access Management für VPC finden Sie unter Identity and Access Management für Amazon VPC im Benutzerhandbuch zu Amazon VPC.

Inhalt

Serviceverknüpfte Rollen für IPAM

Serviceverknüpfte Rollen in AWS Identity and Access Management (IAM) ermöglichen es AWS-Services, andere AWS-Services in Ihrem Namen aufzurufen. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden serviceverknüpfter Rollen im IAM-Benutzerhandbuch.

Es gibt derzeit nur eine serviceverknüpfte Rolle für IPAM: AWSServiceRoleForIPAM.

Von der serviceverknüpften Rolle erteilte Berechtigungen

IPAM verwendet die serviceverknüpfte Rolle AWSServiceRoleForIPAM, um die Aktionen in der angehängten verwalteten AWSIPAMServiceRolePolicy-Richtlinie aufzurufen. Weitere Informationen zu den zulässigen Aktionen in dieser Richtlinie finden Sie unter AWS verwaltete Richtlinien für IPAM.

Diese serviceverknüpfte Rolle verfügt auch über eine IAM-Vertrauensrichtlinie, die es dem `ipam.amazonaws.com`-Service-Prinzipal erlaubt, die erforderliche serviceverknüpfte Rolle zu übernehmen.

Erstellen der serviceverknüpften Rolle

IPAM überwacht die IP-Adressnutzung in einem oder mehreren Konten, indem es die servicegebundene Rolle in einem Konto übernimmt, die Ressourcen und ihre CIDRs erkennt und die Ressourcen in IPAM integriert.

Die serviceverknüpfte Rolle wird auf zwei Arten erstellt:

- Wenn Sie sich mit AWS-Organisationen integrieren

  Wenn Sie mit der IPAM-Konsole Integrieren von IPAM mit Konten in einer - AWS Organisation oder den `enable-ipam-organization-admin-account` AWS CLI-Befehl verwenden, wird die serviceverknüpfte Rolle AWSServiceRoleForIPAM automatisch in jedem Ihrer AWS-Organisationen-Mitgliedskonten erstellt. Infolgedessen sind die Ressourcen in allen Mitgliedskonten von IPAM auffindbar.

  > **Important**
  >
  > Damit IPAM die serviceverknüpfte Rolle in Ihrem Namen erstellen kann:
  >
  > - Das AWS-Organisationsverwaltungskonto, welches die IPAM-Integration mit AWS-Organisationen ermöglicht, müssen eine IAM-Richtlinie angehängt haben, die folgende Aktionen zulässt:
  >   - `ec2:EnableIpamOrganizationAdminAccount`
  >   - `organizations:EnableAwsServiceAccess`
  >   - `organizations:RegisterDelegatedAdministrator`
  >   - `iam:CreateServiceLinkedRole`
  > - Dem IPAM-Konto muss eine IAM-Richtlinie beigefügt sein, welche die Aktion `iam:CreateServiceLinkedRole` erlaubt.

- Wenn Sie ein IPAM mithilfe eines einzigen AWS-Kontos erstellen

  Wenn Sie Verwenden Sie IPAM mit einem einzigen Konto, wird die serviceverknüpfte AWSServiceRoleForIPAM automatisch erstellt, wenn Sie ein IPAM als Konto erstellen.

> **Important**
>
> Wenn Sie IPAM mit einem einzigen AWS-Konto verwenden, bevor Sie ein IPAM erstellen, müssen Sie sicherstellen, dass dem AWS-Konto, das Sie verwenden, eine IAM-Richtlinie angehängt ist, welche die `iam:CreateServiceLinkedRole`-Aktion zulässt. Wenn Sie ein IPAM erstellen, erstellen Sie automatisch die serviceverknüpfte Rolle AWSServiceRoleForIPAM. Informationen zum Verwalten von IAM-Richtlinien finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

Bearbeiten der serviceverknüpften Rolle

Sie können die serviceverknüpfte Rolle AWSServiceRoleForIPAM nicht bearbeiten.

Löschen der serviceverknüpften Rolle

Wenn Sie IPAM nicht mehr benötigen, empfehlen wir, die serviceverknüpfte Rolle AWSServiceRoleForIPAM zu löschen.

> **Note**
>
> Sie können die serviceverknüpfte Rolle erst löschen, nachdem Sie alle IPAM-Ressourcen in Ihrem AWS-Konto gelöscht haben. Auf diese Weise wird sichergestellt, dass Sie die Überwachungsfunktion von IPAM nicht versehentlich entfernen.

Führen Sie diese Schritte aus, um die serviceverknüpfte Rolle über die AWS CLI zu löschen:

1. Löschen Sie Ihre IPAM-Ressourcen mit deprovision-ipam-pool-cidr und delete-ipam. Weitere Informationen finden Sie unter Deprovisionierung von CIDRs aus einem Pool und Löschen Sie ein IPAM.
2. Deaktivieren Sie das IPAM-Konto mit disable-ipam-organization-admin-account.
3. Deaktivieren Sie den IPAM-Service mit disable-aws-service-access mit der `--service-principal ipam.amazonaws.com`-Option.
4. Löschen der serviceverknüpften Rolle delete-service-linked-role. Wenn Sie die serviceverknüpfte Rolle löschen, wird die von IPAM verwaltete Richtlinie ebenfalls gelöscht. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für IPAM

Wenn Sie IPAM mit einem einzigen AWS-Konto verwenden und Sie einen IPAM erstellen, wird die verwaltete Richtlinie AWSIPAMServiceRolePolicy automatisch in Ihrem IAM-Konto erstellt und an die serviceverknüpfte Rolle AWSServiceRoleForIPAM angehängt.

Wenn Sie die IPAM-Integration mit AWS-Organisationen aktivieren, wird die verwaltete Richtlinie AWSIPAMServiceRolePolicy automatisch in Ihrem IAM-Konto und in jedem Ihrer AWS-Organisationen-Mitgliedskonten erstellt und die verwaltete Richtlinie wird an die service-verknüpfte Rolle AWSServiceRoleForIPAM angefügt.

Mit dieser verwalteten Richtlinie hat IPAM folgende Möglichkeiten:

- Überwachen Sie CIDRs, die Netzwerkressourcen für alle Mitglieder Ihrer AWS-Organization zugewiesen sind.
- Speichern Sie Metriken in Bezug auf IPAM in Amazon CloudWatch, z. B. den in Ihren IPAM-Pools verfügbaren IP-Adressraum und die Anzahl der Ressourcen-CIDRs, die den Zuweisungsregeln entsprechen.

Das folgende Beispiel zeigt die Details der erstellten verwalteten Richtlinie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IPAMDiscoveryDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses",
```

```
                "ec2:GetIpamDiscoveredResourceCidrs",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:ListByoipCidrs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsPublishActions",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

Die erste Anweisung im vorherigen Beispiel ermöglicht IPAM, die CIDRs, die von Ihrem einzelnen AWS-Konto oder von den Mitgliedern Ihrer AWS-Organisation verwendet werden, zu überwachen.

Die zweite Anweisung im vorhergehenden Beispiel verwendet `cloudwatch:PutMetricData`-Bedingungsschlüssel, damit IPAM IPAM-Metriken in Ihrem `AWS/IPAM` Amazon-CloudWatch-Namespace speichern kann. Diese Metriken werden von der AWS-Managementkonsole zur Anzeige von Daten über die Zuweisungen in Ihren IPAM-Pools und Bereichen verwendet. Weitere Informationen finden Sie unter Überwachen der CIDR-Nutzung mit dem IPAM-Dashboard.

Aktualisierungen der AWS verwalteten Richtlinie

Anzeigen von Details zu Aktualisierungen für AWS-verwaltete Richtlinien für IPAM, seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat.

Änderung	Beschreibung	Datum
AWSIPAMServiceRolePolicy	Der verwalteten Richtlinie AWSIPAMServiceRolePolicy	13. November 2023

Änderung	Beschreibung	Datum
	(`ec2:GetIpamDiscoveredPublicAddresses`) wurde eine Aktion hinzugefügt, damit IPAM während der Ressourcenerkennung öffentliche IP-Adressen abrufen kann.	
AWSIPAMServiceRolePolicy	Der verwalteten Richtlinie AWSIPAMServiceRolePolicy (`ec2:DescribeAccountAttributes`, `ec2:DescribeNetworkInterfaces`, `ec2:DescribeSecurityGroups`, `ec2:DescribeSecurityGroupRules`, `ec2:DescribeVpnConnections`, `globalaccelerator:ListAccelerators`, and `globalaccelerator:ListByoipCidrs`) wurden Aktionen hinzugefügt, damit IPAM während der Ressourcenerkennung öffentliche IP-Adressen abrufen kann.	1. November 2023

Änderung	Beschreibung	Datum
AWSIPAMServiceRolePolicy	Der verwalteten Richtlinie AWSIPAMServiceRolePolicy wurden zwei Aktionen (`ec2:GetIpamDiscoveredAccounts` und `ec2:GetIpamDiscoveredResourceCidrs`) hinzugefügt, damit IPAM die AWS-Konten und -Ressourcen-CIDRs abrufen kann, die während der Ressourcenerkennung überwacht werden.	25. Januar 2023
IPAM hat mit der Verfolgung von Änderungen begonnen	IPAM hat mit der Verfolgung von Änderungen für seine AWS-verwalteten Richtlinien begonnen.	2. Dezember 2021

Beispielrichtline

Die Beispielrichtlinie in diesem Abschnitt enthält alle relevanten AWS Identity and Access Management (IAM-) Aktionen für die vollständige IPAM-Nutzung. Je nachdem, wie Sie IPAM verwenden, müssen Sie möglicherweise nicht alle IAM-Aktionen einbeziehen. Für eine vollständige Nutzung der IPAM-Konsole müssen Sie möglicherweise zusätzliche IAM-Aktionen für Services wie AWS Organizations, AWS Resource Access Manager (RAM) und Amazon CloudWatch hinzufügen.

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIpamByoasn",
                "ec2:DeprovisionIpamByoasn",
                "ec2:DescribeIpamByoasn",
```

```
                "ec2:DisassociateIpamByoasn",
                "ec2:ProvisionIpamByoasn",
                "ec2:CreateIpam",
                "ec2:DescribeIpams",
                "ec2:ModifyIpam",
                "ec2:DeleteIpam",
                "ec2:CreateIpamScope",
                "ec2:DescribeIpamScopes",
                "ec2:ModifyIpamScope",
                "ec2:DeleteIpamScope",
                "ec2:CreateIpamPool",
                "ec2:DescribeIpamPools",
                "ec2:ModifyIpamPool",
                "ec2:DeleteIpamPool",
                "ec2:ProvisionIpamPoolCidr",
                "ec2:GetIpamPoolCidrs",
                "ec2:DeprovisionIpamPoolCidr",
                "ec2:AllocateIpamPoolCidr",
                "ec2:GetIpamPoolAllocations",
                "ec2:ReleaseIpamPoolAllocation",
                "ec2:CreateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveries",
                "ec2:ModifyIpamResourceDiscovery",
                "ec2:DeleteIpamResourceDiscovery",
                "ec2:AssociateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveryAssociations",
                "ec2:DisassociateIpamResourceDiscovery",
                "ec2:GetIpamResourceCidrs",
                "ec2:ModifyIpamResourceCidr",
                "ec2:GetIpamAddressHistory",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ipam.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

Kontingente für Ihr IPAM

In diesem Abschnitt werden die Kontingente im Zusammenhang mit IPAM aufgeführt. Die Konsole „Service Quotas“ stellt auch Informationen zu IPAM-Kontingenten bereit. Sie können die Service Quotas-Konsole verwenden, um Standard-Kontingente anzuzeigen und Kontingent-Erhöhungen für einstellbare Kontingente anzufordern. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service Quotas-Benutzerhandbuch.

Name	Standard	Anpassbar
Von Amazon bereitgestellte IPv6-CIDR-Block-Netzmaskenlänge	/52	Ja. Sie müssen das AWS Support Center kontaktieren, wie unter AWS-Service Quotas in der Allgemeine AWS-Referenz beschrieben.
Von Amazon bereitgestellte IPv6-CIDR-Blöcke pro regionalem Pool	1	Ja. Sie müssen das AWS Support Center kontaktieren, wie unter AWS-Service Quotas in der Allgemeine AWS-Referenz beschrieben.
Autonome Systemnummern (ASNs), die Sie in IPAM einbinden können	5	Ja. Sie müssen das AWS Support Center kontaktieren, wie unter AWS-Service Quotas in der Allgemeine AWS-Referenz beschrieben.

Name	Standard	Anpassbar
CIDRs pro Pool	50	Ja
IPAM-Administratoren pro Organisation	1	Nein
IPAMs pro Region	1	Nein
Pooltiefe (Anzahl der Pools innerhalb von Pools)	10	Ja
Pools pro Bereich	50	Ja
Zuordnungen zur Ressourcenerkennung pro IPAM	5	Ja
Ressourcenergebnisse pro Region	1	Nein
Metriken zur Ressourcenauslastung	50	Ja. Sie müssen das AWS Support Center kontaktieren, wie unter AWS-Service Quotas in der Allgemeine AWS-Referenz beschrieben.

Name	Standard	Anpassbar
Bereiche pro IPAM	5	Ja. Wenn Sie ein IPAM erstellen, werden Standardb ereiche (ein privater und ein öffentlic her) für Sie erstellt. Wenn Sie zusätzlic he Bereiche erstellen möchten, handelt es sich um private Bereiche. Sie können keine zusätzlichen öffentlichen Bereiche erstellen.

Preise für IPAM

In diesem Abschnitt wird beschrieben, wie Sie preisbezogene Informationen und Ihre aktuellen IPAM-Kosten anzeigen.

Preisinformationen anzeigen

IPAM bietet zwei Stufen: die kostenlose Stufe und die erweiterte Stufe. Weitere Informationen zu den in den einzelnen Kontingenten verfügbaren Features und den Kosten der Kontingente finden Sie unter Preise für Amazon VPC auf der Registerkarte IPAM.

Sehen Sie sich Ihre aktuellen Kosten und Nutzung an unter AWS Cost Explorer

Wenn Sie die erweiterte IPAM-Stufe nutzen, zahlen Sie einen Stundenpreis pro aktiver IP-Adresse, die von IPAM verwaltet wird. Wenn Sie Ihre IPAM-Kosten und -Nutzung einsehen und analysieren möchten, können Sie AWS Cost Explorer verwenden.

1. Öffnen Sie die AWS Cost Management Konsole unter https://console.aws.amazon.com/cost-management/home.
2. Starten Sie Cost Explorer.
3. Filtern Sie nach der IPAM-Nutzung, indem Sie den Verwendungstyp auswählen und **`IPAddressManager`** eingeben.
4. Wählen Sie mindestens ein Kontrollkästchen aus. Jeder von ihnen steht für eine andere AWS Region.
5. Klicken Sie auf Apply (Anwenden).

Wenn Sie beispielsweise USE1-IP AddressManager -IP-Hours (Hrs) auswählen und us-east-1 Ihre IPAM-Heimatregion ist, werden Ihnen die Anzahl der aktiven IP-Stunden, die IPAM in allen Regionen in Rechnung stellt, und die Kosten angezeigt. Wenn die Nutzung in Stunden beispielsweise 18 beträgt, bedeutet dies, dass Sie eine aktive IP-Adresse für 18 Stunden, 3 IP-Adressen in 3 verschiedenen Regionen, die jeweils für 6 Stunden aktiv sind, oder eine beliebige Kombination davon haben könnten, die zusammen 18 Stunden ergeben.

Weitere Informationen zu AWS Cost Explorer finden Sie unter Analysieren Ihrer Kosten mit AWS Cost Explorer im AWS Cost Management Benutzerhandbuch.

Ähnliche Informationen

Die folgenden verwandten Ressourcen bieten Ihnen nützliche Informationen für die Arbeit mit diesem Service.

- Amazon VPC IP Address Manager Best Practices: Ein AWS Blog mit bewährten Methoden für die Planung und Erstellung eines skalierbaren Adressschemas mit Amazon VPC IP Address Manager.
- Network Address Management and Auditing at Scale with Amazon VPC IP Address Manager: Ein AWS Blog, der Amazon VPC IP Address Manager vorstellt und zeigt, wie Sie den Service in der AWS-Konsole verwenden.
- Konfigurieren des differenzierten Zugriffs auf Ihre freigegebenen Ressourcen mit AWS Resource Access Manager: Ein AWS-Blog, der erklärt, wie Sie einen IPAM-Pool für die Konten in einer Organisationseinheit einer AWS-Organisation freigeben.

Dokumentverlauf für IPAM

Die folgende Tabelle beschreibt die Versionen für IPAM.

Feature	Beschreibung	Veröffentlichungsdatum
Kostenlose und erweiterte Kontingente für IPAM	Sie können jetzt für Ihren IPAM zwischen dem kostenlosen Kontingent und dem erweiterten Kontingent wählen.	17. November 2023
Einblicke in öffentliche IP-Adressen	Bisher konnten Sie Einblicke in öffentliche IPs nur in einer einzigen Region einsehen. Sie können jetzt Einblicke in öffentliche IPs in allen Regionen einsehen. Darüber hinaus können Sie jetzt Einblicke in öffentliche IPs in Amazon CloudWatch einsehen.	17. November 2023
Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen	Sie können jetzt IPAM verwenden, um den Subnetz-IP-Bereich innerhalb einer VPC zu planen und IP-Adress-Metriken auf Subnetz- und VPC-Ebene zu überwachen.	17. November 2023
Bring your own ASN (BYOASN)	Sie können jetzt Ihre eigene autonome Systemnummer (ASN) in AWS einbinden.	17. November 2023
Von AWS verwaltete Richtlinienaktualisierungen – Aktualisierung einer vorhandenen Richtlinie	Vorhandene AWSIPAMServiceRolePolicy wurde aktualisiert.	17. November 2023
Von AWS verwaltete Richtlinienaktualisierungen – Aktualisierung einer	Vorhandene AWSIPAMServiceRolePolicy wurde aktualisiert.	1. November 2023

Feature	Beschreibung	Veröffentlichungsdatum
vorhandenen Richtlinie		
Metriken zur Ressourcenauslastung	IPAM veröffentlicht jetzt IP-Auslastungsmetriken für Ressourcen, die der IPAM überwacht, in Amazon CloudWatch.	2. August 2023
Einblicke in öffentliche IP-Adressen	Einblicke in öffentliche IP-Adressen lassen alle öffentlichen IPv4-Adressen erkennen, die von Services in dieser Region in Ihrem Konto verwendet werden. Anhand dieser Einblicke können Sie die Nutzung öffentlicher IPv4-Adressen ermitteln und Empfehlungen zur Freigabe ungenutzter Elastic-IP-Adressen anzeigen.	28. Juli 2023
Von AWS verwaltete Richtlinienaktualisierungen – Aktualisierung einer vorhandenen Richtlinie	Vorhandene AWSIPAMServiceRolePolicy wurde aktualisiert.	25. Januar 2023
Integrieren von IPAM mit Konten außerhalb Ihrer Organisation	Sie können jetzt IP-Adressen außerhalb Ihrer Organisation von einem einzigen IPAM-Konto aus verwalten und IPAM-Pools mit den Konten anderer AWS Organizations teilen.	25. Januar 2023
Von Amazon bereitgestellter zusammenhängender IPv6-CIDR-Block für IPAM-Pools	Wenn Sie einen IPAM-Pool im öffentlichen Bereich erstellen, können Sie dem Pool jetzt einen von Amazon bereitgestellten zusammenhängenden IPv6-CIDR-Block bereitstellen. Weitere Informationen finden Sie unter Erstellen von IPv6-Pools.	25. Januar 2023

Feature	Beschreibung	Veröffentlichungsdatum
Erstversion	In dieser Version wird der IP-Adressen-Manager von Amazon VPC eingeführt.	2. Dezember 2021

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.