IP-Adress-Manager

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: IP-Adress-Manager

Table of Contents

Was ist IPAM?

Amazon VPC IP Address Manager (IPAM) ist eine VPC-Funktion, die es Ihnen erleichtert, IP-Adressen für Ihre Workloads zu planen, nachzuverfolgen und zu überwachen. AWS 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
- Automatische Zuweisung nach bestimmten Geschäftsregeln CIDRs VPCs
- Fehlerbehebung bei Netzwerk-Verbindungsproblemen
- Aktivieren Sie regionsübergreifende und kontoübergreifende Freigabe Ihrer Bring Your Own IP (BYOIP)-Adressen
- Bereitstellen von Amazon bereitgestellter zusammenhängender IPv6 CIDR-Blöcke für Pools zur VPC-Erstellung

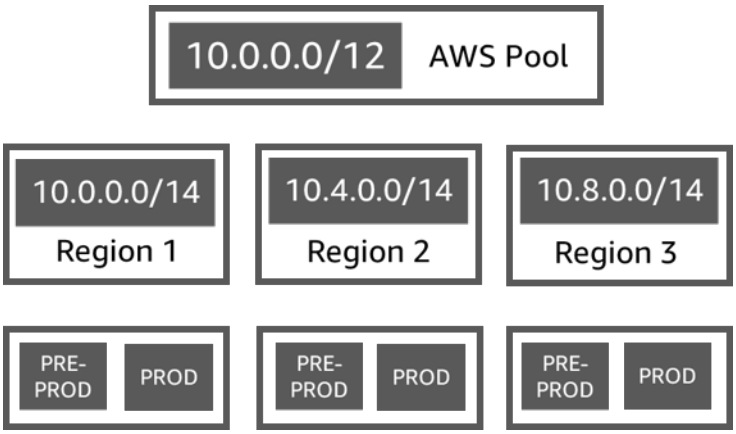
Dieses Handbuch enthält die folgenden Abschnitte:

- Funktionsweise von IPAM: IPAM-Kernkonzepte und Terminologie.
- Erste Schritte mit IPAM: Schritte zur Aktivierung der unternehmensweiten IP-Adressverwaltung mit AWS Organizations, zur Erstellung eines IPAM und zur Planung 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: Ausführliche step-by-step Anleitungen zum Erstellen eines IPAM und von Pools, zum Zuweisen von VPC CIDRs und zum Hinzufügen Ihrer eigenen öffentlichen IP-Adresse CIDRs zu IPAM.

Funktionsweise von IPAM

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

Das folgende Diagramm zeigt eine IPAM-Poolhierarchie für mehrere AWS Regionen innerhalb eines IPAM-Pools der obersten Ebene. Jeder AWS regionale Pool enthält zwei IPAM-Entwicklungspools, einen Pool für die Vorproduktion und einen Pool für Produktionsressourcen. 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 das IPAM erstellen, wählen Sie aus, in welcher AWS Region es 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. Wenn Sie IPAM erstellen, werden automatisch ein öffentlicher und ein privater Standardbereich für Sie erstellt. Jeder Bereich repräsentiert den IP-Bereich für ein einzelnes Netzwerk. Der private Bereich ist für alle IP-Adressen vorgesehen, die nicht im Internet angekündigt werden können. Der öffentliche Bereich ist im Allgemeinen für alle IP-Adressen vorgesehen, von denen aus im Internet Werbung gemacht werden kann. AWS Beachten Sie, dass Sie bei der Bereitstellung von BYOIPv6 Adressen für einen IPAM-Pool die Adressen so konfigurieren können, dass sie nicht öffentlich bekannt gegeben werden können, obwohl sie sich im öffentlichen Bereich befinden. 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 CIDRs Sie Ressourcen zu. AWS
- 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 öffentlichen und privaten Raum verwalten und überwachen. IPv6 Weitere Informationen zu öffentlichen und privaten IPv6 Adressen finden Sie unter IPv6 Adressen im Amazon VPC-Benutzerhandbuch.

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. Dieser Abschnitt soll Ihnen einen schnellen Einstieg in IPAM ermöglichen. Möglicherweise stellen Sie jedoch fest, dass die in diesem Abschnitt beschriebenen Schritte nicht Ihren Anforderungen entsprechen. Informationen zu den verschiedenen Verwendungsmöglichkeiten von IPAM finden Sie unter Planen der Bereitstellung von IP-Adressen und Tutorials für Amazon VPC IP Address Manager.

In diesem Abschnitt greifen Sie 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.

Aufgaben

- Zugriff auf IPAM
- Konfigurieren von Integrationsoptionen für Ihr IPAM
- Erstellen eines IPAM
- Planen der Bereitstellung von IP-Adressen
- CIDRs Aus einem IPAM-Pool zuweisen

Zugriff auf IPAM

Wie bei anderen AWS Diensten können Sie Ihr IPAM mit den folgenden Methoden erstellen, darauf zugreifen und es verwalten:

- AWS Management Console: Stellt eine Weboberfläche bereit, mit der Sie Ihr IPAM erstellen und verwalten können. Siehe https://console.aws.amazon.com/ipam/.
- AWS Befehlszeilenschnittstelle (AWS CLI): Stellt Befehle für eine Vielzahl von AWS Diensten bereit, einschließlich Amazon VPC. Die AWS CLI wird unter Windows, MacOS und Linux unterstützt. Informationen zum Abrufen der AWS CLI finden Sie unter AWS Command Line Interface.
- AWS SDKs: Geben Sie eine sprachspezifische Sprache APIs an. AWS SDKsSie kümmern sich um viele Verbindungsdetails, z. B. um die Berechnung von Signaturen, die Bearbeitung von Wiederholungsversuchen von Anfragen 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 Amazon EC2 API-Referenz.

Dieses Handbuch konzentriert sich hauptsächlich auf die Verwendung der AWS Management Console für die Erstellung, den Zugriff und die Verwaltung Ihres IPAM. In jeder Beschreibung, wie ein Prozess in der Konsole abgeschlossen wird, finden Sie Links zur AWS CLI-Dokumentation, die Ihnen zeigt, wie Sie dasselbe mit der AWS CLI tun 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 von Integrationsoptionen für Ihr IPAM fortfahren.

Konfigurieren von Integrationsoptionen für Ihr IPAM

In diesem Abschnitt werden Ihre Optionen beschrieben, wie Sie IPAM in AWS Organizations oder andere AWS Konten integrieren oder es mit einem einzigen AWS Konto verwenden können.

Bevor Sie mit der Verwendung von IPAM beginnen, müssen Sie eine der Optionen in diesem Abschnitt auswählen, damit IPAM die EC2 Netzwerkressourcen überwachen CIDRs und Messwerte speichern kann:

- Informationen zur Aktivierung der Integration von IPAM AWS Organizations , damit der Amazon VPC IPAM-Service Netzwerkressourcen verwalten und überwachen kann, die von den Mitgliedskonten aller AWS Organizations erstellt wurden, finden Sie unter. Integrieren Sie IPAM mit Konten in einer Organisation AWS
- Informationen zur Integration von IPAM mit AWS Organizations Konten außerhalb Ihrer Organisation nach der Integration finden Sie unter. Integrieren von IPAM mit Konten außerhalb Ihrer Organisation
- Informationen zur Verwendung eines einzelnen AWS Kontos mit IPAM und zur Aktivierung des Amazon VPC IPAM-Service zur Verwaltung und Überwachung der Netzwerkressourcen, die Sie mit dem einzelnen Konto erstellen, finden Sie unter. 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 Sie IPAM mit Konten in einer Organisation AWS

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 haben die folgenden Vorteile:

- Teilen Sie Ihre IPAM-Pools mit Ihrer Organisation: Wenn Sie ein IPAM-Konto delegieren, ermöglicht IPAM anderen AWS Organisationskonten in der Organisation, IPAM-Pools zuzuweisen CIDRs , die mit AWS Resource Access Manager (RAM) gemeinsam genutzt 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 Daten, CIDRs die von bestehenden VPCs Mitgliedskonten anderer AWS Organizations verwendet werden, in IPAM.

Wenn Sie ein AWS Organisations-Mitgliedskonto nicht als IPAM-Konto delegieren, überwacht IPAM nur die Ressourcen in dem AWS Konto, mit dem Sie das IPAM erstellen.

> **Note**
>
> Bei der Integration mit AWS Organizations:

- Sie müssen die Integration mit AWS Organizations aktivieren, indem Sie IPAM in der AWS Managementkonsole oder den enable-ipam-organization-admin AWS CLI-Befehl - account verwenden. Dadurch wird sichergestellt, dass die `AWSServiceRoleForIPAM`-serviceverknüpfte Rolle erstellt wird. Wenn Sie den vertrauenswürdigen Zugriff mit AWS Organizations mithilfe der AWS Organisationskonsole oder des register-delegated-administrator AWS CLI-Befehls aktivieren, wird die `AWSServiceRoleForIPAM` serviceverknüpfte Rolle nicht erstellt, und Sie können keine Ressourcen innerhalb Ihrer Organisation verwalten oder überwachen.
- Das IPAM-Konto muss ein Mitgliedskonto einer AWS Organizations sein. Sie können das AWS Organisationsverwaltungskonto nicht als IPAM-Konto verwenden. Um zu überprüfen, ob Ihr IPAM bereits in AWS Organizations integriert ist, gehen Sie wie folgt vor und sehen Sie sich die Details der Integration in den Organisationseinstellungen an.
- 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 über ein Konto bei AWS Organizations und ein Verwaltungskonto mit einem oder mehreren Mitgliedskonten verfügen. 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 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 mit dem AWSService RoleFor IPAM-Dienst verknüpfte Rolle.
- Der mit dem AWS Organisationsverwaltungskonto verknüpfte Benutzer muss eine IAM-Rolle verwenden, der die folgenden IAM-Richtlinienaktionen zugeordnet 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 mit dem AWS Organisationsverwaltungskonto verknüpfte Benutzer kann eine IAM-Rolle verwenden, der die folgenden IAM-Richtlinienaktionen angehängt sind,

um Ihre aktuellen delegierten Administratoren von AWS-Organisationen aufzulisten: `organizations:ListDelegatedAdministrators`

AWS Management Console

So wählen Sie ein IPAM-Konto aus

1. Öffnen Sie mit dem Verwaltungskonto für AWS Organizations die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie in der AWS Management Console 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 für AWS Organizations angemeldet haben. Wählen Sie Delegieren.
5. Geben Sie die AWS Konto-ID für ein IPAM-Konto ein. Der IPAM-Administrator muss ein Mitgliedskonto einer AWS Organizations sein.
6. Wählen Sie Änderungen speichern.

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-Administratorkonto zu delegieren: -account enable-ipam-organization-admin

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 IP-Adressnutzung in diesen Konten, indem es die dienstbezogene IAM-Rolle in jedem Mitgliedskonto übernimmt, die Ressourcen und ihre Ressourcen ermittelt und sie CIDRs 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 Sie IPAM mit Konten in einer Organisation AWS 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 dem Teilen mit den Befehlen get-ipam-discovered-resource-cidrs und get-ipam-discovered-accountsCLI oder GetIpamDiscoveredResourceCidrsund anzeigen. GetIpamDiscoveredAccounts

APIs 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. Handelt es sich bei dem Besitzerkonto um ein AWS Dienstkonto eines Drittanbieters, das Ressourcen für mehrere seiner eigenen Kunden erstellt, werden diese Ressourcen bei der Ressourcensuche erkannt. Wenn das AWS Drittanbieter-Dienstkonto die Ressourcensuche mit einem AWS Endbenutzerkonto teilt, hat der Endbenutzer Einblick in die Ressourcen der anderen Kunden des AWS Drittanbieterdienstes. Aus diesem Grund sollte der AWS Drittanbieter-Service bei der Erstellung und gemeinsamen Nutzung von Ressourcenentdeckungen Vorsicht walten lassen oder für jeden Kunden ein separates AWS Konto verwenden.

Prozessübersicht

In diesem Abschnitt wird erklärt, wie Sie Ihr IPAM mit AWS Konten außerhalb Ihrer Organisation integrieren können. 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 in den Prozess involviert:

- Primärer Organisationsinhaber — Das AWS Organizations Verwaltungskonto für Organisation 1.
- IPAM-Konto der primären Organisation – Das delegierte IPAM-Administratorkonto für Organisation 1.
- Sekundärer Organisationsinhaber — 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 Sie IPAM mit Konten in einer Organisation AWS).
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 Sie IPAM mit Konten in einer Organisation AWS).
4. Das sekundäre Administratorkonto der Organisation erstellt eine Ressourcenerkennung und teilt diese mithilfe von AWS RAM (siehe Erstellen einer Ressourcenerkennung, um sie in ein anderes IPAM zu integrieren undEine Ressourcenerkennung mit einem anderen AWS Konto teilen) mit dem IPAM-Konto der primären Organisation. Die Ressourcenerkennung muss in derselben Heimatregion wie das IPAM der primären Organisation erstellt werden.
5. Das primäre IPAM-Konto der Organisation akzeptiert die Einladung zur gemeinsamen Nutzung von Ressourcen mit AWS RAM (siehe Einladungen zur gemeinsamen Nutzung annehmen und ablehnen 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 mithilfe von RAM AWS).
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 dies nicht möchtenIntegrieren Sie IPAM mit Konten in einer Organisation AWS, 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 (IAM) erstellt.

Serviceverknüpfte Rollen sind eine Art von IAM-Rolle, die es AWS Diensten ermöglicht, in Ihrem Namen auf andere Services zuzugreifen. AWS Sie vereinfachen den Prozess der Rechteverwaltung,

indem sie automatisch die erforderlichen Berechtigungen für bestimmte AWS Dienste erstellen und verwalten, um die erforderlichen Aktionen auszuführen, wodurch die Einrichtung und Verwaltung dieser Dienste optimiert wird.

IPAM verwendet die dienstbezogene Rolle, um Metriken für CIDRs Netzwerkressourcen zu überwachen und zu EC2 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, das Sie zur Erstellung des IPAM verwenden, eine IAM-Rolle mit einer zugehörigen Richtlinie verwendet, die die Aktion zulässt. `iam:CreateServiceLinkedRole` Wenn Sie das IPAM erstellen, erstellen Sie automatisch die mit dem IPAM-Dienst verknüpfte Rolle. AWSService RoleFor Informationen zum Verwalten von IAM-Richtlinien finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

Sobald das einzelne AWS Konto über die Berechtigung verfügt, die mit dem IPAM-Dienst verknüpfte Rolle zu erstellen, wechseln 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 zwischen Konten (von Mitgliedskonten bis zum delegierten IPAM-Mitgliedskonto) und regionsübergreifend (von AWS Betriebsregionen bis zur Heimatregion Ihres IPAM) 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 aus, in denen das IPAM IP-Adressen verwalten darf. CIDRs Diese AWS Regionen werden als Betriebsregionen bezeichnet. IPAM erkennt und überwacht Ressourcen nur in den AWS Regionen, die Sie als Betriebsregionen auswählen. IPAM speichert keine Daten außerhalb der von Ihnen ausgewählten Betriebsregionen.

Die folgende Beispielhierarchie zeigt, wie sich die AWS Regionen, die Sie bei der Erstellung des IPAM zuweisen, auf die Regionen auswirken, die für Pools verfügbar sind, die Sie später erstellen.

- IPAM ist in AWS Region 1 und AWS Region 2 tätig
  - 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 Management Console die AWS Region aus, 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 Betriebsregionen die AWS Regionen aus, in denen dieses IPAM Ressourcen verwalten und ermitteln kann. Die AWS Region, in der Sie Ihr IPAM erstellen, ist standardmäßig als eine der Betriebsregionen ausgewählt. Wenn Sie dieses IPAM

beispielsweise in AWS Region erstellen, `us-east-1` aber später regionale IPAM-Pools erstellen möchten, die Zugriff CIDRs darauf VPCs bieten, wählen Sie hier aus. `us-west-2` `us-west-2` 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 aus, ob Sie Private IPv6 GUA aktivieren möchten. CIDRs Weitere Informationen zu dieser Option finden Sie unter Bereitstellung von privater IPv6 GUA aktivieren CIDRs.
8. Wählen Sie, ob Sie den Messmodus aktivieren möchten. Weitere Informationen zu dieser Option finden Sie unter Kostenverteilung aktivieren.
9. 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, um Details zu Ihrem IPAM zu erstellen, zu ändern und anzuzeigen:

1. Erstellen Sie das IPAM: create-ipam
2. Zeigen Sie das von Ihnen erstellte IPAM an: describe-ipams
3. Sehen Sie sich 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 IPAMs im linken Navigationsbereich der Konsole die Option 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 Prozess der Poolerstellung unterscheidet sich für Pools in öffentlichen und privaten Bereichen. Dieser Abschnitt enthält Schritte zur Erstellung 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 Sie IPAM mit Konten in einer Organisation AWS.

In IPAM ist ein Pool eine Sammlung von zusammenhängenden IP-Adressbereichen (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
      - Regionalpool 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 Sie einen Pool auf oberster Ebene IPv4 aus und fahren Sie dann mit CIDRs Aus einem IPAM-Pool zuweisen fort.

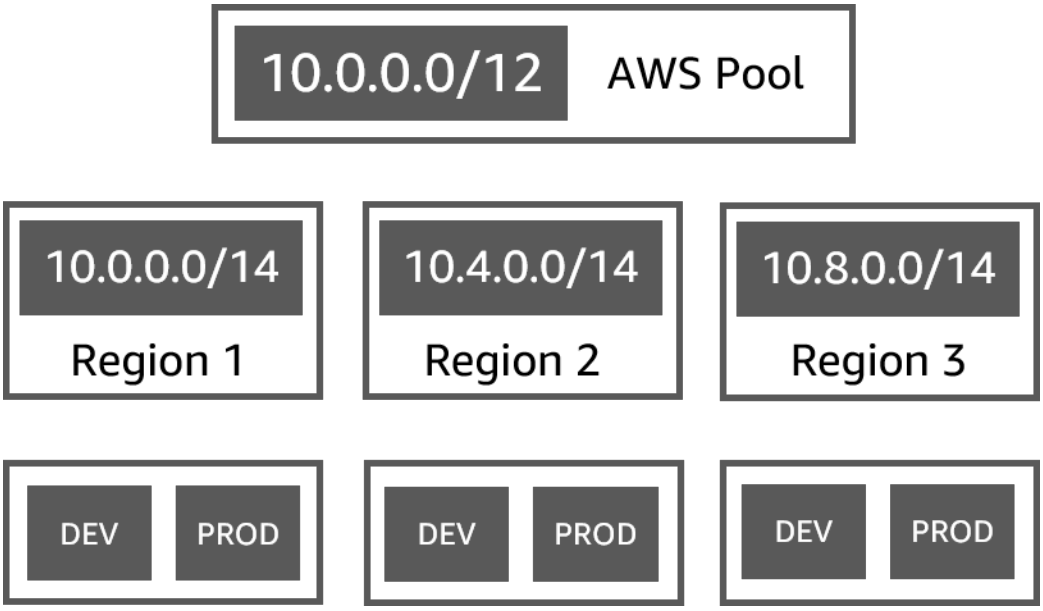
Inhalt

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.

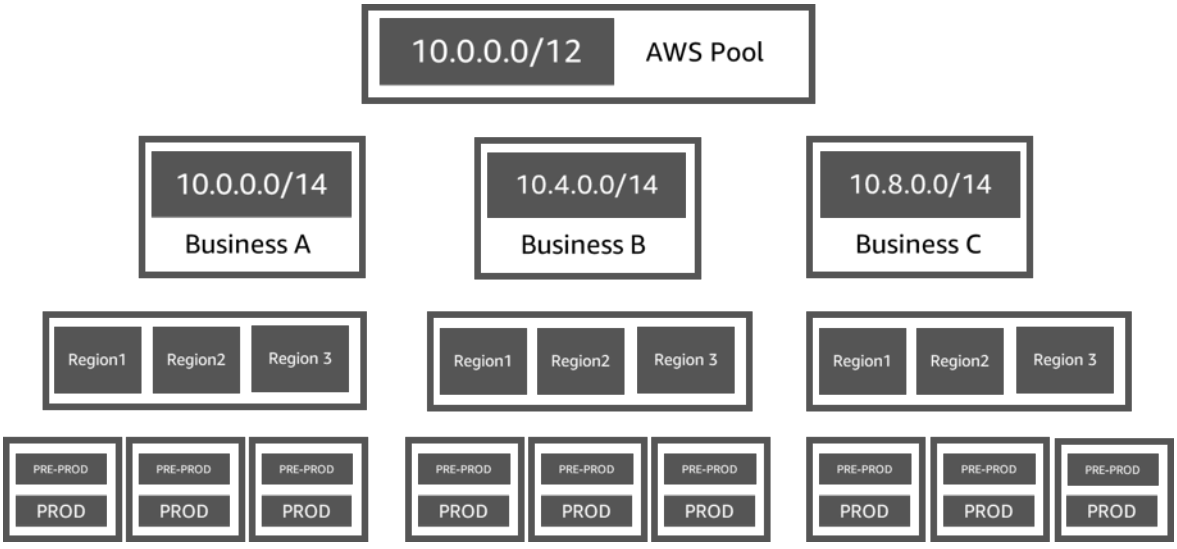
IPv4 Pools in mehreren AWS Regionen

Das folgende Beispiel zeigt eine IPAM-Poolhierarchie für mehrere AWS Regionen innerhalb eines Pools der obersten Ebene. Jeder AWS regionale Pool enthält zwei IPAM-Entwicklungspools, einen Pool für Entwicklungsressourcen und einen Pool für Produktionsressourcen.



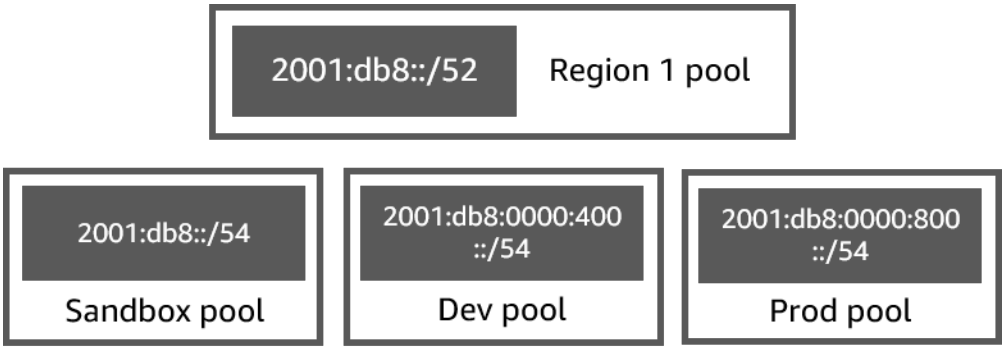
IPv4 Pools für mehrere Geschäftsbereiche

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



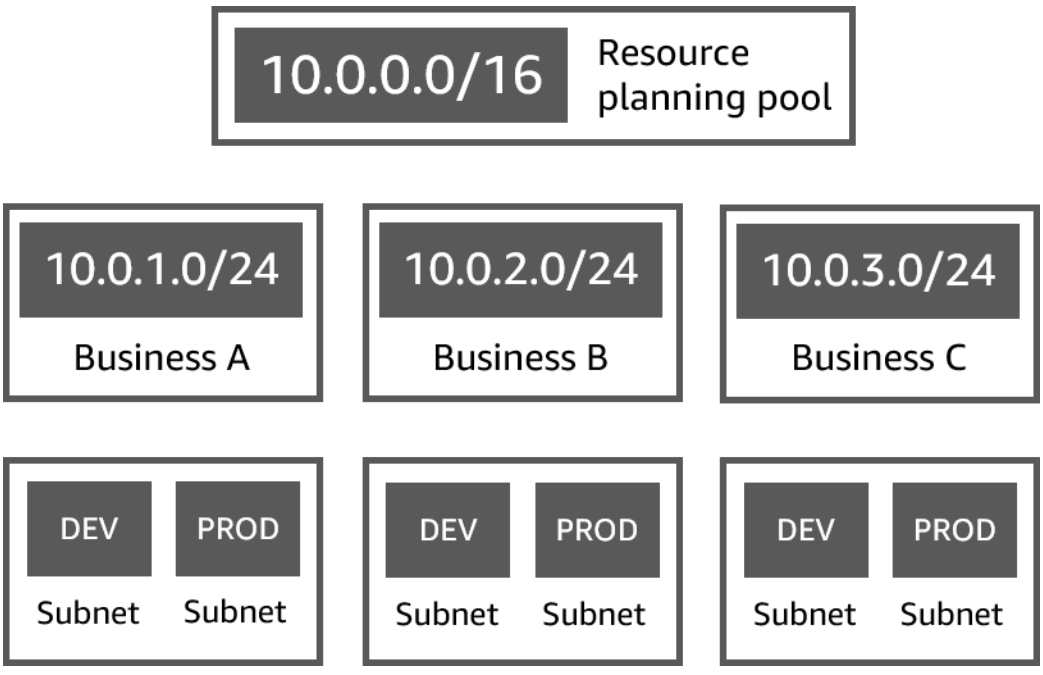
IPv6 Pools in einer AWS Region

Das folgende Beispiel zeigt eine IPv6 IPAM-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.



IPv4 Pools erstellen

Folgen Sie den Schritten in diesem Abschnitt, 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 ist in AWS Region 1 und AWS Region 2 tätig
  - Privater Bereich
    - Top-level Pool (10.0.0.0/8)
      - Regionalpool 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 vorherigen Beispiel handelt es sich bei den CIDRs verwendeten nur um Beispiele. Sie veranschaulichen, dass jeder Pool innerhalb des Pools der obersten Ebene mit einem Teil des CIDR der obersten Ebene bereitgestellt wird.

Inhalt

Erstellen Sie einen Pool auf oberster Ebene IPv4

Folgen Sie den Schritten in diesem Abschnitt, um einen IPAM-Pool der IPv4 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 ist in AWS Region 1 und Region 2 tätig AWS
  - Privater Bereich
    - Top-level Pool (10.0.0.0/8)
      - Regionalpool in AWS Region 1 (10.0.0.0/16)
        - Entwicklungspool für nicht VPCs produktive Zwecke (10.0.0.0/24)
          - Zuweisung für eine VPC (10.0.0.0/25)

Im vorherigen Beispiel sind CIDRs die verwendeten 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:

- Gibt an, ob IPAM automatisch CIDRs in den IPAM-Pool importiert werden soll, wenn sie innerhalb des CIDR-Bereichs dieses Pools gefunden werden
- Die erforderliche Netzmaskenlänge für Zuweisungen innerhalb des Pools
- Die erforderlichen Tags für Ressourcen im Pool
- Das erforderliche Gebietsschema für Ressourcen innerhalb des Pools. Das Gebietsschema 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, der eine gemeinsam genutzte AWS Ressource im Resource Access Manager (RAM) ist, muss der Ressourcenbesitzer als Principal im AWS RAM konfiguriert werden. Weitere Informationen zum Freigeben von Pools mit RAM finden Sie unter Teilen Sie einen IPAM-Pool mithilfe von RAM AWS.

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 könnten beispielsweise eine Zuweisungsregel festlegen, die besagt, dass nur VPCs mit dem Tag prod Daten CIDRs aus einem IPAM-Pool abgerufen werden können. Sie könnten auch eine Regel festlegen, die besagt, dass die CIDRs Zuweisung aus diesem Pool nicht größer als /24 sein darf. In diesem Fall verstößt das Erstellen einer Ressource mit einem CIDR größer als /24 aus diesem Pool gegen eine Zuweisungsregel für den Pool und die Erstellung schlägt fehl. Bestehende Ressourcen mit einem CIDR-Wert größer als /24 werden als nicht konform gekennzeichnet.

> **Important**
>
> In diesem Thema wird beschrieben, wie Sie einen IPv4 Pool der obersten Ebene mit einem IP-Adressbereich erstellen, der von bereitgestellt wird. AWS Wenn Sie Ihren eigenen IPv4 Adressbereich auf AWS (BYOIP) übertragen möchten, müssen bestimmte 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 IPv6 Pools IPv4 oder 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 die Option aus IPv4.
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 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.

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 einen IPv4 CIDR ein, der für den Pool bereitgestellt werden soll. Wenn Sie Ihren eigenen Adressbereich IPv4 oder Ihren IPv6 IP-Adressbereich verwenden möchten, müssen bestimmte AWS 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 Ressourcen CIDRs , die diesen Ressourcen zugewiesen werden, dürfen nicht bereits anderen Ressourcen zugewiesen 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 CIDRs dieser Überschneidungen feststellt, importiert IPAM nur den größten CIDR.
      - Wenn IPAM mehrere CIDRs mit übereinstimmendem Ergebnis entdeckt CIDRs, importiert IPAM nach dem Zufallsprinzip 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 liegen zwischen 0 und 32. Mögliche Netzmaskenlängen für IPv6 Adressen sind 0 bis 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.
- Gebietsschema: Das Gebietsschema, das für Ressourcen benötigt wird, die diesen Pool verwenden CIDRs . 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 Sie einen regionalen IPv4 Pool.

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 Pool der obersten Ebene in Ihrem IPAM zu erstellen oder zu bearbeiten:

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

Erstellen Sie einen regionalen IPv4 Pool

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 CIDRs Aus einem IPAM-Pool zuweisen fort.

> **Note**
>
> Der Prozess der Poolerstellung unterscheidet sich für Pools in öffentlichen und privaten Bereichen. Dieser Abschnitt enthält Schritte zur Erstellung 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 ist in AWS Region 1 und AWS Region 2 tätig

- Privater Bereich
  - Top-level Pool (10.0.0.0/8)
    - Regionalpool in AWS Region 1 (10.0.0.0/16)
      - Entwicklungspool für nicht VPCs produktive Zwecke (10.0.0.0/24)
        - Zuweisung für eine VPC (10.0.0.0/25)

Im vorherigen Beispiel handelt es sich bei den verwendeten CIDRs nur um 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. Wenn Sie diesen Pool im öffentlichen Bereich erstellen, wird eine Option für die Adressfamilie angezeigt. Wählen Sie IPv4.
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. 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.

10. Wenn Sie diesen Pool im öffentlichen Bereich erstellen, wird eine Option für Service angezeigt. Wählen Sie EC2(EIP/VPC). 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 CIDRs zugewiesenen Daten für den Amazon-Service (für Elastic IP-Adressen) und den Amazon EC2 VPC-Service (für verknüpft mit) beworben werden. CIDRs VPCs
11. (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 etwas CIDRs hinzufügen, indem Sie den Pool bearbeiten.
12. 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 Sie einen Pool auf oberster Ebene IPv4 . 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.
13. (Optional) Wählen Sie Tags für den Pool.
14. Wenn Sie mit der Konfiguration Ihres Pools fertig sind, wählen Sie Create pool (Pool erstellen) aus.
15. Siehe Erstellen Sie einen 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 Sie einen 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 CIDRs Aus einem IPAM-Pool zuweisen 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 ist in AWS Region 1 und AWS Region 2 tätig
  - Privater Bereich
    - Top-level Pool (10.0.0.0/8)
      - Regionalpool in AWS Region 1 (10.0.0.0/16)
        - Entwicklungspool für nicht VPCs produktive Zwecke (10.0.0.0/24)
          - Zuweisung für eine VPC (10.0.1.0/25)

Im vorherigen Beispiel handelt es sich bei den verwendeten CIDRs nur um 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 etwas hinzufügen CIDRs , 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 Sie einen Pool auf oberster Ebene IPv4 . 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 CIDRs Aus einem IPAM-Pool zuweisen.

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 Entwicklungspools im Regionalpool zu erstellen.

Erstellen Sie IPv6 Adresspools in Ihrem IPAM

AWS bietet IPv6 Konnektivität für viele seiner Dienste EC2, einschließlich VPC und S3, sodass Sie den erweiterten Adressraum und die erweiterten Sicherheitsfunktionen von IPv6 nutzen können. IPv6wurde entwickelt, um diese grundlegende Einschränkung von IPv4 zu beheben. Die Umstellung auf einen 128-Bit-Adressraum IPv6 bietet eine große Anzahl einzigartiger IP-Adressen. Diese massive Adresserweiterung ermöglicht die kontinuierliche Verbreitung von vernetzten Technologien, von Smartphones und IoT-Geräten bis hin zur Cloud-Infrastruktur.

Darüber hinaus können Sie mit IPAM sicherstellen, dass Sie Contiguous IPv6 CIDRs für die VPC-Erstellung verwenden. Zusammenhängend zugewiesene Bereiche, die sequentiell zugewiesen CIDRs werden. CIDRs Sie ermöglichen es Ihnen, Ihre Sicherheits- und Netzwerkregeln zu vereinfachen. Sie IPv6 CIDRs können in einem einzigen Eintrag für Netzwerk- und Sicherheitskonstrukte wie Zugriffskontrolllisten, Routing-Tabellen, Sicherheitsgruppen und Firewalls zusammengefasst werden.

Folgen Sie den Schritten in diesem Abschnitt, 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.

> **Note**
>
> Sowohl öffentliche als auch private IPv6 Adressierung sind in AWS verfügbar. AWS berücksichtigt öffentliche IP-Adressen, von denen aus im Internet Werbung gemacht wird AWS, während private IP-Adressen nicht im Internet beworben werden und können. AWS Wenn Sie möchten, dass Ihre privaten Netzwerke den Datenverkehr von diesen Adressen ins Internet weiterleiten, IPv6 und Sie nicht beabsichtigen, den Datenverkehr von diesen Adressen ins Internet weiterzuleiten, erstellen Sie Ihren IPv6 Pool in einem privaten Bereich. Weitere Informationen zu öffentlichen und privaten IPv6 Adressen finden Sie unter IPv6Adressen im Amazon VPC-Benutzerhandbuch.

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-Pool-Hierarchie:

- IPAM ist in AWS Region 1 und AWS Region 2 tätig
  - Scope
    - Regionalpool in AWS Region 1 (2001:db8: :/52)
      - Entwicklungspool (2001:db8::/54)
        - Zuweisung für eine VPC (2001:db8::/56)

Im vorherigen Beispiel sind CIDRs die verwendeten nur Beispiele. Sie veranschaulichen, dass der Entwicklungspool innerhalb des regionalen Pools mit einem Teil des CIDR des regionalen Pools bereitgestellt wird.

Inhalt

Erstellen Sie einen regionalen IPv6 Adresspool in Ihrem IPAM

Folgen Sie den Schritten in diesem Abschnitt, um einen IPv6 regionalen IPAM-Pool zu erstellen. Wenn Sie einen von Amazon bereitgestellten IPv6 CIDR-Block für einen Pool bereitstellen, muss

er für einen Pool bereitgestellt werden, für den ein Gebietsschema (Region) ausgewählt ist.AWS 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 IPAM-Pool: IPv6

- IPAM ist in AWS Region 1 und AWS Region 2 tätig
  - Scope
    - Regionalpool in AWS Region 1 (2001:db8: :/52)
      - Entwicklungspool (2001:db8::/54)
        - Zuweisung für eine VPC (2001:db8::/56)

Im vorherigen Beispiel sind CIDRs die verwendeten nur Beispiele. Sie veranschaulichen, dass jeder Pool innerhalb des IPv6 regionalen Pools mit einem Teil des IPv6 regionalen CIDR ausgestattet ist.

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 Gebietsschema 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.

> **Note**
>
> Es gibt eine zusätzliche implizite Regel, die in den Zuweisungsregeln nicht angezeigt wird. Wenn sich die Ressource in einem IPAM-Pool befindet, der eine gemeinsam genutzte AWS Ressource im Resource Access Manager (RAM) ist, muss der Ressourcenbesitzer als

Principal im AWS RAM konfiguriert werden. Weitere Informationen zum Freigeben von Pools mit RAM finden Sie unter Teilen Sie einen IPAM-Pool mithilfe von RAM AWS.

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 könnten beispielsweise eine Zuweisungsregel festlegen, die besagt, dass nur VPCs mit dem Tag prod Daten CIDRs aus einem IPAM-Pool abgerufen werden können.

Note

- In diesem Thema wird beschrieben, wie Sie einen IPv6 regionalen Pool mit einem IPv6 Adressbereich erstellen, der von AWS oder mit einem privaten IPv6 Bereich bereitgestellt wird. Wenn Sie Ihre eigenen öffentlichen Adressbereiche IPv4 oder IPv6 IP-Adressbereiche AWS (BYOIP) verwenden möchten, müssen bestimmte Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Tutorial: Mitbringen eigener IP-Adressen in IPAM.
- Wenn Sie einen IPv6 Pool in einem privaten Bereich erstellen, können Sie einen privaten IPv6 GUA- oder ULA-Bereich verwenden. Um einen privaten GUA-Bereich verwenden zu können, muss die Option zunächst auf Ihrem IPAM aktiviert sein (siehe Bereitstellung von privater IPv6 GUA aktivieren CIDRs).

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 einen privaten oder öffentlichen Bereich aus. Wenn Sie möchten, dass Ihre privaten Netzwerke den Datenverkehr von diesen Adressen ins Internet

weiterleiten, IPv6 und Sie nicht beabsichtigen, den Datenverkehr von diesen Adressen ins Internet weiterzuleiten, wählen Sie einen privaten Bereich. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.

Wenn Sie einen Pool erstellen, ist standardmäßig der private Standardbereich ausgewählt.

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 aus IPv6. Wenn Sie diesen Pool öffentlich erstellen, können alle Inhalte CIDRs dieses Pools öffentlich beworben werden.
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 möchten, muss er für einen Pool bereitgestellt werden, für den ein Gebietsschema (Region) ausgewählt ist.AWS 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 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.

10. (Optional) Wenn Sie einen IPv6 Pool im öffentlichen Bereich erstellen, wählen Sie unter Service die Option 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 CIDRs zugewiesenen Daten für den Amazon-Service (für Elastic IP-Adressen) und den Amazon EC2 VPC-Service (für verknüpft mit) beworben werden. CIDRs VPCs
11. (Optional) Wenn Sie einen IPv6 Pool im öffentlichen Bereich erstellen, wählen Sie unter der Option Öffentliche IP-Quelle die Option Amazon Owned aus, um einen IPv6 Adressbereich für diesen Pool AWS angeben zu lassen. Wie oben auf dieser Seite erwähnt, wird in diesem Thema beschrieben, wie Sie einen IPv6 regionalen Pool mit einem IP-Adressbereich erstellen, der von bereitgestellt wird AWS. Wenn Sie Ihren eigenen IPv4 oder einen IPv6 Adressbereich zu AWS (BYOIP) hinzufügen möchten, müssen bestimmte Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Tutorial: Mitbringen eigener IP-Adressen in IPAM.
12. (Optional) Sie können einen Pool ohne CIDR erstellen, aber Sie können den Pool erst für Zuordnungen verwenden, wenn Sie ein CIDR dafür bereitgestellt haben. Führen Sie einen der folgenden Schritte aus, um ein CIDR bereitzustellen:

    - Wenn Sie einen IPv6 Pool im öffentlichen Bereich mit der öffentlichen IP-Quelle im Besitz von Amazon erstellen, um einen CIDR bereitzustellen, wählen Sie unter CIDRs Zur Bereitstellung die Option Amazon-Owned CIDR hinzufügen und wählen Sie die Netzmaskengröße zwischen /40 und /52 für den CIDR. Wenn Sie im Dropdownmenü eine Netzmaskenlänge auswählen, sehen Sie die Netzmaskenlänge sowie die Zahl von /56, für die die Netzmaske steht. CIDRs 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 einen IPv6 Pool in einem privaten Bereich erstellen, können Sie einen privaten IPv6 GUA- oder ULA-Bereich verwenden:
        - Wichtige Informationen IPv6 zur privaten Adressierung finden Sie unter Private IPv6 Adressen im Amazon VPC-Benutzerhandbuch.
        - Um einen privaten IPv6 ULA-Bereich zu verwenden, wählen Sie unter CIDRsZur Bereitstellung die Option ULA-CIDR nach Netzmaske hinzufügen und wählen Sie eine Netzmaskengröße aus oder wählen Sie Private IPv6 CIDR eingeben und geben Sie einen ULA-Bereich ein. Gültiger IPv6 ULA-Speicherplatz ist alles unter fd00: :/8, das sich nicht mit dem von Amazon reservierten Bereich fd00: :/16 überschneidet.

- Um einen privaten IPv6 GUA-Bereich zu verwenden, müssen Sie zuerst die Option auf Ihrem IPAM aktiviert haben (siehe). Bereitstellung von privater IPv6 GUA aktivieren CIDRs Nachdem Sie private IPv6 GUA aktiviert haben CIDRs, geben Sie eine IPv6 GUA in Input private IPv6 CIDR ein.

13. 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 liegen zwischen 0 und 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.
    - Gebietsschema: Das Gebietsschema, das für Ressourcen benötigt wird, die diesen Pool verwenden. CIDRs 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.

14. (Optional) Wählen Sie Tags für den Pool.
15. Wählen Sie Pool erstellen.
16. Siehe Erstellen Sie einen IPv6 Adresspool für Entwickler in Ihrem 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.

Verwenden Sie die folgenden AWS CLI Befehle, um einen IPv6 regionalen Pool in Ihrem IPAM zu erstellen oder zu bearbeiten:

1. Wenn Sie die Bereitstellung einer privaten IPv6 GUA aktivieren möchten CIDRs, ändern Sie das IPAM mit modify-ipam und fügen Sie die Option hinzu. `enable-private-gua` Weitere Informationen finden Sie unter Bereitstellung von privater IPv6 GUA aktivieren CIDRs.
2. create-ipam-poolErstellen Sie einen Pool mit.
3. Stellen Sie dem Pool ein CIDR bereit: provision-ipam-pool-cidr.
4. Bearbeiten Sie den Pool, nachdem Sie ihn erstellt haben, um die Zuweisungsregeln zu ändern: modify-ipam-pool.

Erstellen Sie einen IPv6 Adresspool für Entwickler in Ihrem IPAM

Folgen Sie den Schritten in diesem Abschnitt, um einen Entwicklungspool in Ihrem IPv6 regionalen Pool zu erstellen. Wenn Sie nur einen regionalen Pool und keine Entwicklungspools benötigen, fahren Sie mit CIDRs Aus einem IPAM-Pool zuweisen 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 ist in AWS Region 1 und AWS Region 2 tätig
  - Scope
    - Regionalpool in AWS Region 1 (2001:db8: :/52)
      - Entwicklungspool (2001:db8::/54)
        - Zuweisung für eine VPC (2001:db8::/56)

Im vorherigen Beispiel sind CIDRs die verwendeten 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

Um einen Entwicklungspool innerhalb eines IPv6 regionalen Pools zu erstellen

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 einen Bereich aus. 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 unter Quellpool den IPv6 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 etwas hinzufügen CIDRs , indem Sie den Pool bearbeiten.
9. Sie haben hier dieselben Optionen für Zuweisungsregeln wie bei der Erstellung des IPv6 regionalen Pools. Für eine Erläuterung der Optionen, die beim Erstellen von Pools verfügbar sind, siehe Erstellen Sie einen regionalen IPv6 Adresspool in Ihrem IPAM.
   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 CIDRs Aus einem IPAM-Pool zuweisen.

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 IPv6 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 weitere Entwicklungspools innerhalb des IPv6 regionalen Pools zu erstellen.

CIDRs Aus einem IPAM-Pool zuweisen

Ein wichtiges Feature von IPAM ist die Möglichkeit, IP-Adressraum zuzuweisen und zu verwalten. Beim Erstellen einer VPC müssen Sie einen IP-Adress-CIDR-Block angeben, der den Bereich der für diese VPC verfügbaren IP-Adressen definiert. IPAM vereinfacht diesen Prozess, indem es einen globalen Überblick über Ihren gesamten IP-Adressbestand bietet und Ihnen hilft, IP-Präfixe strategisch mehreren zuzuweisen und wiederzuverwenden. VPCs

Diese Zuweisung von Adressraum ist entscheidend, um sicherzustellen, dass es keine sich überschneidenden IP-Bereiche gibt, die Routing-Konflikte und Konnektivitätsprobleme verursachen könnten. IPAM ermöglicht es Ihnen außerdem, IP-Adressraum für zukünftige VPC-Erweiterungen zu reservieren, sodass später keine komplexe Neunummerierung erforderlich ist.

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 Zuweisungen CIDRs aus einem IPAM-Pool auf folgende Weise vornehmen:

- Verwenden Sie einen AWS Service, der in IPAM integriert ist, z. B. Amazon VPC, und wählen Sie die Option, einen IPAM-Pool für den CIDR zu verwenden. IPAM erstellt automatisch die Zuteilung im Pool für Sie.
- Ordnen Sie ein CIDR innerhalb eines IPAM-Pool manuell zu, um es für die spätere Verwendung mit einem in IPAM integrierten AWS Service wie Amazon VPC zu reservieren.

In diesem Abschnitt werden Sie durch beide Optionen geführt: wie Sie die in IPAM integrierten AWS Dienste verwenden, um einen IPAM-Pool-CIDR bereitzustellen, und wie Sie manuell IP-Adressraum reservieren.

Inhalt

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

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie AWS Ressourcen in einem logisch isolierten virtuellen Netzwerk starten, das Sie definiert haben. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk, das Ihrem AWS Konto gewidmet ist. Es ist von anderen virtuellen Netzwerken in der AWS Cloud getrennt. Sie können einen IP-Adressbereich für die VPC festlegen, Subnetze und Gateways hinzufügen und Sicherheitsgruppen zuordnen.

Folgen Sie den Schritten unter Erstellen einer VPC im Amazon VPC-Benutzerhandbuch. 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 bei der Erstellung der VPC die Option wählen, einen IPAM-Pool zu verwenden, AWS weist dem IPAM-Pool ein CIDR 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 zur Verwendung der AWS CLI, einschließlich der Erstellung einer VPC, finden Sie im Tutorials für Amazon VPC IP Address Manager Abschnitt.

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 es CIDRs Überschneidungen mit Ihrem lokalen IP-Bereich gibt.

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 für die Zuweisung hinzufügen möchten (z. B. für IPv4 oder `10.0.0.0/24` `2001:db8::/52` für IPv6) oder ob Sie ein CIDR nach Größe hinzufügen möchten, indem Sie nur die Netzmaskenlänge wählen (z. B. für oder für). `/24` IPv4 `/52` 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, um einem Pool manuell einen CIDR zuzuweisen:

1. Rufen Sie die ID des IPAM-Pools ab, in dem Sie die Zuweisung erstellen möchten:. describe-ipam-pools
2. Erstellen Sie die Zuweisung: allocate-ipam-pool-cidr.
3. Die Zuordnung anzeigen: 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. Beachten Sie, dass dieser Abschnitt eine Gruppierung von Verfahren darstellt, die sich alle auf die Arbeit mit IPAM beziehen. Die Verfahren sind alphabetisch geordnet.

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

Ändern Sie den 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:

- Überwacht: Die VPC CIDR wurde von IPAM erkannt und wird auf Überschneidungen mit anderen Daten und die Einhaltung von CIDRs Zuweisungsregeln überwacht.
- Ignored (ignoriert): Das VPC CIDR wird von der Überwachung ausgenommen. Ignorierte VPC CIDRs werden nicht auf Überschneidungen mit anderen CIDRs oder die Einhaltung von Zuweisungsregeln geprüft. 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 eine der der VPC CIDRs zugewiesenen Optionen aus und wählen Sie Aktionen > Als ignoriert markieren oder Als ignoriert markieren aus.
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, um den Überwachungsstatus einer VPC CIDR zu ändern:

1. Holen Sie sich eine Bereichs-ID: describe-ipam-scopes
2. Den aktuellen Überwachungsstatus für die VPC CIDR anzeigen: get-ipam-resource-cidrs
3. Ändern Sie den Status der VPC CIDR: modify-ipam-resource-cidr
4. Sehen Sie sich den neuen Überwachungsstatus für die VPC CIDR an: get-ipam-resource-cidrs

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 privat IPv4 oder privat entdeckt IPv6 CIDRs, CIDRs werden die Ressourcen in den privaten Standardbereich importiert und erscheinen nicht in zusätzlichen privaten Bereichen, die Sie erstellen. Sie können CIDRs vom privaten Standardbereich zu einem anderen privaten Bereich wechseln. Weitere Informationen finden Sie unter VPC CIDRs zwischen Bereichen verschieben.

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, um einen zusätzlichen privaten Bereich zu erstellen:

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

Löschen Sie ein IPAM

Sie können ein IPAM löschen, wenn es nicht mehr benötigt wird, wenn Sie Ihre IP-Adressverwaltung umstrukturieren müssen oder wenn Sie mit einer neuen IPAM-Konfiguration beginnen möchten. Das Löschen eines IPAMs kann dazu beitragen, Ihre IP-Adressverwaltung zu vereinfachen und an sich ändernde geschäftliche oder betriebliche Anforderungen anzupassen.

Um einen IPAM zu löschen, führen Sie die Schritte in diesem Abschnitt aus. Informationen darüber, wie Sie die Standardanzahl von IPAM erhöhen IPAMs können, anstatt ein vorhandenes IPAM zu löschen, finden Sie unterKontingente für Ihr IPAM.

> **Note**
>
> Durch das Löschen eines IPAM werden alle überwachten Daten entfernt, die mit dem IPAM verknüpft sind, einschließlich der historischen Daten 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 IPAMs aus.
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 VPC-Ressourcen (z. B. VPCs) in Pools in privaten Bereichen frei.

> **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.

- Macht die IPv4 CIDRs Bereitstellung aller IPAM-Pools, die in privaten Bereichen bereitgestellt wurden, rückgängig.
- 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.
  - Deprovisionierung, die für Pools innerhalb des CIDRs IPAM bereitgestellt wurde, aufheben. Weitere Informationen finden Sie unter Deprovisionierung 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 die folgenden AWS CLI Befehle, um ein IPAM zu löschen:

1. Aktuell anzeigen IPAMs: describe-ipams
2. Löschen Sie ein IPAM: delete-ipam
3. Sehen Sie sich Ihre aktualisierten Versionen an: describe-ipams IPAMs

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

Einen Pool löschen

Ein IPAM-Pool in AWS stellt einen definierten Bereich von IP-Adressen dar, die innerhalb einer bestimmten AWS Umgebung oder Organisation zugewiesen und verwaltet werden können. Pools werden verwendet, um den IP-Adressraum zu organisieren, eine automatisierte IP-Adressverwaltung zu ermöglichen und IP-Adressverwaltungsrichtlinien in Ihrer Cloud-Infrastruktur durchzusetzen.

Sie können einen IPAM-Pool löschen, um ungenutzten oder überflüssigen IP-Adressraum zu entfernen und ihn für andere Zwecke zu nutzen. Sie können einen IP-Adresspool nicht löschen, wenn es Zuweisungen gibt. Sie müssen zuerst die Allokationen und Deprovisionierung CIDRs aus einem Pool freigeben, bevor Sie den Pool löschen können.

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

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 die folgenden AWS CLI Befehle, um einen Pool zu löschen:

1. Pools anzeigen und eine IPAM-Pool-ID abrufen: describe-ipam-pools

2. Einen Pool löschen: delete-ipam-pool
3. Sehen Sie sich Ihre Pools an: describe-ipam-pools

Um einen neuen Pool zu erstellen, siehe Erstellen Sie einen Pool auf oberster Ebene IPv4 .

Einen Bereich löschen

Sie können einen IPAM-Bereich löschen, wenn er seinen Zweck nicht mehr erfüllt, z. B. wenn Sie Ihr Netzwerk umstrukturieren, Regionen konsolidieren oder Ihre IP-Adresszuweisung anpassen. Das Löschen ungenutzter Bereiche kann dazu beitragen, Ihre IPAM-Konfiguration zu rationalisieren und Ihre IP-Adressverwaltung innerhalb von AWS zu optimieren.

> **Note**
>
> 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 die folgenden AWS CLI Befehle, um einen Bereich zu löschen:

1. Bereiche anzeigen: describe-ipam-scopes
2. Löschen Sie einen Bereich: 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.

Deprovisionierung CIDRs aus einem Pool

Sie können die Bereitstellung eines Pool-CIDR aufheben, um IP-Adressraum freizugeben, die IP-Adressverwaltung zu vereinfachen, sich auf Netzwerkänderungen vorzubereiten oder Compliance-Anforderungen zu erfüllen. Die Aufhebung der Bereitstellung eines Pool-CIDR ermöglicht eine bessere Kontrolle und Optimierung Ihrer IP-Adressenzuweisungen innerhalb von IPAM und stellt gleichzeitig sicher, dass ungenutzte IP-Bereiche zurückgewonnen und für die zukünftige Nutzung verfügbar gemacht werden. Sie können die Bereitstellung des CIDR nicht aufheben, wenn der Pool Zuweisungen enthält. Um Zuweisungen zu entfernen, siehe the section called “Eine Zuweisung freigeben”.

Folgen Sie den Schritten in diesem Abschnitt, um die Bereitstellung CIDRs aus einem IPAM-Pool aufzuheben. Wenn Sie die Bereitstellung aller Pools aufheben CIDRs, 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.

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 Bereitstellung CIDRs Sie aufheben möchten.
5. Wählen Sie die Registerkarte CIDRs aus.
6. Wählen Sie einen oder mehrere aus CIDRs und wählen Sie CIDRsDeprovision 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, um die Bereitstellung eines Pool-CIDR aufzuheben:

1. Holen Sie sich eine IPAM-Pool-ID: describe-ipam-pools
2. Ihre aktuelle Version CIDRs für den Pool anzeigen: get-ipam-pool-cidrs
3. Deprovisionierung CIDRs: deprovision-ipam-pool-cidr
4. Sehen Sie sich Ihr aktualisiertes CIDRs an: get-ipam-pool-cidrs

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

Bearbeiten eines IPAM-Pools

Sie können einen Pool bearbeiten, um eine der folgenden Aktionen durchzuführen:

- Ändern der Zuteilungsregeln für den Pool. Weitere Informationen zu Zuweisungsregeln finden Sie unter Erstellen Sie einen Pool auf oberster Ebene IPv4 .
- Ändern des Namens, der Beschreibung oder anderer Metadaten des Pools, um die Organisation und Sichtbarkeit innerhalb von IPAM zu verbessern
- Ändern von Pool-Optionen wie den automatischen Import erkannter Ressourcen, um die automatisierte IP-Adressverwaltung von IPAM zu optimieren.

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

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 Sie einen Pool auf oberster Ebene IPv4 .
7. Wählen Sie Aktualisieren.

Command line

Verwenden Sie die folgenden AWS CLI Befehle, um einen Pool zu bearbeiten:

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

Kostenverteilung aktivieren

Wenn Sie die Kostenverteilung aktivieren, verteilen Sie die Gebühren für aktive IP-Adressen auf die Konten, die die IP-Adressen verwenden, und nicht auf den IPAM-Besitzer. Dies ist nützlich für große Organisationen, in denen der delegierte IPAM-Administrator die IP-Adressen zentral mithilfe von IPAM verwaltet und jedes Konto für seine eigene Nutzung verantwortlich ist, sodass keine manuellen Abrechnungsberechnungen erforderlich sind.

Die Option zur Kostenverteilung ist verfügbar, wenn Sie ein IPAM erstellen oder ein IPAM im Messmodus ändern, wobei:

- IPAM-Besitzer (Standard): Dem AWS Konto, dem das IPAM gehört, werden für alle aktiven IP-Adressen, die in IPAM verwaltet werden, Gebühren berechnet.
- Besitzer der Ressource: Dem AWS Konto, dem die IP-Adresse gehört, wird die aktive IP-Adresse in Rechnung gestellt.

Voraussetzungen

- Ihr IPAM muss in AWS Organizations integriert sein.
- Das IPAM muss vom delegierten IPAM-Administrator in Ihrer Organisation erstellt worden sein. AWS
- Die Heimatregion des IPAM muss eine Region sein, die standardmäßig aktiviert ist. Es kann sich nicht um eine Opt-in-Region handeln.

Wie funktioniert das Aufladen

- Sie können zwar die Gebühren für IP-Adressen innerhalb einer Organisation verteilen, aber alle IPAM-Gebühren werden über die konsolidierte Abrechnung der Organisation auf das Zahlerkonto der AWS Organizations konsolidiert.
- Wenn die Kostenverteilung aktiviert ist, können die Mitgliedskonten der Organisation weiterhin ihre individuelle IPAM-Nutzung und die Gebühren in ihren Kontorechnungen einsehen.
- Der IPAM-ARN erscheint auf den einzelnen Kontorechnungen, wenn die Kostenverteilung aktiviert ist, sodass Ressourcenbesitzer ihre aktive IPAM-IP-Nutzung verfolgen können. Wenn Sie diese Option verwenden AWS Data Exports, werden die IPAM-Gebühren zusammen mit dem zugehörigen IPAM-ARN sowohl in konsolidierten als auch in individuellen Kontorechnungen angezeigt.
- Nur Konten innerhalb der Organisation des delegierten Administrators können Gebühren für die Ressourcen erhalten, deren Eigentümer sie sind. Kosten für IP-Adressen außerhalb der Organisation werden dem IPAM-Besitzer in Rechnung gestellt.

Zeitliche Einschränkungen

- Sie haben 24 Stunden Zeit, sich abzumelden, nachdem Sie die Kostenverteilung aktiviert haben. Nach 24 Stunden können Sie die Einstellung 7 Tage lang nicht ändern. Nach 7 Tagen können Sie die Kostenverteilung deaktivieren.

Bereitstellung von privater IPv6 GUA aktivieren CIDRs

Wenn Sie möchten, dass Ihre privaten Netzwerke den Datenverkehr von diesen Adressen ins Internet weiterleiten, können Sie einen privaten IPv6 ULA- oder GUA-Bereich für einen IPAM-Pool in einem privaten Bereich bereitstellen. IPv6

Wichtige Informationen IPv6 zur privaten Adressierung finden Sie unter Private IPv6 Adressen im Amazon VPC-Benutzerhandbuch.

Es gibt zwei Arten von privaten IPv6 Adressen:

- IPv6 ULA-Bereiche: IPv6 Adressen wie in definiert RFC4193. Diese Adressbereiche beginnen immer mit „fc“ oder „fd“, wodurch sie leicht identifizierbar sind. Gültiger IPv6 ULA-Speicherplatz ist alles unter fd00: :/8, das sich nicht mit dem von Amazon reservierten Bereich fd00: :/16 überschneidet.
- IPv6 GUA-Bereiche: Adressen wie in definiert. IPv6 RFC3587 Die Option, IPv6 GUA-Bereiche als private IPv6 Adressen zu verwenden, ist standardmäßig deaktiviert und muss aktiviert werden, bevor Sie sie verwenden können.

Um IPv6 ULA-Adressbereiche zu verwenden, wählen Sie die IPv6 Option, wenn Sie einen CIDR für einen IPAM-Pool bereitstellen und den IPv6 ULA-Bereich eingeben. Um Ihre eigenen IPv6 GUA-Bereiche als private IPv6 Adressen zu verwenden, müssen Sie jedoch zuerst die Schritte in diesem Abschnitt ausführen. Die Option ist standardmäßig deaktiviert.

> **Note**
>
> - Wenn Sie private IPv6 GUA-Bereiche verwenden, setzen wir voraus, dass Sie IPv6 GUA-Bereiche verwenden, die Ihnen gehören.
> - IPAM erkennt Ressourcen mit IPv6 ULA- und GUA-Adressen und überwacht Pools auf sich überschneidende IPv6 ULA- und GUA-Adressräume.
> - Wenn Sie von einer Ressource mit einer privaten IPv6 Adresse aus eine Verbindung zum Internet herstellen möchten, können Sie dies tun. Sie müssen den Datenverkehr jedoch über eine Ressource in einem anderen Subnetz mit einer öffentlichen IPv6 Adresse weiterleiten, um dies zu erreichen.
> - Wenn Sie einer VPC einen privaten IPv6 GUA-Bereich zugewiesen haben, können Sie keinen öffentlichen IPv6 GUA-Bereich verwenden, der sich mit dem privaten IPv6 GUA-Bereich in derselben VPC überschneidet.

- Die Kommunikation zwischen Ressourcen mit privaten IPv6 ULA- und GUA-Adressbereichen wird unterstützt (z. B. über Direct Connect). VPC-Peering, Transit-Gateway oder VPN-Verbindungen).
- Ein privater IPv6 GUA-Bereich kann nicht in einen öffentlich IPv6 beworbenen GUA-Bereich umgewandelt werden.

AWS Management Console

Um die Bereitstellung einer privaten GUA zu aktivieren IPv6 CIDRs

1. Öffnen Sie die IPAM-Konsole unter. https://console.aws.amazon.com/ipam/
2. Wählen Sie im Navigationsbereich IPAMs aus.
3. Wählen Sie Ihr IPAM und dann Aktionen > Bearbeiten aus.
4. Wählen Sie unter Private IPv6 GUA CIDRs die Option Bereitstellung von GUA-CIDR-Speicherplatz in privaten IPv6 IPAM-Pools aktivieren aus.
5. Wählen Sie Änderungen speichern.

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 die Bereitstellung einer privaten IPv6 GUA CIDRs zu aktivieren:

1. Aktuelle Informationen IPAMs mit describe-ipams anzeigen
2. Ändern Sie das IPAM mit modify-ipam und fügen Sie die Option zu `enable-private-gua` hinzu.

Sobald Sie die Option zur Bereitstellung einer privaten IPv6 GUA aktiviert haben CIDRs, können Sie eine private GUA-CIDR für einen Pool bereitstellen. IPv6 Weitere Informationen finden Sie unter Bereitstellung CIDRs für einen Pool.

Erzwingen Sie die IPAM-Verwendung für die VPC-Erstellung mit SCPs

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

In diesem Abschnitt wird beschrieben, wie Sie eine Dienststeuerungsrichtlinie erstellen AWS Organizations , nach der Mitglieder in Ihrer Organisation IPAM verwenden müssen, wenn sie eine VPC erstellen. Dienststeuerungsrichtlinien (SCPs) sind eine Art von Organisationsrichtlinie, mit der Sie Berechtigungen in Ihrer Organisation verwalten können. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.

Erzwingen Sie IPAM bei der Erstellung VPCs

Folgen Sie den Schritten in diesem Abschnitt, um zu verlangen, dass Mitglieder in Ihrer Organisation beim Erstellen IPAM verwenden. VPCs

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

1. Folgen Sie den Schritten unter Erstellen einer Dienststeuerungsrichtlinie im AWS Organizations Benutzerhandbuch und geben Sie den folgenden Text in den JSON-Editor ein:

   JSON

```
{
    "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 Richtlinien anhängen und Richtlinien trennen im AWS Organizations Benutzerhandbuch.

Erzwingen Sie bei der Erstellung einen IPAM-Pool VPCs

Folgen Sie den Schritten in diesem Abschnitt, um zu verlangen, dass Mitglieder in Ihrer Organisation bei der Erstellung einen bestimmten IPAM-Pool verwenden. VPCs

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

1. Folgen Sie den Schritten unter Erstellen einer Dienststeuerungsrichtlinie im AWS Organizations Benutzerhandbuch und geben Sie den folgenden Text in den JSON-Editor ein:

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Deny",
        "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
        "Resource": "arn:aws:ec2:*:*:vpc/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Ipv4IpamPoolId": "ipam-pool-0123456789abcdefg"
            }
          }
    }]
}
```

2. Ändern Sie den `ipam-pool-0123456789abcdefg` Beispielwert in 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 Richtlinien anhängen und Richtlinien trennen im AWS Organizations Benutzerhandbuch.

Erzwingen Sie IPAM für alle außer einer bestimmten Liste von OUs

Folgen Sie den Schritten in diesem Abschnitt, um IPAM für alle außer einer bestimmten Liste von Organisationseinheiten durchzusetzen ()OUs. Die in diesem Abschnitt beschriebene Richtlinie erfordert OUs in der Organisation, mit Ausnahme der OUs , die Sie in angeben, dass IPAM `aws:PrincipalOrgPaths` zum Erstellen und Erweitern verwendet werden soll. VPCs Die aufgelisteten OUs können entweder IPAM beim Erstellen verwenden VPCs oder einen IP-Adressbereich manuell angeben.

Um ein SCP zu erstellen und IPAM für alle außer einer bestimmten Liste von durchzusetzen OUs

1. Folgen Sie den Schritten unter Erstellen einer Dienststeuerungsrichtlinie im AWS Organizations Benutzerhandbuch und geben Sie den folgenden Text in den JSON-Editor ein:

   JSON

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

2. Entfernen Sie die Beispielwerte (likeo-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/) und fügen Sie die AWS Organisations-Entitätspfade der Entitäten hinzu, für OUs die Sie die Option (aber nicht erforderlich) zur Verwendung von IPAM haben möchten.

Weitere Informationen zum Entitätspfad finden Sie unter AWS Understand the Organizations entity path und aws: PrincipalOrgPaths im IAM-Benutzerhandbuch.

3. Fügen Sie die Richtlinie zum Organisations-Root hinzu. Weitere Informationen finden Sie unter Richtlinien anhängen und Richtlinien trennen im AWS Organizations Benutzerhandbuch.

Ausschließen von Organisationseinheiten von IPAM

Wenn Ihr IPAM in AWS Organizations integriert ist, können Sie eine Organisationseinheit (OU) von der Verwaltung durch IPAM ausschließen. Wenn Sie eine Organisationseinheit ausschließen, verwaltet IPAM die IP-Adressen der Konten in dieser Organisationseinheit nicht. Dieses Feature bietet Ihnen mehr Flexibilität bei der Verwendung von IPAM.

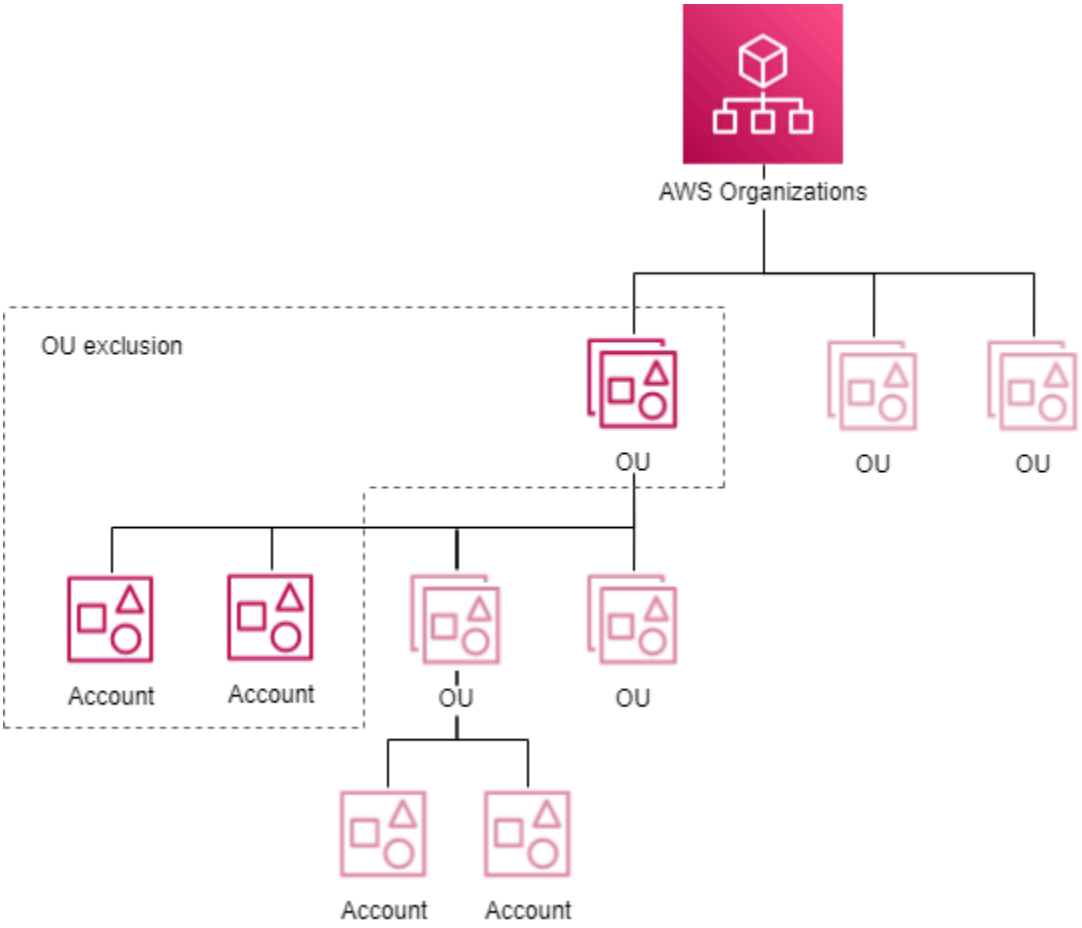
Sie können OU-Ausschlüsse auf folgende Weise verwenden:

- Aktivieren Sie IPAM für bestimmte Teile Ihres Unternehmens: Wenn Sie mehrere Geschäftsbereiche oder Tochtergesellschaften in AWS Organizations haben, können Sie IPAM jetzt nur für die Bereiche nutzen, die es benötigen.
- Halten Sie Ihre Sandbox-Konten getrennt: Sie können Ihre Sandbox-Konten von IPAM ausschließen und sich nur auf die Konten konzentrieren, die für Ihr IP-Management wirklich wichtig sind.

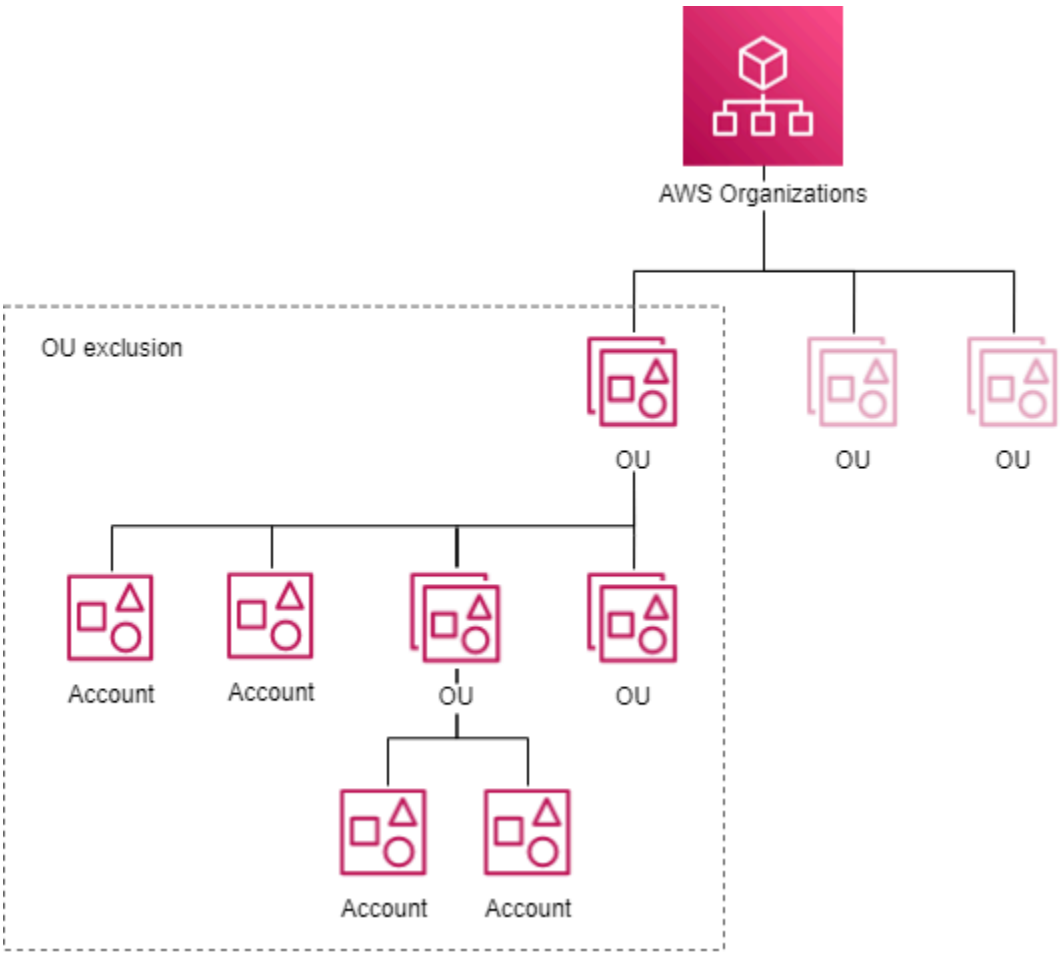
So funktionieren OU-Ausschlüsse

Die Diagramme in diesem Abschnitt zeigen zwei Anwendungsfälle für das Hinzufügen von OU-Ausschlüssen in IPAM.

Das erste Diagramm zeigt die Auswirkungen des Hinzufügens eines Ausschlusses einer Organisationseinheit (OU) nur auf eine übergeordnete OU. Infolgedessen verwaltet IPAM die IP-Adressen in Konten in der übergeordneten OU nicht. IPAM verwaltet die IP-Adressen der Konten in den anderen Konten OUs außerhalb des Ausschlusses.



Das zweite Diagramm zeigt, wie sich das Hinzufügen eines Ausschlusses aus Organisationseinheiten (OU) auf eine übergeordnete Organisationseinheit und alle OUs untergeordneten Einheiten auswirkt. Daher verwaltet IPAM nicht die IP-Adressen in Konten in der übergeordneten Organisationseinheit oder in Konten OUs untergeordneter Organisationen. IPAM verwaltet die IP-Adressen in Konten OUs außerhalb der Ausnahmeregelung.



Hinzufügen oder Entfernen von OU-Ausschlüssen

Führen Sie die Schritte in diesem Abschnitt aus, um OU-Ausschlüsse hinzuzufügen oder zu entfernen.

> **Note**
>
> - Das delegierte IPAM-Administratorkonto wird nicht ausgeschlossen, auch wenn es sich in einer ausgeschlossenen OU befindet.
> - Ihr IPAM muss integriert sein AWS Organizations , um einen OU-Ausschluss hinzuzufügen. Die Organisation muss etwas OUs enthalten.
> - Sie müssen der delegierte IPAM-Administrator sein, um OU-Ausschlüsse anzuzeigen, hinzuzufügen oder zu entfernen.
> - Es dauert einige Zeit, bis IPAM kürzlich erstellte Organisationseinheiten erkennt.

- Es gibt ein Standardkontingent für die Anzahl der Ausschlüsse, die Sie pro Ressourcenerkennung hinzufügen können. Weitere Informationen finden Sie unter Ausschlüsse von Organisationseinheiten pro Ressourcenerkennung in Kontingente für Ihr IPAM.
- Wenn Sie eine Resource Discovery mit einem anderen Konto teilen, kann dieses Konto die zugehörigen OU-Ausschlüsse sehen, die Informationen wie die Organisations- und Root-ID sowie die Organisationseinheit IDs der Organisation des Besitzers der Resource Discovery enthalten.

AWS Management Console

So fügen Sie OU-Ausschlüsse hinzu oder entfernen sie

1. Öffnen Sie die IPAM-Konsole unter. https://console.aws.amazon.com/ipam/
2. Wählen Sie im Navigationsbereich Ressourcenergebnisse aus.
3. Wählen Sie Ihre standardmäßige Ressourcenerkennung aus.
4. Wählen Sie Edit (Bearbeiten) aus.
5. Gehen Sie unter Ausschlüsse von Organisationseinheiten wie folgt vor:
   - So fügen Sie einen OU-Ausschluss hinzu:
     - Wenn Sie die Organisationseinheit und ihr gesamtes OUs untergeordnetes Element ausschließen möchten:
       - Suchen Sie die OU in der Tabelle und aktivieren Sie das Kontrollkästchen. Alle untergeordneten OUs Elemente werden automatisch ausgewählt.
     - Wenn Sie nur übergeordnete OU-Konten ausschließen möchten:
       - Suchen Sie die OU in der Tabelle und aktivieren Sie das Kontrollkästchen. Alle Kinder OUs werden automatisch ausgewählt. Alle Kinder OUs abwählen.
     - Alternativ können Sie die Spalte Aktionen verwenden, um nur eine übergeordnete Organisationseinheit oder ein Elternteil und ein Kind OUs auszuwählen:
       - Alle Kinder auswählen OUs: Schließt jedes Kind OUs in den Ausschluss ein. Nach der Auswahl einer OU wird die OU auf dem Bildschirm hinzugefügt. Jede OU enthält die ID und den Pfad der Entität des OU-Ausschlusses.

- Nur diese OU auswählen: Beziehen Sie nur diese OU in den Ausschluss ein. Nach der Auswahl einer OU wird die OU auf dem Bildschirm hinzugefügt. Jede OU enthält die ID und den Pfad der Entität des OU-Ausschlusses.
- OU-Entitätspfad kopieren: Kopieren Sie den AWS Organizations Entitätspfad, der nach Bedarf verwendet werden soll.

- Wenn Sie den Entitätspfad der AWS Organizations bereits kennen oder ihn erstellen möchten:
  - Wählen Sie Ausschluss der Organisationseinheit eingeben aus und geben Sie den Pfad der Entität des OU-Ausschlusses ein. Erstellen Sie den Pfad für die OU (s) mithilfe von AWS Organizations, die durch a IDs getrennt sind`/`. Schließen Sie alle untergeordneten OUs Elemente ein, indem Sie den Pfad mit beenden`/*`.
    - Beispiel 1
      - Pfad zu einer untergeordneten OU: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscccccc/ou-jkl0-awsdddddd/`
      - In diesem Beispiel `o-a1b2c3d4e5` ist es die Organisations-ID, `r-f6g7h8i9j0example` ist die Root-ID, `ou-ghi0-awscccccc` ist eine OU-ID und `ou-jkl0-awsdddddd` ist eine untergeordnete OU-ID.
      - IPAM verwaltet die IP-Adressen der Konten in der untergeordneten OU nicht.
    - Beispiel 2
      - Pfad, in dem alle untergeordneten Elemente Teil des Ausschlusses sein OUs werden: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscccccc/*`
      - In diesem Beispiel verwaltet IPAM nicht die IP-Adressen in Konten in der Organisationseinheit (`ou-ghi0-awscccccc`) oder in Konten in Konten in Konten OUs , die der Organisationseinheit untergeordnet sind.
- So entfernen Sie einen OU-Ausschluss:
  - Wählen Sie das X neben einer OU aus, die bereits hinzugefügt wurde. Die ID `/*` hinter der Organisationseinheit gibt an, dass es sich um eine übergeordnete Organisationseinheit OUs handelt und dass das untergeordnete Unternehmen Teil des Ausschlusses der Organisationseinheit ist.

6. Wählen Sie Änderungen speichern.

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. Sehen Sie sich die Details zur Ressourcenerkennung an, um die ID der Standard-Ressourcenerkennung für den nächsten Schritt mit abzurufen describe-ipam-resource-discoveries.

   Eingabe:

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

   Ausgabe:

   ```
   {

       "IpamResourceDiscoveries": [

           {

               "OwnerId": "111122223333",

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

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

               "OperatingRegions": [

                   {

                       "RegionName": "us-east-1"

                   },

                   {

                       "RegionName": "us-west-1"
   ```

```
                },
                {
                    "RegionName": "us-west-2"
                }
            ],
            "IsDefault": true,
            "State": "modify-complete",
            "Tags": []
        }
    ]
}
```

2. Fügen Sie mit den `--remove-organizational-unit-exclusions` Optionen oder oder einen Ausschluss einer Organisationseinheit zu einer modify-ipam-resource-discoveryRessourcensuche hinzu `--add-organizational-unit-exclusions` oder entfernen Sie ihn. Sie müssen einen Entitätspfad für AWS Organizations eingeben. Erstellen Sie den Pfad für die OU (s) mithilfe von AWS Organizations, die durch a IDs getrennt sind`/`. Schließen Sie alle untergeordneten OUs Elemente ein, indem Sie den Pfad mit beenden`/*`. Sie können denselben Entitätspfad nicht mehr als einmal in die Parameter zum Hinzufügen oder Entfernen aufnehmen.

   - Beispiel 1
     - Pfad zu einer untergeordneten OU: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
     - In diesem Beispiel `o-a1b2c3d4e5` ist es die Organisations-ID, `r-f6g7h8i9j0example` ist die Root-ID, `ou-ghi0-awsccccc` ist eine OU-ID und `ou-jkl0-awsddddd` ist eine untergeordnete OU-ID.
     - IPAM verwaltet die IP-Adressen der Konten in der untergeordneten OU nicht.
   - Beispiel 2

- Pfad, in dem alle untergeordneten Elemente Teil des Ausschlusses sein OUs werden: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
- In diesem Beispiel verwaltet IPAM nicht die IP-Adressen in Konten in der Organisationseinheit (`ou-ghi0-awsccccc`) oder in Konten in Konten in Konten OUs , die der Organisationseinheit untergeordnet sind.

> **Note**
>
> Der daraus resultierende Satz von Ausschlüssen darf sich nicht „überschneiden“, d. h. zwei oder mehr OU-Ausschlüsse dürfen dieselbe Organisationseinheit nicht ausschließen.
> Beispiel für sich nicht überschneidende Entitätspfade:
>
> - Pfad 1 ="o-1/r-1/ou-1/“
> - Pfad 2 ="o-1/r-1/ou-1/ou-2/“
>
> Diese Pfade überschneiden sich nicht, da Pfad 1 nur die Konten unter ou-1 und Pfad 2 nur Konten unter ou-2 ausschließt.
> Beispiel für überlappende Entitätspfade:
>
> - Pfad 1 ="o-1/r-1/ou-1/*“
> - Pfad 2 ="o-1/r-1/ou-1/ou-2/“
>
> Diese Pfade überschneiden sich, weil Pfad 1 sowohl für „o-1/r-1/ou-1/“ als auch für „o-1/r-1/ou-1/ou-2/“ steht und „o-1/r-1/ou-1/ou-2/“ sich mit Pfad 2 überschneidet.

Eingabe:

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

Ausgabe:

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

Ändern einer IPAM-Stufe

IPAM bietet zwei Stufen: das kostenlose Kontingent und das erweiterte Kontingent. Der Wechsel zur Stufe „Erweitert“ von Amazon VPC IP Address Manager bietet eine differenziertere Kontrolle über Ihre IP-Adressverwaltung. Dies kann bei zunehmender Komplexität Ihres Netzwerks von Vorteil sein, da Sie so Ihren IP-Adressraum besser optimieren und verwalten können. 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“.

> **Note**
>
> 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 IPAMs aus.
3. Wählen Sie im Inhaltsbereich Ihr IPAM aus.
4. Wählen Sie Actions (Aktionen) und Edit (Bearbeiten).

> **Note**
>
> Wenn Sie das kostenlose Kontingent nutzen, sehen Sie, dass Ihre geschätzte Gesamtzahl der aktiven IPAM-IP-Adressen... .
> Die Gesamtzahl der aktiven IP-Adressen ist die Anzahl der aktiven IP-Adressen in Ihrem IPAM, die Ihnen in Rechnung gestellt würden, wenn Sie vom kostenlosen Tarif zum erweiterten Tarif wechseln würden. Eine aktive IP-Adresse ist definiert als eine IP-Adresse oder ein Präfix, das einem Elastic Network Interface (ENI) zugeordnet ist, das an eine Ressource wie eine EC2 Instance angehängt ist.
>
> - Diese Metrik ist nur für Kunden im kostenlosen Kontingent verfügbar.
> - Wenn Ihr IPAM in AWS Organizations integriert ist, deckt die Anzahl der aktiven IP-Adressen alle Unternehmenskonten ab.
> - Sie können keine Aufschlüsselung der Anzahl der aktiven IP-Adressen nach IP-Typ (public/private) or class (IPv4/IPv6) anzeigen.
> - IPAM zählt nur von Konten, die ENIs sich im Besitz IPs von überwachten Konten befinden. Die Zählung kann für freigegebene Subnetze ungenau sein. IP-Adressen werden ausgeschlossen, wenn der Subnetz- oder ENI-Eigentümer nicht von IPAM erfasst wird.

5. Wählen Sie die IPAM-Stufe aus, die Sie für den IPAM verwenden möchten.
6. Wählen Sie Änderungen speichern.

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. Aktuelle Version anzeigen IPAMs: describe-ipams
2. Ändern Sie die IPAM-Stufe: modify-ipam
3. Sehen Sie sich Ihre aktualisierten Versionen an: describe-ipams IPAMs

Ändern der IPAM-Betriebsregionen

Betriebsregionen sind AWS Regionen, in denen das IPAM IP-Adressen CIDRs verwalten darf. IPAM erkennt und überwacht nur Ressourcen in den AWS Regionen, die Sie als Betriebsregionen auswählen.

Wenn Sie einem IPAM eine Betriebsregion hinzufügen, können Sie den IP-Adressraum über mehrere Regionen hinweg verwalten. AWS Dies kann die Nutzung von IP-Adressen verbessern, eine regionale Segmentierung ermöglichen und eine geografisch verteilte Infrastruktur unterstützen. Die Erweiterung des regionalen Geltungsbereichs von IPAM bietet mehr Flexibilität und Kontrolle über Ihre gesamte IP-Adressverwaltung.

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 IPAMs aus.
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 Änderungen speichern.

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. Aktuell anzeigen IPAMs: describe-ipams
2. Hinzufügen oder Entfernen der IPAM-Betriebsregionen: modify-ipam
3. Sehen Sie sich Ihre aktualisierten: describe-ipams an IPAMs

Bereitstellung CIDRs für einen Pool

Folgen Sie den Schritten in diesem Abschnitt, um die Bereitstellung CIDRs für einen Pool durchzuführen. Wenn Sie bei der Erstellung des Pools bereits einen CIDR bereitgestellt haben, müssen Sie möglicherweise weitere bereitstellen, CIDRs wenn ein Pool fast vollständig zugewiesen ist. 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

Um eine Bereitstellung für einen Pool durchzuführen CIDRs

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. Wählen Sie „Aktionen“ > „Bereitstellung CIDRs“.
6. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie ein CIDR für einen Pool im öffentlichen Bereich bereitstellen, geben Sie die Netzmaske ein.
   - Wenn Sie einen CIDR für einen IPv4 Pool im privaten Bereich bereitstellen, geben Sie den CIDR ein.
   - Wenn Sie einen CIDR für einen IPv6 Pool im privaten Bereich bereitstellen, beachten Sie Folgendes:
     - Wichtige Informationen IPv6 zur privaten Adressierung finden Sie unter Private IPv6 Adressen im Amazon VPC-Benutzerhandbuch.
     - Um einen privaten IPv6 ULA-Bereich zu verwenden, wählen Sie unter CIDRsZur Bereitstellung die Option ULA-CIDR nach Netzmaske hinzufügen und wählen Sie eine Netzmaskengröße aus oder wählen Sie Private IPv6 CIDR eingeben und geben Sie einen ULA-Bereich ein. Gültige Bereiche für private IPv6 ULA sind /9 bis /60, beginnend mit fd80: :/9.
     - Um einen privaten IPv6 GUA-Bereich zu verwenden, müssen Sie zuerst die Option auf Ihrem IPAM aktiviert haben (siehe). Bereitstellung von privater IPv6 GUA aktivieren CIDRs Nachdem Sie private IPv6 GUA aktiviert haben CIDRs, geben Sie eine IPv6 GUA in Input private IPv6 CIDR ein.

> **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 für einen Pool innerhalb eines Pools bereitstellen CIDRs , muss der CIDR-Speicherplatz, den Sie bereitstellen möchten, im Pool verfügbar sein.

7. Wählen Sie Bereitstellung.
8. Sie können den CIDR in IPAM anzeigen, indem Sie im Navigationsbereich Pools auswählen, einen Pool auswählen und die CIDRs Registerkarte für den Pool aufrufen.

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 die Bereitstellung CIDRs für einen Pool durchzuführen:

1. Rufen Sie die ID eines IPAM-Pools ab: describe-ipam-pools
2. Holen Sie sich CIDRs die, die für den Pool bereitgestellt wurden: get-ipam-pool-cidrs
3. Stellen Sie dem Pool ein neues CIDR bereit: provision-ipam-pool-cidr
4. Holen Sie sich die CIDRs , die für den Pool bereitgestellt wurden, und sehen Sie sich das neue CIDR an: get-ipam-pool-cidrs

VPC CIDRs zwischen Bereichen verschieben

Wenn Sie CIDRs zwischen Bereichen wechseln, können Sie die IP-Adresszuweisung optimieren, nach Regionen organisieren, Probleme voneinander trennen, die Einhaltung von Vorschriften durchsetzen und sich an Änderungen der Infrastruktur anpassen. Diese Flexibilität hilft Ihnen, Ihren IP-Adressraum effizient zu verwalten, wenn sich Ihre Workloads weiterentwickeln.

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 eine VPC CIDR verschieben, wird auch das Subnetz der VPC CIDRs automatisch verschoben.

- Sie können VPC nur CIDRs von einem privaten Bereich in einen anderen verschieben. Sie können VPC nicht CIDRs aus einem öffentlichen Bereich in einen privaten Bereich oder von 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 eine der der Ressource CIDRs zugewiesenen Ressourcen aus und wählen Sie Aktionen > CIDR in einen anderen Bereich verschieben.
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 eine VPC-CIDR zu verschieben:

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

Eine Zuweisung freigeben

Wenn Sie vorhaben, einen Pool zu löschen, müssen Sie möglicherweise eine Pool-Zuweisung freigeben. In der Zuweisung ist eine CIDR-Zuweisung von einem IPAM-Pool zu einer anderen Ressource oder einem IPAM-Pool.

Sie können Pools nicht löschen, wenn die Pools CIDRs bereitgestellt wurden, und Sie können die Bereitstellung nicht aufheben, CIDRs wenn sie CIDRs Ressourcen zugewiesen sind.

Note

- Um eine manuelle Zuweisung freizugeben, führen Sie die Schritte in diesem Abschnitt aus oder rufen Sie die API aufReleaseIpamPoolAllocation .
- Um eine Zuweisung in einem privaten Bereich freizugeben, müssen Sie die Ressource-CIDR ignorieren oder löschen. Weitere Informationen finden Sie unter Ändern Sie den 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 öffentliche Ressourcen nicht ignorieren CIDRs. 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. Wenn Sie IPAM in der Stufe „Erweitert“ verwenden, dauert es einige Minuten, bis das CIDR für künftige Zuweisungen verfügbar ist. Wenn Sie IPAM im kostenlosen Kontingent verwenden, dauert es bis zu 48 Stunden, bis das CIDR für künftige Zuweisungen 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 Pool-Zuweisung. IPv4
   - subnet: Eine Subnetzzuweisung.
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, um eine Poolzuweisung freizugeben:

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. Geben Sie eine Zuordnung frei: release-ipam-pool-allocation
4. Sehen Sie sich Ihre aktualisierten Zuweisungen an: get-ipam-pool-allocations

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

Teilen Sie einen IPAM-Pool mithilfe von RAM AWS

Folgen Sie den Schritten in diesem Abschnitt, um einen IPAM-Pool mit AWS Resource Access Manager (RAM) gemeinsam zu nutzen. Wenn Sie einen IPAM-Pool mit RAM gemeinsam nutzen, können „Principals“ AWS Ressourcen CIDRs aus dem Pool zuweisen, z. B. aus ihren jeweiligen VPCs Konten. Ein Principal ist ein Konzept in RAM, das jedes AWS Konto, jede IAM-Rolle oder jede Organisationseinheit in AWS Organizations bezeichnet. Weitere Informationen finden Sie im AWS RAM-Benutzerhandbuch unter Gemeinsame Nutzung Ihrer AWS Ressourcen.

> **Note**
>
> - Sie können einen IPAM-Pool nur mit AWS RAM teilen, wenn Sie IPAM in Organizations integriert haben. AWS Weitere Informationen finden Sie unter Integrieren Sie IPAM mit Konten in einer Organisation AWS. Sie können einen IPAM-Pool nicht mit AWS RAM gemeinsam nutzen, wenn Sie ein IPAM-Benutzer mit einem einzigen Konto sind.
> - Sie müssen die gemeinsame Nutzung von Ressourcen mit AWS Organizations im AWS RAM aktivieren. Weitere Informationen finden Sie unter Aktivieren der gemeinsamen Nutzung von Ressourcen innerhalb von AWS Organizations im AWS RAM-Benutzerhandbuch.
> - RAM-Sharing 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.
- Sie können IPAM-Pools zwar mit jedem AWS Konto außerhalb einer AWS Organisation gemeinsam nutzen, aber IPAM überwacht die IP-Adressen in Konten außerhalb der Organisation nur, wenn der Kontoinhaber den Prozess durchlaufen hat, seine Ressourcenerkennung mit dem delegierten IPAM-Administrator zu teilen, wie unter beschrieben. Integrieren von IPAM mit Konten außerhalb Ihrer Organisation

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 im 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 Weiter.
10. Wählen Sie eine der Berechtigungen für die Ressourcenfreigabe aus:

    - AWSRAMDefaultPermissionsIpamPool: Wählen Sie diese Berechtigung, um den Prinzipalen zu ermöglichen, die Zuordnungen CIDRs und die Zuweisungen im gemeinsam genutzten IPAM-Pool einzusehen und sie im Pool zuzuweisen/freizugeben. CIDRs
    - AWSRAMPermissionIpamPoolByoipCidrImport: Wählen Sie diese Berechtigung, um Prinzipalen zu erlauben, BYOIP in den gemeinsam genutzten IPAM-Pool zu importieren.

CIDRs Sie benötigen diese Berechtigung nur, wenn Sie bereits über BYOIP verfügen und diese in IPAM importieren CIDRs und für Prinzipale freigeben möchten. Weitere Informationen zu CIDRs BYOIP to IPAM finden Sie unter. Tutorial: Eine BYOIP IPv4 CIDR auf IPAM übertragen

11. Wählen Sie die Hauptbenutzer aus, die auf diese Ressource zugreifen dürfen. Wenn Prinzipale vorhandenes BYOIP in diesen gemeinsam genutzten IPAM-Pool importieren CIDRs , fügen Sie das BYOIP-CIDR-Besitzerkonto als Principal 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, um einen IPAM-Pool mithilfe von RAM gemeinsam zu nutzen:

1. Holen Sie sich den ARN des IPAM: describe-ipam-pools
2. Erstellen Sie die Ressourcenfreigabe: create-resource-share
3. Den Ressourcenanteil anzeigen: get-resource-shares

Durch die Erstellung der Ressourcenfreigabe im RAM können nun andere Prinzipale Ressourcen mithilfe des IPAM-Pool CIDRs zuweisen. 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 gemeinsam genutzten IPAM-Pool finden Sie unter Create a VPC im Amazon VPC-Benutzerhandbuch.

Arbeiten mit Ressourcenergebnissen

Eine Ressourcenerkennung ist eine IPAM-Komponente, die es IPAM ermöglicht, Ressourcen zu verwalten und zu überwachen, die dem Konto gehören, das Ressourcenerkennung besitzt. Auf diese Weise kann IPAM ein up-to-date Inventar der IP-Adressnutzung in Ihren Workloads führen, was die Verwaltung und Planung von IP-Adressen erleichtert.

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.

Beachten Sie, dass dieser Abschnitt eine Gruppierung von Verfahren darstellt, die sich alle auf die Arbeit mit Ressourcenerkennungen beziehen.

Inhalt

Erstellen einer Ressourcenerkennung, um sie in ein anderes IPAM zu integrieren

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 Bezeichnung, die Sie einer AWS Ressource zuweisen. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags verwenden, um Ihre Ressourcen zu suchen und zu filtern oder Ihre AWS Kosten zu verfolgen.
6. (Optional) Fügen Sie eine Beschreibung hinzu.
7. Wählen Sie unter Betriebsregionen die AWS Regionen aus, in denen Ressourcen entdeckt werden sollen. 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 Create (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 Sie eine Ressourcenerkennung: create-ipam-resource-discovery

Anzeigen von Details der Ressourcenerkennung

Die Anzeige der Details einer Ressourcenerkennung in AWS IPAM kann wertvolle Erkenntnisse liefern, wie z. B.:

- Identifizieren der spezifischen AWS Ressourcen, die importiert wurden, und der zugehörigen IP-Adresszuweisungen.
- Überwachung des Status und des Fortschritts des Ressourcenerkennungsprozesses
- Behebung von Problemen oder Diskrepanzen zwischen IPAM und den erkannten Ressourcen
- Analyse der IP-Adressnutzung und der Trends

Diese Informationen können Ihnen helfen, Ihre IP-Adressverwaltung zu optimieren und sicherzustellen, dass IPAM und Ihre tatsächlichen Ressourcenbereitstellungen aufeinander abgestimmt sind.

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 die folgenden Ressourcentypen VPCs: Öffentliche IPv4 Pools, VPC-Subnetze und Elastic IP-Adressen.
     - Name (Ressourcen-ID) – Ressourcenerkennungs-ID.
     - IPs zugewiesen — Der Prozentsatz des genutzten IP-Adressraums. Um die Dezimalzahl in einen Prozentsatz umzurechnen, multiplizieren Sie die Dezimalzahl mit 100. Beachten Sie Folgendes:
       - Für Ressourcen, die das sind VPCs, ist dies der Prozentsatz des IP-Adressraums in der VPC, der vom CIDRs Subnetz belegt wird.
       - Bei Ressourcen, bei denen es sich um Subnetze handelt, ist dies der Prozentsatz des IPv4 Adressraums im Subnetz, der verwendet wird, wenn für das Subnetz ein IPv4 CIDR bereitgestellt wurde. Wenn für das Subnetz ein IPv6 CIDR bereitgestellt wurde, wird der Prozentsatz des IPv6 verwendeten 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-Adressraums 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.

- Entdeckte Konten: AWS Konten, die im Rahmen einer Ressourcenerkennung überwacht werden. Wenn Sie IPAM mit AWS Organizations integriert haben, sind alle Konten in der Organisation 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 Bezeichnung, die Sie einer AWS Ressource zuweisen. 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.

- Einzelheiten zur Ressourcenerkennung anzeigen: describe-ipam-resource-discoveries

Eine Ressourcenerkennung mit einem anderen AWS Konto teilen

Folgen Sie den Schritten in diesem Abschnitt, um eine Ressourcenerkennung mit anderen zu teilen AWS Resource Access Manager. Weitere Informationen dazu AWS RAM finden Sie im AWS RAM Benutzerhandbuch unter Teilen Ihrer AWS Ressourcen.

> **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 erstellen, AWS RAM um eine Ressourcensuche gemeinsam zu nutzen, müssen Sie die Ressourcenfreigabe in der Heimatregion der primären Organisation IPAM 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 eine Resource Discovery mit einem anderen Konto teilen, kann dieses Konto alle Ausschlüsse von Organisationseinheiten sehen. Diese Informationen enthalten Informationen wie die Organisations- und Root-ID sowie die Organisationseinheit IDs der Organisation des Besitzers der Resource Discovery.

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 wird geöffnet, in der Sie die Ressourcenfreigabe erstellen.
5. Wählen Sie in der AWS RAM Konsole Einstellungen aus.
6. Wählen Sie „Teilen aktivieren mit AWS Organizations“ und anschließend „Einstellungen speichern“.
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 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 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. Den Ressourcenanteil anzeigen: get-resource-shares

Zuordnung einer Ressourcenerkennung zu einem IPAM

In diesem Abschnitt wird beschrieben, wie Sie eine Ressourcenerkennung einem IPAM zuordnen. Wenn Sie eine Ressourcenerkennung mit einem IPAM verknüpfen, überwacht das IPAM alle Ressourcen CIDRs und Konten, die im Rahmen 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 IPAMs aus.
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.

- Ordnen Sie eine Ressourcenerkennung zu: associate-ipam-resource-discovery

Aufhebung der Zuordnung einer Ressourcenerkennung

In diesem Abschnitt wird beschrieben, wie Sie eine Ressourcenerkennung von einem IPAM trennen. Wenn Sie eine Ressourcenerkennung von einem IPAM trennen, 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 IPAMs aus.
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 trennen Sie die Zuordnung zu einer Ressourcenerkennung: 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

Verfolgung der IP-Adressnutzung in IPAM

Amazon VPC IP Address Manager bietet Funktionen zur Nachverfolgung der Nutzung von IP-Adressen, von denen jeder profitieren kann, der komplexe Netzwerkumgebungen verwaltet. IPAM bietet Einblick in die Zuweisung, Nutzung und Nutzungstrends von IP-Adressen in AWS. Dies hilft Ihnen, ungenutzte oder ineffizient genutzte IP-Adressen zu identifizieren, den Adressraum zu optimieren und eine mögliche Erschöpfung der IP-Adressen zu verhindern.

IPAM verfolgt die Nutzung von IP-Adressen auf CIDR-, Bereichs- und IPAM-Ebene nach und bietet detaillierte Berichte und Analysen. Dies ist nützlich für umfangreiche Bereitstellungen, Setups mit mehreren Konten und sich ändernde Netzwerkanforderungen.

Mithilfe der IPAM-Nutzungsverfolgung können Sie fundierte Entscheidungen treffen, die Verwaltung von IP-Adressen verbessern und die effiziente Nutzung von IP-Ressourcen sicherstellen.

> **Note**
>
> 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.

Inhalt

Überwachen der CIDR-Nutzung mit dem IPAM-Dashboard

Das IPAM-Dashboard in Amazon VPC IP Address Manager ermöglicht Ihnen die Überwachung der CIDR-Nutzung für mehrere wichtige Szenarien:

- Identifizieren Sie ungenutzten oder nicht ausgelasteten IP-Adressraum: Das Dashboard bietet Einblick in die CIDR-Auslastung, sodass Sie anhand der verfügbaren Kapazität ermitteln CIDRs können, die zurückgewonnen oder neu zugewiesen werden kann.
- Optimieren der Verwaltung von IP-Adressen: Indem Sie die CIDR-Nutzung genau verfolgen, können Sie fundierte Entscheidungen über die Erweiterung, Verkleinerung oder Neuzuweisung von IP-Adressblöcken treffen, um veränderten Geschäfts- und Infrastrukturanforderungen gerecht zu werden.
- Verhindern der Erschöpfung von IP-Adressen: Durch die Überwachung der CIDR-Nutzung können Sie vorhersehen, wann Sie zusätzlichen IP-Adressraum benötigen. So können Sie proaktiv planen und Serviceunterbrechungen aufgrund der Erschöpfung von IP-Adressen vermeiden.
- Sicherstellung von Compliance und Governance: Mit dem IPAM-Dashboard können Sie IP-Adressnutzungsmuster nachweisen, um gesetzliche Anforderungen oder interne Richtlinien zur IP-Adressverwaltung zu erfüllen.
- Behebung von Netzwerkproblemen: Detaillierte CIDR-Nutzungsdaten können Ihnen helfen, die Ursachen von Netzwerkkonnektivitätsproblemen oder Ressourcenkonflikten zu identifizieren.

Durch die genaue Überwachung der CIDR-Nutzung über das IPAM-Dashboard können Sie die Effizienz, Ausfallsicherheit und Compliance Ihrer IP-Adressverwaltung innerhalb von AWS verbessern.

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 deren CIDRs Umfang. 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 Ressourcentypen CIDRs im Bereich.
  - Subnetz: Die Anzahl der CIDRs vier Subnetze.
  - VPC: Die Anzahl von CIDRs für VPCs.
  - EIPs: Die Anzahl von vier CIDRs Elastic IP-Adressen.
  - Öffentliche IPv4 Pools: Die Anzahl von CIDRs vier öffentlichen IPv4 Pools.
- Verwaltungsstatus: Der Verwaltungsstatus von CIDRs.
  - Nicht verwaltet CIDRs: Die Anzahl der Ressourcen CIDRs für nicht verwaltete Ressourcen in diesem Bereich.
  - Ignoriert CIDRs: Die Anzahl der Ressourcen CIDRs , für die Sie ausgewählt haben, dass sie von der Überwachung ausgenommen werden sollen, wenn IPAM im Geltungsbereich enthalten ist. 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).
  - Verwaltet CIDRs: Die Anzahl der Ressourcen CIDRs für verwaltbare Ressourcen (VPCsoder öffentliche IPv4 Pools), die einem IPAM-Pool im Bereich zugewiesen wurden.
- Überlappende Ressourcen CIDRs: Die Anzahl der sich überschneidenden und nicht überlappenden Ressourcen. CIDRs Überlappungen CIDRs können zu einem falschen Routing in Ihrem führen. VPCs

    - Überlappung CIDRs: Die Anzahl der Überschneidungen CIDRs , die sich derzeit innerhalb der IPAM-Pools in diesem Bereich überschneiden. Überschneidungen CIDRs können zu falschem Routing in Ihrem führen. VPCs
    - Nicht überlappend CIDRs: Die Anzahl der Ressourcen CIDRs , die sich innerhalb der IPAM-Pools in diesem Bereich nicht überschneiden.
- Kompatible Ressource CIDRs: Die Anzahl der kompatiblen Ressourcen. CIDRs
    - Konform CIDRs: Die Anzahl der Ressourcen CIDRs , die den Zuweisungsregeln für IPAM-Pools im Bereich entsprechen.
    - Nicht konform CIDRs: Die Anzahl der Ressourcen CIDRs , die nicht den Zuweisungsregeln für die IPAM-Pools im Bereich entsprechen.
- Überschneidungsstatus: Die Anzahl CIDRs dieser Überschneidungen im Laufe der Zeit.
    - OverlappingResourceCidrs: Die Anzahl CIDRs dieser Überschneidungen innerhalb der IPAM-Pools in diesem Bereich. Überschneidungen CIDRs können zu falschem Routing in Ihrem führen. VPCs
- Konformitätsstatus: Die Anzahl der Personen CIDRs , die die Zuteilungsregeln für IPAM-Pools im Geltungsbereich im Laufe der Zeit erfüllen oder nicht einhalten.
    - CompliantResourceCidrs: Die Anzahl der Ressourcen CIDRs , die den Zuweisungsregeln entsprechen.
    - NoncompliantResourceCidrs: Die Anzahl der Ressourcen CIDRs , die den Zuweisungsregeln nicht entsprechen.
- VPC-Nutzung: VPCs (IPv4 und IPv6) mit der höchsten oder niedrigsten IP-Auslastung. Sie können diese Informationen verwenden, um CloudWatch Amazon-Alarme so zu konfigurieren, dass Sie benachrichtigt werden, wenn ein IP-Nutzungsschwellenwert überschritten wird. Weitere Informationen finden Sie unter Metriken zur IPAM-Ressourcenauslastung.
- Subnetznutzung: Subnetze (IPv4 nur) mit der höchsten oder niedrigsten IP-Auslastung. Anhand dieser Informationen können Sie entscheiden, ob Sie wenig ausgelastete Ressourcen behalten oder löschen möchten. Weitere Informationen finden Sie unter Metriken zur IPAM-Ressourcenauslastung.
- VPCs mit der höchsten IPs Zuweisung: Die VPCs , denen der höchste Prozentsatz an IP-Adressraum zugewiesen ist, der Subnetzen zugewiesen ist. Dies ist nützlich, um Ihnen zu zeigen, ob Sie zusätzlichen IP-Adressraum für die VPCs bereitstellen müssen.

- Subnetze mit der höchsten IPs Zuweisung: Die Subnetze mit dem höchsten Prozentsatz an zugewiesenem IP-Adressraum für Ressourcen. 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 gespeichert sind CloudWatch. Weitere Informationen zu den in Amazon CloudWatch gespeicherten Kennzahlen finden Sie unterÜberwachen Sie IPAM mit Amazon CloudWatch. Verwenden Sie die CloudWatch Amazon-Optionen in der AWS CLI-Referenz, um Metriken für Zuweisungen in Ihren IPAM-Pools und -Bereichen anzuzeigen.

Wenn Sie feststellen, dass das CIDR, das für einen Pool bereitgestellt wurde, fast vollständig zugewiesen ist, müssen Sie möglicherweise zusätzliche Ressourcen bereitstellen. CIDRs Weitere Informationen finden Sie unter Bereitstellung CIDRs für einen Pool.

Überwachen Sie die CIDR-Nutzung nach Ressourcen

Die Ansicht Ressourcen in Amazon VPC IP Address Manager bietet einen zentralen Überblick über die Nutzung von IP-Adressen in Ihren AWS Ressourcen. So können Sie schnell feststellen, welche Ressourcen IP-Adressen verbrauchen, Trends bei der Adresszuweisung nachverfolgen und Ihre IP-Adressverwaltung optimieren, um sie an Ihre sich entwickelnde Infrastruktur und Ihre Geschäftsanforderungen anzupassen.

In IPAM ist eine Ressource eine AWS Serviceeinheit, der eine IP-Adresse oder ein CIDR-Block zugewiesen wurde. IPAM verwaltet einige Ressourcen, überwacht andere Ressourcen jedoch nur. Daher ist es wichtig, den Unterschied zwischen den beiden zu verstehen:

- Managed resource (Verwaltete Ressource): Eine verwaltete Ressource hat ein CIDR aus einem IPAM-Pool zugewiesen. IPAM überwacht den CIDR auf mögliche Überschneidungen von IP-Adressen mit anderen IP-Adressen CIDRs im Pool und überwacht, ob der CIDR die Zuweisungsregeln eines Pools einhält. IPAM unterstützt die Verwaltung der folgenden Arten von Ressourcen:

- Elastic-IP-Adressen
- Öffentliche Schwimmbäder IPv4

> **Note**
>
> Öffentliche IPv4 Pools und IPAM-Pools werden von unterschiedlichen Ressourcen in AWS verwaltet. Öffentliche IPv4 Pools sind Ressourcen mit einem einzigen Konto, mit denen Sie Ihre öffentlichen IP-Adressen in Elastic CIDRs umwandeln können. IPAM-Pools können verwendet werden, um Ihren öffentlichen Speicherplatz öffentlichen Pools zuzuweisen. IPv4

- VPCs

- 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 sie `get-ipam-resource-cidrs` mit der AWS CLI verwenden oder wenn Sie Ressourcen im Navigationsbereich anzeigen. IPAM unterstützt die Überwachung der folgenden Ressourcen:
  - Elastic-IP-Adressen
  - Öffentliche IPv4 Schwimmbäder
  - VPCs
  - VPC-Subnetze

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 IP-Dropdown-Menü oben im Inhaltsbereich das IP-Adressprotokoll aus, das Sie verwenden möchten: IPv4 oder. IPv6
4. Wählen Sie im Dropdown-Menü „Bereich“ oben im Inhaltsbereich den gewünschten Bereich aus. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.
5. 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.

6. 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 einen CIDR verfügt, der die Parameter für die Netzmaskenlänge des IPAM-Pools nicht erfüllt, oder wenn sich die Ressource nicht in derselben AWS Region wie der IPAM-Pool befindet, wird sie 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.

- IPs zugewiesen: Für Ressourcen, die zugewiesen sind VPCs, ist dies der Prozentsatz des IP-Adressraums in der VPC, der vom CIDRs Subnetz belegt wird. Bei Ressourcen, bei denen es sich um Subnetze handelt, ist dies der Prozentsatz des verwendeten IPv4 Adressraums im Subnetz, wenn für das Subnetz ein IPv4 CIDR bereitgestellt wurde. Wenn für das Subnetz ein IPv6 CIDR bereitgestellt wurde, wird der Prozentsatz des IPv6 verwendeten 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-Adressraums im Pool, der Elastic IP-Adressen (EIPs) zugewiesen wurde.
- Region: Die AWS Region der Ressource.
- Besitzer-ID: 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.

7. 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, um die CIDR-Nutzung nach Ressourcen zu überwachen:

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

Überwachen Sie IPAM mit Amazon CloudWatch

IPAM speichert automatisch Messwerte zur IP-Adressnutzung (wie den in Ihren IPAM-Pools verfügbaren IP-Adressraum und die Anzahl der Ressourcen CIDRs , die den Zuweisungsregeln entsprechen) und zur Ressourcennutzung im `AWS/IPAM` CloudWatch Amazon-Namespace in der Heimatregion Ihres IPAM.

Die Integration von IPAM mit CloudWatch verbessert Ihre Fähigkeit, Ihre IP-Adressverwaltung innerhalb von IPAM zu überwachen, zu analysieren und zu optimieren. AWS

Zu den Anwendungsfällen zählen:

- Verfolgung von Trends bei der Nutzung von IP-Adressen: CloudWatch Kann die Nutzung des CIDR-Pools, die Bereichszuweisung und andere IPAM-Metriken überwachen und Sie so proaktiv dabei unterstützen, potenzielle Risiken der Erschöpfung von IP-Adressen zu erkennen.
- Einstellung nutzungsabhängiger Warnmeldungen: Sie können CloudWatch Alarme so konfigurieren, dass Sie benachrichtigt werden, wenn die CIDR-Auslastung festgelegte Schwellenwerte erreicht, sodass rechtzeitig eingegriffen und optimiert werden kann.
- Überwachung von IPAM-Ereignissen: CloudWatch Kann IPAM-bezogene Ereignisse wie CIDR-Zuweisungen, Freigaben und Änderungen des Geltungsbereichs erfassen und analysieren und bietet so Einblick in die Aktivitäten zur IP-Adressverwaltung.
- Generierung benutzerdefinierter Dashboards: Durch die Kombination von IPAM-Daten mit anderen AWS Metriken können Sie umfassende Dashboards erstellen, um Ihre IP-Adresslandschaft zusammen mit den zugehörigen Infrastruktur- und Leistungsindikatoren zu visualisieren und zu analysieren.

Inhalt

IPAM-Metriken

IPAM veröffentlicht Daten über Ihr IPAM, Ihre Pools und Bereiche auf 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 bei Amazon CloudWatch würde den Rahmen dieses Abschnitts sprengen. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

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

IPAM-Metriken

Der `AWS/IPAM`-Namespace enthält die folgenden IPAM-Metriken.

Metrikname	Beschreibung
TotalActiveIpCount	Die Gesamtzahl der aktiven IP-Adressen ist die Anzahl der aktiven IP-Adressen in Ihrem IPAM, die Ihnen in Rechnung gestellt würden, wenn Sie vom kostenlosen Kontingent zum erweiterten Kontingent wechseln würden. Eine aktive IP-Adresse ist definiert als eine IP-Adresse oder ein Präfix, das einem Elastic Network Interface (ENI) zugeordnet ist, das an eine Ressource wie eine EC2 Instance angehängt ist. • Diese Metrik ist nur für Kunden im kostenlosen Kontingent verfügbar. • Wenn Ihr IPAM in AWS Organizations integriert ist, deckt die Anzahl der aktiven IP-Adressen alle Unternehmenskonten ab. • Sie können keine Aufschlüsselung der Anzahl der aktiven IP-Adressen nach IP-Typ (public/private) or class (IPv4/IPv6) anzeigen. • IPAM zählt nur von Konten, die ENIs sich im Besitz IPs von überwachten Konten befinden. Die Zählung kann für freigegebene Subnetze ungenau sein. IP-Adressen werden ausgeschlossen, wenn der Subnetz- oder ENI-Eigentümer nicht von IPAM erfasst wird.

Metriken zu IPAM-Pools

Der `AWS/IPAM`-Namespace enthält die folgenden Poolmetriken für IPAM.

Metrikname	Beschreibung
CompliantResourceCidrs	Die Anzahl der verwalteten Ressourcen CIDRs , die den Zuweisungsregeln des IPAM-Pools entsprechen. Weitere

Metrikname	Beschreibung
	Informationen zu Zuweisungsregeln finden Sie unter Erstellen Sie einen Pool auf oberster Ebene IPv4 .
NoncompliantResourceCidrs	Die Anzahl der verwalteten Ressourcen CIDRs , die nicht den Zuweisungsregeln des IPAM-Pools entsprechen. Weitere Informationen zu Zuweisungsregeln finden Sie unter Erstellen Sie einen Pool auf oberster Ebene IPv4 .
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

Der `AWS/IPAM`-Namespace enthält die folgenden Bereichsmetriken für IPAM.

Metrikname	Beschreibung
CompliantResourceCidrs	Die Anzahl der Ressourcen CIDRs , die den Zuweisungsregeln 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 Zuweisung sregeln für die IPAM-Pools im Bereich entsprechen.
OverlappingResourceCidrs	Die Anzahl der Ressourcen CIDRs , die sich im Bereich überschneiden.

Metrikname	Beschreibung
UnmanagedResourceCidrs	Die Anzahl der Ressourcen CIDRs im Bereich, die derzeit verwaltbaren Ressourcen zugeordnet sind, aber nicht von IPAM verwaltet werden.

Öffentliche IP-Metriken von IPAM

Der `AWS/IPAM`-Namespace enthält die folgenden öffentlichen IP-Metriken für IPAM.

Metrikname	Beschreibung
AmazonOwnedContigIPs	Die Anzahl der CIDRs darin enthaltenen IP-Adressen wird für von Amazon bereitgestellte zusammenhängende öffentliche IPv4 Pools bereitgestellt, die dem IPAM gehören.
AllocatedAmazonOwnedContigIPs	Die Anzahl der IP-Adressen, die aus einem von Amazon bereitgestellten zusammenhängenden CIDR-Block für öffentliche IPv4 Pools zugewiesen wurden.
UnallocatedAmazonOwnedContigIPs	Die Anzahl der IP-Adressen innerhalb des von Amazon bereitgestellten zusammenhängenden CIDR-Blocks des öffentlichen IPv4 Pools, der dem IPAM gehört.
AssociatedAmazonOwnedContigIPs	Die Anzahl der Elastic IP-Adressen, die aus einem von Amazon bereitgestellten CIDR-Block für zusammenhängende öffentliche IPv4 Pools zugewiesen wurden und die einer elastic network interface zugeordnet sind.
UnassociatedAmazonOwnedContigIPs	Die Anzahl der Elastic IP-Adressen, die aus einem von Amazon bereitgestellten CIDR-Block für zusammenhängende öffentliche IPv4 Pools zugewiesen wurden und nicht mit einer elastic network interface verknüpft sind.

Metrikdimensionen

Verwenden Sie die nachstehenden Dimensionen, um die IPAM-Metriken zu filtern.

Dimension	Beschreibung
AddressFamily	Die IP-Adressfamilie für die Ressource (oder). CIDRs IPv4 IPv6
Locale	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 VPCs mit Amazon CloudWatch finden Sie unter CloudWatch Kennzahlen für Sie VPCs im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Metriken zur IPAM-Ressourcenauslastung

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

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

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

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 enthalten ein 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, die einen CIDR enthalten, der 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. Sie können diese Limits anpassen, indem Sie sich an das AWS Support Center wenden, wie unter AWS Servicekontingenten im beschrieben Allgemeine AWS-Referenz.

Example Beispiel

Nehmen wir an, Ihr 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 IPv4 VPC-IP-Nutzung, darunter:
  - Die 50 VPCs mit der höchsten IPv4 IP-Auslastung
  - Die 50 VPCs mit der niedrigsten IPv4 Auslastung
  - Bis zu 50, VPCs die einen IPv4 CIDR enthalten, der aus einem IPAM-Pool zugewiesen wurde
- Bis zu 150 Metriken für die IPv6 VPC-Nutzung, darunter:
  - Die 50 VPCs mit der höchsten IPv6 IP-Auslastung
  - Die 50 VPCs mit der niedrigsten IPv6 Auslastung
  - Bis zu 50, VPCs die einen IPv6 CIDR enthalten, der aus einem IPAM-Pool zugewiesen wurde

- Bis zu 150 Messwerte für die IPv4 Subnetznutzung, darunter:
  - Die 50 Subnetze mit der höchsten IP-Auslastung IPv4
  - Die 50 Subnetze mit der niedrigsten IP-Auslastung IPv4
  - Bis zu 50 Subnetze, deren VPC einen IPv4 CIDR enthält, der aus einem IPAM-Pool zugewiesen wurde

VPC-Metriken

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

Metrikname	Beschreibung
Vpc IPUsage	Die Summe, die CIDRs in den Subnetzen der VPC IPs abgedeckt ist, geteilt durch die Summe, die von der VPC IPs abgedeckt wird CIDRs . Dies wird für alle VPC CIDRs im gleichen IPAM-Bereich und separat für IPv4 und berechnet. IPv6 CIDRs

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

Dimension	Beschreibung
AddressFamily	Die IP-Adressfamilie für die Ressource 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
Subnetz IPUsage	Die Anzahl der aktiven Personen IPs geteilt durch die Gesamtzahl IPs im CIDR des Subnetzes IPv4.

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

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

Der Name und die Beschreibung der Metrik für öffentliche IPv4 Pools sind unten aufgeführt.

Metrikname	Beschreibung
Öffentlicher IPv4 Pool IPUsage	Die Anzahl der Personen EIPs aus dem öffentlichen IPv4 Pool geteilt durch die Gesamtzahl der Personen IPs im Pool.

Die Dimensionen, die Sie zum Filtern der Messwerte für öffentliche IPv4 Pools verwenden können, sind unten aufgeführt.

Dimension	Beschreibung
OwnerID	Die ID des Besitzers des öffentlichen IPv4 Pools.

Dimension	Beschreibung
Öffentliche IPv4 Pool-ID	Die ID des öffentlichen IPv4 Pools.
Region	Die AWS Region, in der sich das öffentliche IPv4 Schwimmbad befindet.
ScopeID	Die ID des IPAM-Bereichs, zu dem der öffentliche IPv4 Pool gehört.

Metriken von Einblicke in öffentliche IPs

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

Metrikname	Beschreibung
AmazonOwnedElasticIPs	Die Anzahl der Elastic IP-Adressen im Besitz von Amazon, die Sie bereitgestellt oder Ressourcen in Ihrem Konto zugewiesen haben. AWS
AssociatedAmazonOwnedElasticIPs	Die Anzahl der Elastic IP-Adressen, die Amazon gehören und die Sie mit Ressourcen in Ihrem AWS Konto verknüpft haben.
AssociatedBringYourOwnIPs	Die Anzahl der öffentlichen IPv4 Adressen, die Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) genutzt und mit Ressourcen in Ihrem Konto verknüpft haben. AWS
BringYourOwnIPs	Die Anzahl der öffentlichen IPv4 Adressen, die Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) verwendet haben.
EC2ÖffentlichIPs	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 für die automatische Zuweisung einer öffentlichen Adresse konfiguriert wurde. IPv4
ServiceManagedBringYourOwnIPs	Die Anzahl der öffentlichen IPv4 Adressen, auf die Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) zugegriff

Metrikname	Beschreibung
	en haben und die von einem Dienst bereitgestellt und verwaltet werden. AWS
ServiceManagedIPs	Die Anzahl der öffentlichen IPv4 Adressen, die von einem Dienst bereitgestellt und verwaltet werden. AWS
UnassociatedAmazonOwnedElasticIPs	Die Anzahl der Elastic IP-Adressen, die Amazon gehören und die Sie nicht mit Ressourcen in Ihrem AWS Konto verknüpft haben.
UnassociatedBringYourOwnIPs	Die Anzahl der öffentlichen IPv4 Adressen, die Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) verwendet haben und denen Sie keine Ressourcen in Ihrem Konto zugeordnet haben. AWS

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

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 nach den folgenden Ressourcentypen zu CIDRs suchen:

- VPCs
- VPC-Subnetze
- Elastic-IP-Adressen
- EC2 Instanzen
- EC2 Netzwerkschnittstellen, die mit Instanzen verbunden sind

Important

IPAM überwacht zwar keine EC2 Amazon-Instances oder EC2 Netzwerkschnittstellen, die mit Instances verbunden sind, aber Sie können die Funktion „IP-Verlauf durchsuchen“ verwenden, um nach historischen Daten auf EC2 Instances und CIDRs Netzwerkschnittstellen 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 VPC CIDRs zwischen Bereichen verschieben.
- Wenn Sie eine Ressource löschen oder auf ein AWS Konto übertragen, das nicht von Ihrem IPAM überwacht wird, ist jeder neue Verlauf, der sich auf die Ressource bezieht, nicht sichtbar und Ihr IPAM überwacht die Ressource nicht. Die IP-Adresse der Ressource kann jedoch weiterhin gesucht werden.

- Wenn SieIntegrieren von IPAM mit Konten außerhalb Ihrer Organisation, der IPAM-Besitzer, den IP-Adressverlauf aller Ressourcen einsehen können, die diesen Konten CIDRs 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 eine 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 der CIDR in mehreren Fällen vorkommt. VPCs
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.

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

Beispiele dafür, wie Sie die verwenden können, AWS CLI um die IP-Adressnutzung zu analysieren und zu überprüfen, finden Sie unter Tutorial: IP-Adressverlauf mit dem AWS CLI anzeigen.

Die Ergebnisse der Suche sind in folgende Spalten unterteilt:

- Endzeit in Stichprobe: Abgetastete Endzeit der resource-to-CIDR Zuordnung innerhalb des IPAM-Bereichs. Änderungen werden in regelmäßigen Snapshots aufgenommen, sodass die Endzeit möglicherweise vor diesem bestimmten Zeitpunkt eingetreten ist.

- Startzeit in Stichprobe: Abgetastete Startzeit der resource-to-CIDR Assoziation 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 einen IPAM- und IPAM-Pool mit CIDR 10.0.0.0/8 und wählen die Option für den automatischen Import, damit IPAM alle CIDRs Objekte erkennen und importieren kann, die in den 10.0.0.0/8-IP-Adressbereich fallen. Da IPAM Änderungen CIDRs in regelmäßigen Snapshots aufnimmt, erkennt es die 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 einen CIDR verfügt, der die Parameter für die Netzmaskenlänge des IPAM-Pools nicht erfüllt, oder wenn sich die Ressource nicht in derselben AWS Region wie der IPAM-Pool befindet, wird sie 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.
  - Instanz: Das CIDR ist einer Instanz zugeordnet. EC2
  - 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.

- Besitzer-ID: Die AWS Konto-ID des Benutzers, der diese Ressource erstellt hat (falls zutreffend).

Anzeigen von Einblicken in öffentliche IP-Adressen

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 einsehen, die von Diensten in allen AWS Regionen für Ihre gesamte AWS Organisation verwendet werden.
- Wenn Ihr IPAM in ein einziges Konto integriert ist, können Sie alle öffentlichen IPv4 Adressen, die von Diensten in allen AWS Regionen verwendet werden, in Ihrem Konto einsehen.

Eine öffentliche IPv4 Adresse ist eine IPv4 Adresse, die aus dem Internet weitergeleitet werden kann. Eine öffentliche IPv4 Adresse ist notwendig, damit eine Ressource direkt vom Internet IPv4 aus 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 Amazon VPC-Preisseite auf der Registerkarte Öffentliche IPv4 Adresse.

Sie können Einblicke in die folgenden Arten von öffentlichen IPv4 Adressen einsehen:

- Elastische IP-Adressen (EIPs): Von Amazon bereitgestellte statische, öffentliche IPv4 Adressen, die Sie einer EC2 Instance, einer elastic network interface oder einer AWS Ressource zuordnen können.
- EC2 öffentliche IPv4 Adressen: Öffentliche IPv4 Adressen, die einer EC2 Instance von Amazon zugewiesen wurden (wenn die EC2 Instance in einem Standardsubnetz gestartet wird oder wenn die Instance in einem Subnetz gestartet wird, das für die automatische Zuweisung einer öffentlichen IPv4 Adresse konfiguriert wurde).
- BYOIPv4 Adressen: Öffentliche IPv4 Adressen im IPv4 Adressbereich, zu dem Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) gewechselt haben.

- Vom Dienst verwaltete IPv4 Adressen: Öffentliche IPv4 Adressen, die automatisch auf AWS Ressourcen bereitgestellt und von einem Dienst verwaltet werden. AWS Zum Beispiel öffentliche IPv4 Adressen auf Amazon ECS, Amazon RDS oder Amazon WorkSpaces.

Public IP Insights zeigt Ihnen alle öffentlichen IPv4 Adressen, die von Diensten in allen Regionen verwendet werden. Sie können diese Erkenntnisse nutzen, um die Nutzung öffentlicher IPv4 Adressen zu ermitteln und Empfehlungen zur Freigabe ungenutzter Elastic IP-Adressen einzusehen.

- Öffentliche IP-Typen: Die Anzahl der öffentlichen IPv4 Adressen, sortiert nach Typ.
  - Eigentum von Amazon EIPs: Elastic IP-Adressen, die Sie bereitgestellt oder Ressourcen in Ihrem Konto zugewiesen haben. AWS
  - EC2 öffentlich IPs: Öffentliche IPv4 Adressen, die EC2 Instances zugewiesen wurden, als die Instances in einem Standardsubnetz oder in einem Subnetz gestartet wurden, das für die automatische Zuweisung einer öffentlichen Adresse konfiguriert wurde. IPv4
  - BYOIP: Öffentliche IPv4 Adressen, auf die Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) zugegriffen haben.
  - Verwalteter Dienst IPs: Öffentliche IPv4 Adressen, die von einem Dienst bereitgestellt und verwaltet werden. AWS
  - Von IP verwalteter Dienst: Öffentliche IPv4 Adressen, die einem Dienst zugewiesen AWS und von diesem verwaltet werden. AWS
  - Zusammenhängend im Besitz von Amazon EIPs: Elastische IP-Adressen, die aus einem von Amazon bereitgestellten zusammenhängenden öffentlichen IPAM-Pool zugewiesen wurden. IPv4
- EIP-Nutzung: Die Anzahl der Elastic-IP-Adressen, geordnet nach ihrer Nutzungsweise.
  - Zugehöriges Eigentum von Amazon EIPs: 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 verknüpft Im Besitz von Amazon EIPs: Elastic IP-Adressen, die Sie in Ihrem AWS Konto bereitgestellt, aber keiner Netzwerkschnittstelle zugeordnet haben.
  - Nicht zugeordnetes BYOIP: Öffentliche IPv4 Adressen, die Sie AWS mithilfe von BYOIP verwendet haben, aber keiner Netzwerkschnittstelle zugeordnet haben.

  - Verbundene zusammenhängende IP-Adressen im Besitz von Amazon EIPs: Elastische IP-Adressen, die aus einem von Amazon bereitgestellten zusammenhängenden öffentlichen IPv4 IPAM-Pool zugewiesen und einer Ressource zugeordnet sind.
  - Nicht verknüpft, im Besitz von Amazon, zusammenhängend EIPs: Elastische IP-Adressen, die aus einem von Amazon bereitgestellten zusammenhängenden öffentlichen IPAM-Pool zugewiesen wurden und nicht mit einer Ressource verknüpft sind. IPv4
- IPv4 Zusammenhängende Nutzung im Besitz von Amazon: Eine Tabelle, die die zusammenhängende IPs Nutzung öffentlicher IPv4 Adressen im Laufe der Zeit und die zugehörigen IPAM-Pools im Besitz von Amazon zeigt. IPv4
- Öffentliche IP-Adressen: Eine Tabelle mit öffentlichen Adressen und ihren Attributen. IPv4
  - IP-Adresse: Die öffentliche IPv4 Adresse.
  - Zugeordnet: Gibt an, ob die Adresse einer EC2 Instanz, Netzwerkschnittstelle oder AWS Ressource zugeordnet ist oder nicht.
    - Zugeordnet: Die öffentliche IPv4 Adresse ist einer EC2 Instanz, Netzwerkschnittstelle oder AWS Ressource zugeordnet.
    - Nicht verknüpft: Die öffentliche IPv4 Adresse ist keiner Ressource zugeordnet und befindet sich in Ihrem AWS Konto im Leerlauf.
  - Adresstyp: Der Typ der IP-Adresse.
    - EIP im Besitz von Amazon: Die öffentliche IPv4 Adresse ist eine Elastic IP-Adresse.
    - BYOIP: Die öffentliche IPv4 Adresse wurde mithilfe von BYOIP eingerichtet. AWS
    - EC2 öffentliche IP: Die öffentliche IPv4 Adresse wurde automatisch einer Instanz zugewiesen. EC2
    - 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, IPs werden seine öffentlichen Daten nicht aufgeführt. Informationen dazu, wie Sie diese öffentlich anzeigen können IPs, finden Sie unter Benutzerdefinierte 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 es sich bei dieser öffentlichen IPv4 Adresse um eine Elastic IP-Adresszuweisung handelt, handelt es sich um den Namen und die ID der EIP-Zuweisung.
- Netzwerkschnittstellen-ID: Wenn diese öffentliche IPv4 Adresse einer Netzwerkschnittstelle zugeordnet ist, ist dies die ID der Netzwerkschnittstelle.
- Instanz-ID: Wenn diese öffentliche IPv4 Adresse einer EC2 Instanz zugeordnet ist, ist dies die Instanz-ID.
- Sicherheitsgruppen: Wenn diese öffentliche IPv4 Adresse einer EC2 Instance zugeordnet ist, sind dies der Name und die ID der Sicherheitsgruppe, die der Instance zugewiesen ist.
- Öffentlicher IPv4 Pool: Wenn es sich um eine Elastic IP-Adresse aus einem IP-Adresspool handelt, der Amazon gehört und von Amazon verwaltet wird, ist der Wert „-“. Wenn es sich um eine Elastic IP-Adresse aus einem IP-Adressbereich handelt, den Sie besitzen und zu Amazon gebracht haben (mithilfe von BYOIP), entspricht der Wert der öffentlichen IPv4 Pool-ID.
- 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.
- ID der Ressourcenerkennung: ID der Ressourcenerkennung, die diese öffentliche IPv4 Adresse entdeckt hat.
- Service-Ressource: Ressourcen-ARN oder -ID.

Wenn Ihrem Konto eine Elastic IP-Adresse zugewiesen, aber nicht mit einer Netzwerkschnittstelle verknüpft ist, erscheint ein Banner, das Sie darüber informiert, dass Sie EIPs in Ihrem Konto keine Verknüpfung haben und dass Sie sie freigeben sollten.

> **Important**
>
> Einblicke in öffentliche IPs wurde kürzlich aktualisiert. Wenn Sie einen Fehler sehen, der darauf zurückzuführen ist, dass Sie keine Anrufberechtigungen haben 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 eingehende Sicherheitsgruppen: Wenn diese IP-Adresse einer EC2 Instance zugeordnet ist, sind dies die Sicherheitsgruppenregeln, die den eingehenden Datenverkehr zur Instance steuern.
   - Regeln für ausgehende Sicherheitsgruppen: Wenn diese IP-Adresse einer EC2 Instance zugeordnet ist, sind dies die Sicherheitsgruppenregeln, die den ausgehenden Datenverkehr von der 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 Ihnen, wie Sie allgemeine IPAM-Aufgaben mit der AWS CLI ausführen. Informationen zum Abrufen finden Sie AWS CLI unterZugriff auf IPAM. Weitere Informationen zu den IPAM-Konzepten, die in diesen Tutorials erwähnt werden, finden Sie unter Funktionsweise von IPAM.

Inhalt

Erste Schritte mit IPAM mithilfe der CLI AWS

Dieses Tutorial führt Sie durch den Prozess der Einrichtung und Verwendung von Amazon VPC IP Address Manager (IPAM) mit der AWS CLI unter Verwendung eines einzigen AWS Kontos. Am Ende dieses Tutorials haben Sie ein IPAM erstellt, eine Hierarchie von IP-Adresspools erstellt und einer VPC einen CIDR zugewiesen.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Ein AWS Konto mit Berechtigungen zum Erstellen und Verwalten von IPAM-Ressourcen.
- Die AWS CLI wurde mit den entsprechenden Anmeldeinformationen installiert und konfiguriert. Informationen zur Installation der AWS CLI finden Sie unter Installation oder Aktualisierung der neuesten Version der AWS CLI. Informationen zur Konfiguration der AWS CLI finden Sie unter Grundlagen der Konfiguration.

- Grundlegendes Verständnis von IP-Adressierung und CIDR-Notation.
- Grundkenntnisse der Amazon VPC-Konzepte.
- Ungefähr 30 Minuten, um das Tutorial abzuschließen.

Erstellen eines IPAM

Der erste Schritt besteht darin, ein IPAM mit Betriebsregionen zu erstellen. Ein IPAM hilft Ihnen bei der Planung, Nachverfolgung und Überwachung von IP-Adressen für Ihre AWS Workloads.

Erstellen Sie ein IPAM mit Betriebsregionen in us-east-1 und us-west-2:

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

Dieser Befehl erstellt ein IPAM und ermöglicht es ihm, IP-Adressen in den angegebenen Regionen zu verwalten. Die Betriebsregionen sind die AWS Regionen, in denen das IPAM IP-Adressen verwalten darf. CIDRs

Stellen Sie sicher, dass Ihr IPAM erstellt wurde:

```
aws ec2 describe-ipams
```

Notieren Sie sich die IPAM-ID aus der Ausgabe, da Sie sie für nachfolgende Schritte benötigen.

Warten Sie, bis das IPAM vollständig erstellt und verfügbar ist (ca. 20 Sekunden):

```
sleep 20
```

Rufen Sie die IPAM-Bereichs-ID ab

Wenn Sie ein IPAM erstellen, erstellt es AWS automatisch einen privaten und einen öffentlichen Bereich. Für dieses Tutorial verwenden wir den privaten Bereich.

Rufen Sie die IPAM-Details ab und extrahieren Sie die private Bereichs-ID:

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

Ersetzen Sie `ipam-0abcd1234` durch Ihre tatsächliche IPAM-ID.

Identifizieren und notieren Sie sich anhand der Ausgabe die private Bereichs-ID aus dem `PrivateDefaultScopeId` Feld. Dies sieht etwa so aus: `ipam-scope-0abcd1234`.

Erstellen Sie einen Pool der obersten Ebene IPv4

Lassen Sie uns nun einen Pool der obersten Ebene im privaten Bereich erstellen. Dieser Pool wird als übergeordneter Pool für alle anderen Pools in unserer Hierarchie dienen.

Erstellen Sie einen IPv4 Pool der obersten Ebene:

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

`ipam-scope-0abcd1234`Ersetzen Sie es durch Ihre tatsächliche private Bereichs-ID.

Warten Sie, bis der Pool vollständig erstellt und verfügbar ist:

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

`ipam-pool-0abcd1234`Ersetzen Sie es durch Ihre tatsächliche Pool-ID der obersten Ebene. Der Status sollte vorliegen, `create-complete` bevor Sie fortfahren.

Sobald der Pool verfügbar ist, stellen Sie ihm einen CIDR-Block bereit:

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

Warten Sie, bis der CIDR vollständig bereitgestellt ist:

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

`provisioned`Bevor Sie fortfahren, sollten Sie den Status angeben.

Erstellen Sie einen regionalen IPv4 Pool

Als Nächstes erstellen Sie einen regionalen Pool innerhalb des Pools der obersten Ebene. Dieser Pool wird spezifisch für eine bestimmte AWS Region sein.

Erstellen Sie einen regionalen IPv4 Pool:

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

`ipam-scope-0abcd1234`Ersetzen Sie es durch Ihre tatsächliche private Bereichs-ID und `ipam-pool-0abcd1234` durch Ihre Pool-ID der obersten Ebene.

Warten Sie, bis der regionale Pool vollständig erstellt und verfügbar ist:

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

`ipam-pool-1abcd1234`Ersetzen Sie es durch Ihre tatsächliche regionale Pool-ID. `create-complete`Bevor Sie fortfahren, sollten Sie den Status angeben.

Sobald der Pool verfügbar ist, stellen Sie ihm einen CIDR-Block bereit:

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

Warten Sie, bis der CIDR vollständig bereitgestellt ist:

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

`provisioned`Bevor Sie fortfahren, sollten Sie den Status angeben.

Erstellen Sie einen IPv4 Entwicklungspool

Erstellen Sie jetzt einen Entwicklungspool innerhalb des regionalen Pools. Dieser Pool wird für Entwicklungsumgebungen verwendet.

Erstellen Sie einen IPv4 Entwicklungspool:

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

`ipam-scope-0abcd1234`Ersetzen Sie es durch Ihre tatsächliche private Bereichs-ID und `ipam-pool-1abcd1234` durch Ihre regionale Pool-ID.

Hinweis: Es ist wichtig, dass der `--locale` Parameter dem Gebietsschema des übergeordneten Pools entspricht.

Warten Sie, bis der Entwicklungspool vollständig erstellt und verfügbar ist:

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

`ipam-pool-2abcd1234`Ersetzen Sie es durch Ihre tatsächliche Entwicklungspool-ID. Der Status sollte sein, `create-complete` bevor Sie fortfahren.

Sobald der Pool verfügbar ist, stellen Sie ihm einen CIDR-Block bereit:

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

Warten Sie, bis der CIDR vollständig bereitgestellt ist:

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

`provisioned`Bevor Sie fortfahren, sollten Sie den Status angeben.

Erstellen Sie eine VPC mit einem IPAM-Pool-CIDR

Erstellen Sie abschließend eine VPC, die ein CIDR aus Ihrem IPAM-Pool verwendet. Dies zeigt, wie IPAM verwendet werden kann, um Ressourcen IP-Adressraum zuzuweisen. AWS

Erstellen Sie eine VPC mit einem IPAM-Pool-CIDR:

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

Ersetzen Sie es `ipam-pool-2abcd1234` durch Ihre tatsächliche Entwicklungspool-ID.

Der `--ipv4-netmask-length 26` Parameter gibt an, dass ein /26-CIDR-Block (64 IP-Adressen) aus dem Pool zugewiesen werden soll. Diese Netzmaskenlänge wird so gewählt, dass sie kleiner ist als der CIDR-Block des Pools (/24).

Stellen Sie sicher, dass Ihre VPC erstellt wurde:

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

Überprüfen Sie die IPAM-Poolzuweisung

Überprüfen Sie, ob der CIDR aus Ihrem IPAM-Pool zugewiesen wurde:

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

Ersetzen Sie es `ipam-pool-2abcd1234` durch Ihre tatsächliche Entwicklungspool-ID.

Dieser Befehl zeigt alle Zuweisungen aus dem angegebenen IPAM-Pool an, einschließlich der VPC, die Sie gerade erstellt haben.

Fehlerbehebung

Hier sind einige häufig auftretende Probleme, auf die Sie bei der Arbeit mit IPAM stoßen können:

- Berechtigungsfehler: Stellen Sie sicher, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle über die erforderlichen Berechtigungen zum Erstellen und Verwalten von IPAM-Ressourcen verfügt.

Möglicherweise benötigen Sie die `ec2:CreateIpamec2:CreateIpamPool`, und andere zugehörige Berechtigungen.

- Ressourcenlimit überschritten: Standardmäßig können Sie nur ein IPAM pro Konto erstellen. Wenn Sie bereits ein IPAM haben, müssen Sie es löschen, bevor Sie ein neues erstellen oder das vorhandene verwenden können.
- Fehler bei der CIDR-Zuweisung: Stellen Sie bei der Bereitstellung CIDRs für Pools sicher, dass sich das CIDR, das Sie bereitstellen möchten, nicht mit vorhandenen Zuweisungen in anderen Pools überschneidet.
- Timeouts bei API-Anfragen: Wenn Sie auf "RequestExpired" -Fehler stoßen, kann dies an Netzwerklatenz oder Problemen mit der Zeitsynchronisierung liegen. Versuchen Sie es erneut mit dem Befehl.
- Falsche Statusfehler: Wenn Sie "IncorrectState" -Fehler erhalten, liegt das möglicherweise daran, dass Sie versuchen, einen Vorgang mit einer Ressource auszuführen, die sich nicht im richtigen Zustand befindet. Warten Sie, bis die Ressource vollständig erstellt oder bereitgestellt wurde, bevor Sie fortfahren.
- Fehler bei der Zuordnungsgröße: Wenn Sie "InvalidParameterValue" Fehler zur Zuordnungsgröße erhalten, stellen Sie sicher, dass die von Ihnen angeforderte Netzmaskenlänge der Poolgröße entspricht. Beispielsweise können Sie einem /24-Pool kein /25-CIDR zuweisen.
- Verstöße gegen Abhängigkeiten: Beim Bereinigen von Ressourcen können "" -Fehler auftreten. DependencyViolation Das liegt daran, dass Ressourcen voneinander abhängig sind. Stellen Sie sicher, dass Sie Ressourcen in der umgekehrten Reihenfolge der Erstellung und Deprovisionierung löschen, CIDRs bevor Sie Pools löschen.

Bereinigen von -Ressourcen

Wenn Sie mit diesem Tutorial fertig sind, sollten Sie die von Ihnen erstellten Ressourcen bereinigen, um unnötige Kosten zu vermeiden.

1. Löschen der VPC:

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

2. Trennen Sie die Bereitstellung von CIDR aus dem Entwicklungspool:

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

3. Löschen Sie den Entwicklungspool:

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

4. Den CIDR aus dem Regionalpool entfernen:

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

5. Löschen Sie den Regionalpool:

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

6. Entfernen Sie die Bereitstellung des CIDR aus dem Pool der obersten Ebene:

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

7. Löschen Sie den Pool der obersten Ebene:

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

8. Löschen Sie das IPAM:

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

Ersetzen Sie alle IDs durch Ihre tatsächliche Ressource IDs.

> **Note**
>
> Möglicherweise müssen Sie zwischen diesen Vorgängen warten, bis die Ressourcen vollständig gelöscht sind, bevor Sie mit dem nächsten Schritt fortfahren können. Wenn Sie auf Verstöße gegen Abhängigkeiten stoßen, warten Sie einige Sekunden und versuchen Sie es erneut.

Nächste Schritte

Nachdem Sie nun gelernt haben, wie Sie IPAM mit der AWS CLI erstellen und verwenden, möchten Sie sich vielleicht mit erweiterten Funktionen vertraut machen:

- Planen der Bereitstellung von IP-Adressen— Erfahren Sie, wie Sie Ihren IP-Adressraum effektiv planen
- Überwachen Sie die CIDR-Nutzung nach Ressourcen— Verstehen Sie, wie Sie die Nutzung von IP-Adressen überwachen
- Teilen Sie einen IPAM-Pool mithilfe von RAM AWS— Erfahren Sie, wie Sie IPAM-Pools für mehrere AWS Konten gemeinsam nutzen
- Integrieren Sie IPAM mit Konten in einer Organisation AWS— Erfahren Sie, wie Sie IPAM in Ihrem Unternehmen einsetzen können

Tutorial: Erstellen eines IPAM und von Pools über die Konsole

In diesem Tutorial erstellen Sie ein IPAM, integrieren es AWS Organizations, erstellen IP-Adresspools und erstellen 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.

Sie können IPAM zwar als Einzelbenutzer verwenden, aber durch die Integration mit 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

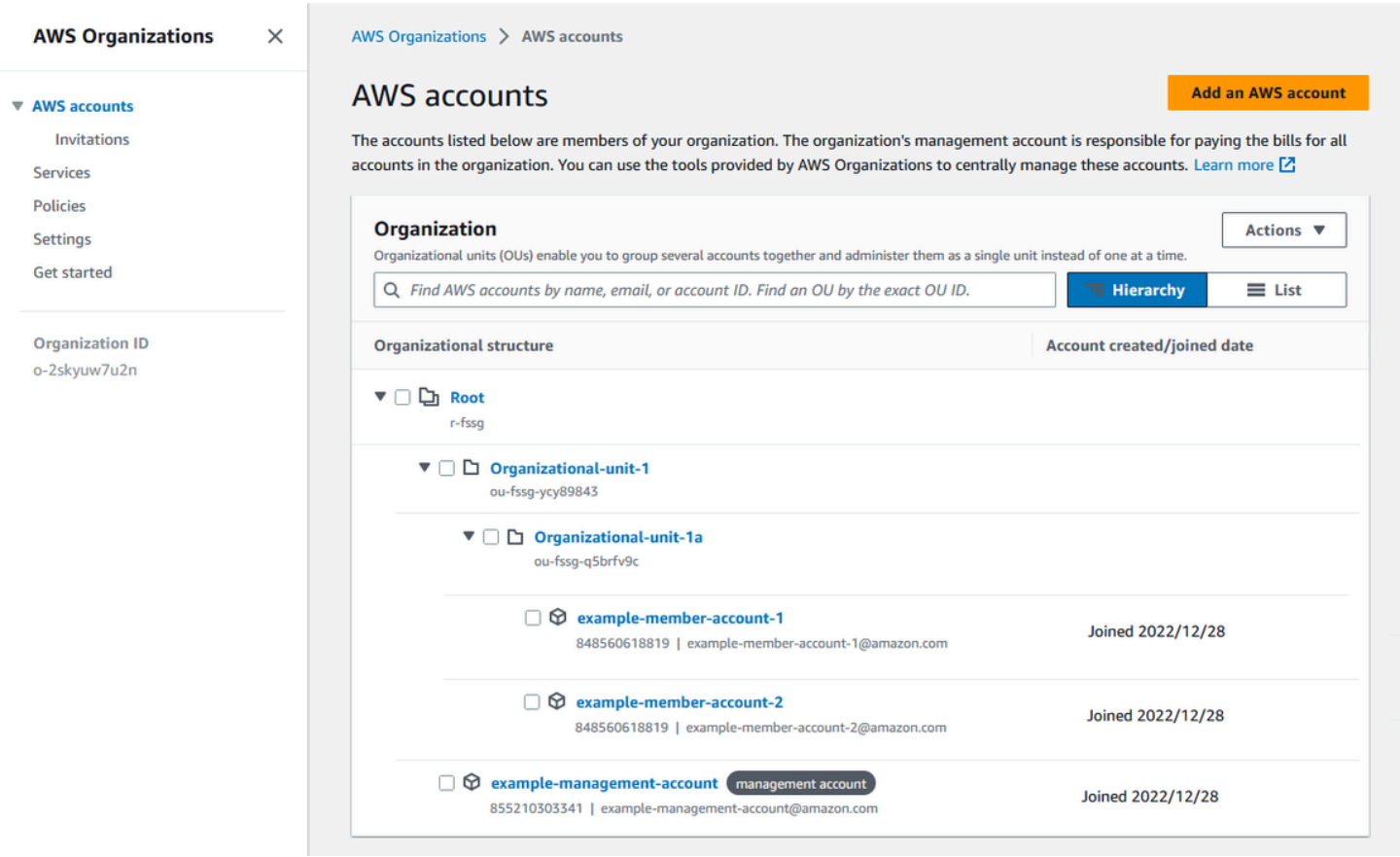
Bevor Sie beginnen, müssen Sie ein AWS Organizations Konto mit mindestens einem Mitgliedskonto eingerichtet haben. Entsprechende Anweisungen finden Sie unter Erstellen und Konfigurieren einer Organisation im Benutzerhandbuch von AWS Organizations .

Wie AWS Organizations lässt es sich mit IPAM integrieren

Dieser Abschnitt zeigt 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 (example-management-accountin der folgenden Abbildung 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 (im Folgenden oben example-member-account-2 genannt) als Entwicklerkonto. Dieses Konto erstellt eine VPC mit einem CIDR, das aus einem IPAM-Pool zugewiesen wird.



Zusätzlich zu den Konten benötigen Sie die ID der Organisationseinheit (ou-fssg-q5brfv9c im vorherigen Bild), die das Mitgliedskonto enthält, das Sie als Entwicklerkonto verwenden werden. 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 AWS Organizations Kontotypen wie Verwaltungs - und Mitgliedskonten finden Sie unter Terminologie und Konzepte.AWS Organizations

Schritt 1: Delegieren eines IPAM-Administrators

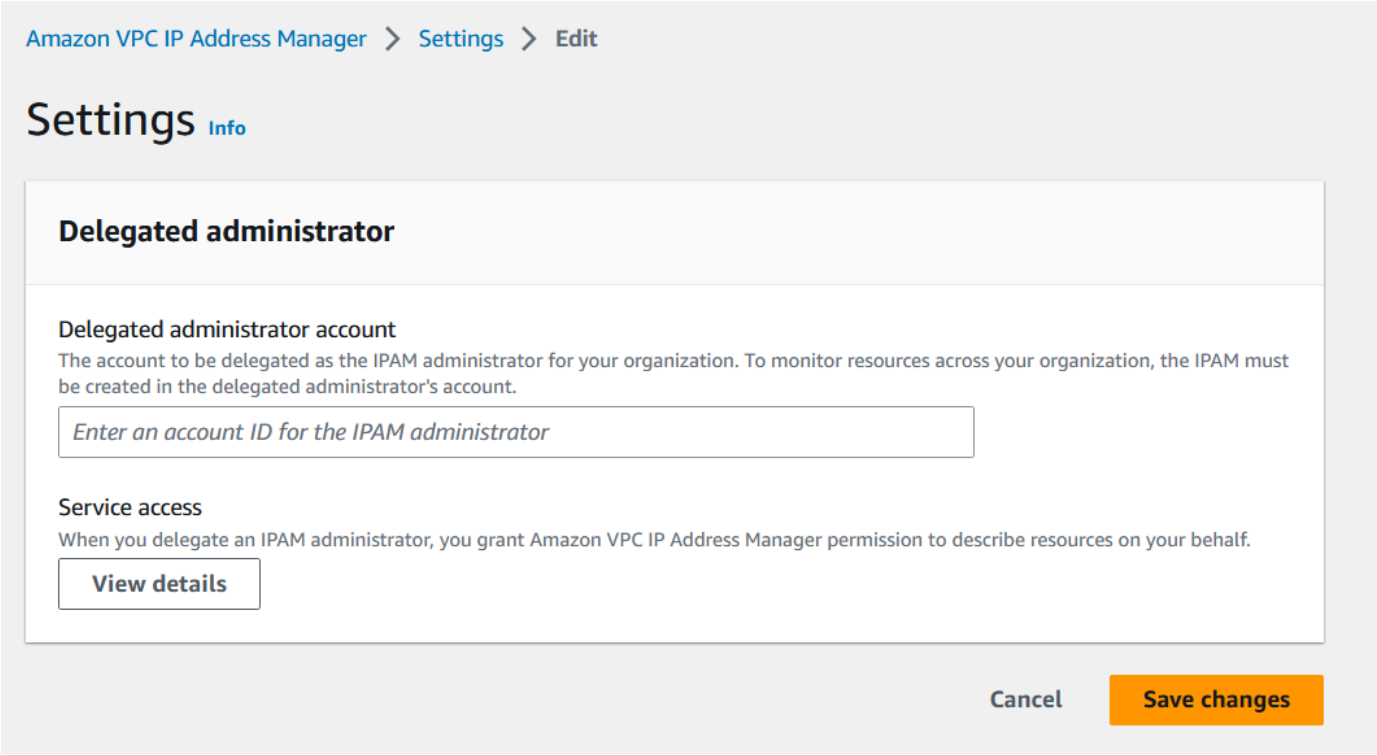
In diesem Schritt delegieren Sie ein AWS Organizations Mitgliedskonto als IPAM-Administrator. Wenn Sie einen IPAM-Administrator delegieren, wird in jedem Ihrer Mitgliedskonten automatisch eine

dienstbezogene Rolle erstellt. AWS Organizations IPAM überwacht die Nutzung der IP-Adresse in diesen Konten durch Übernahme der serviceverknüpften Rolle in jedem Mitgliedskonto. Es kann dann die Ressourcen und ihre Ressourcen CIDRs unabhängig von ihrer Organisationseinheit ermitteln.

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

So delegieren Sie ein IPAM-Administratorkonto

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



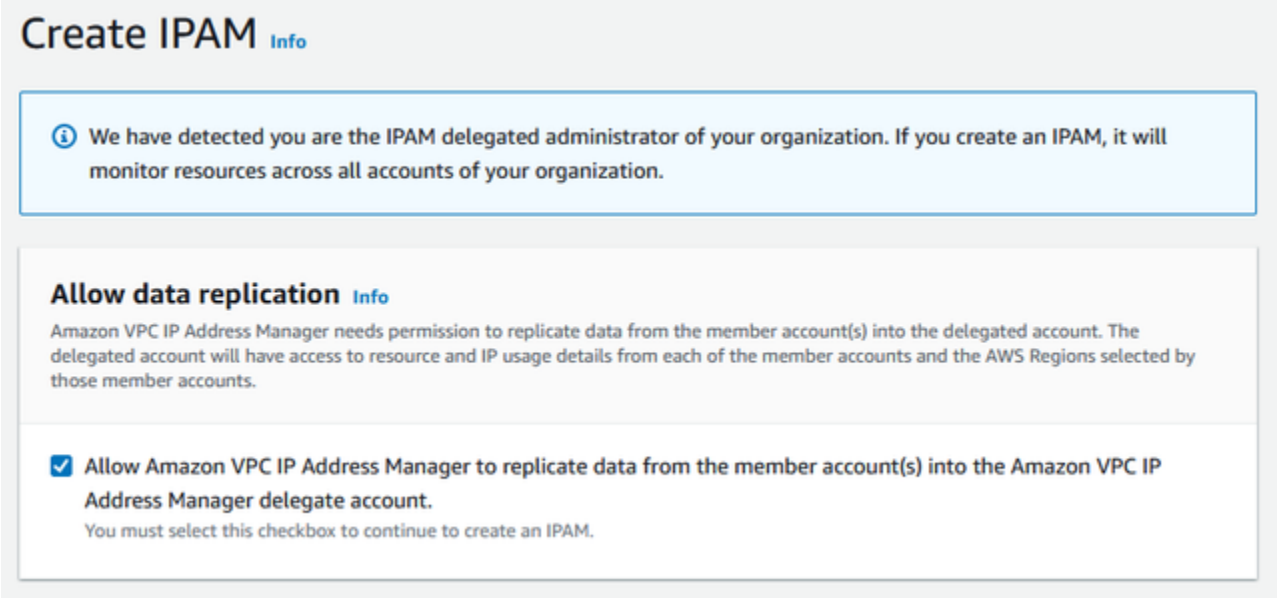
6. Wählen Sie Änderungen speichern. Das Feld Delegierter Administrator wird mit Informationen zum Mitgliedskonto gefüllt.

Schritt 2: Erstellen eines IPAMs

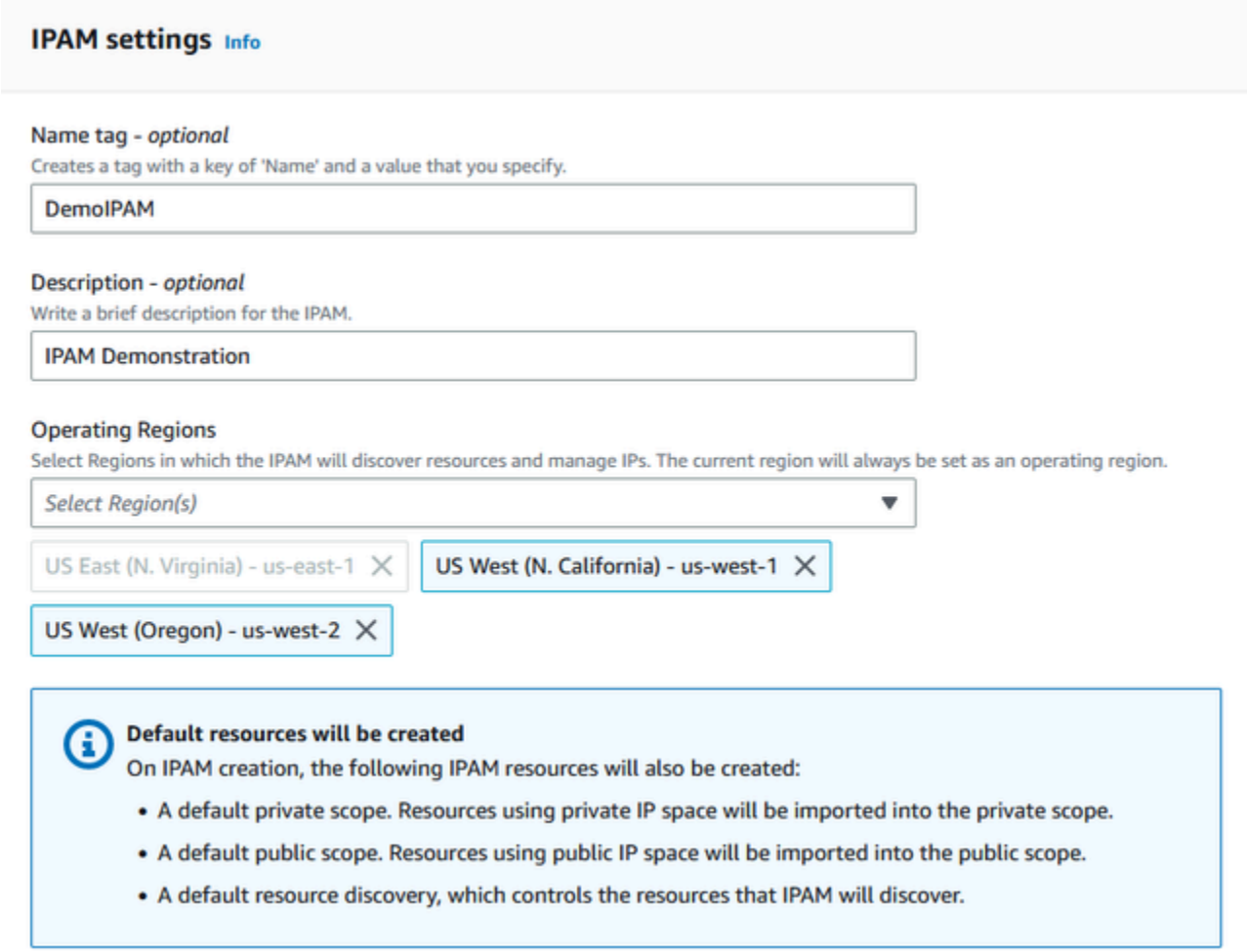
In diesem Schritt erstellen Sie einen IPAM. Wenn Sie einen IPAM erstellen, werden automatisch zwei Bereiche für den IPAM erstellt: der privaten Bereich, der für den gesamten privaten Adressraum vorgesehen ist, und der öffentliche Bereich für den gesamten öffentlichen Adressraum. Die Bereiche sind zusammen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

Erstellen eines IPAM

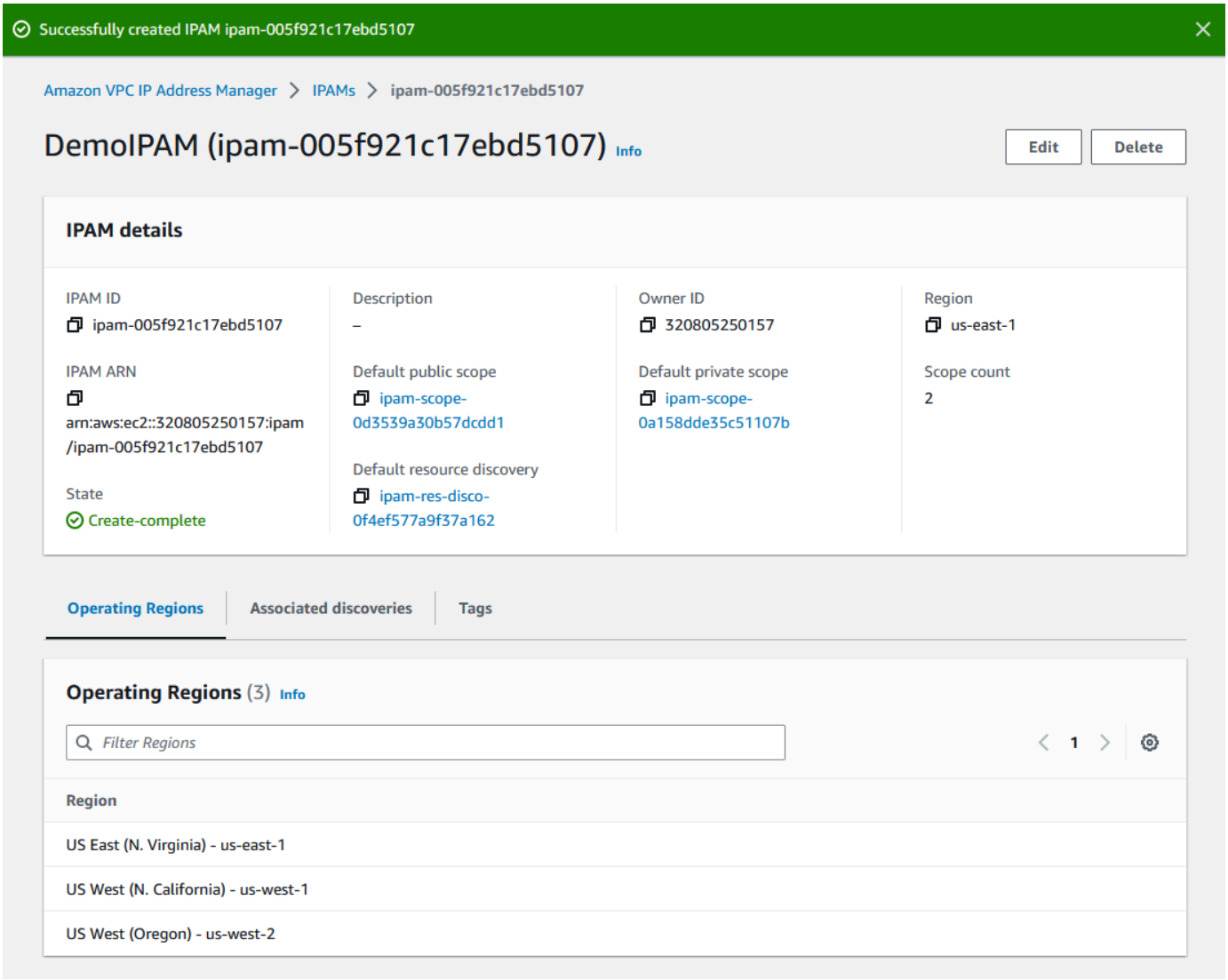
1. Verwenden Sie das AWS Organizations Mitgliedskonto, das im vorherigen Schritt als IPAM-Administrator delegiert wurde, und öffnen Sie die IPAM-Konsole unter. https://console.aws.amazon.com/ipam/
2. Wählen Sie in der AWS Management Console die AWS Region aus, in der Sie das IPAM erstellen möchten. Erstellen 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 dieses IPAM Ressourcen verwalten und ermitteln kann. Die AWS Region, in der Sie Ihr 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

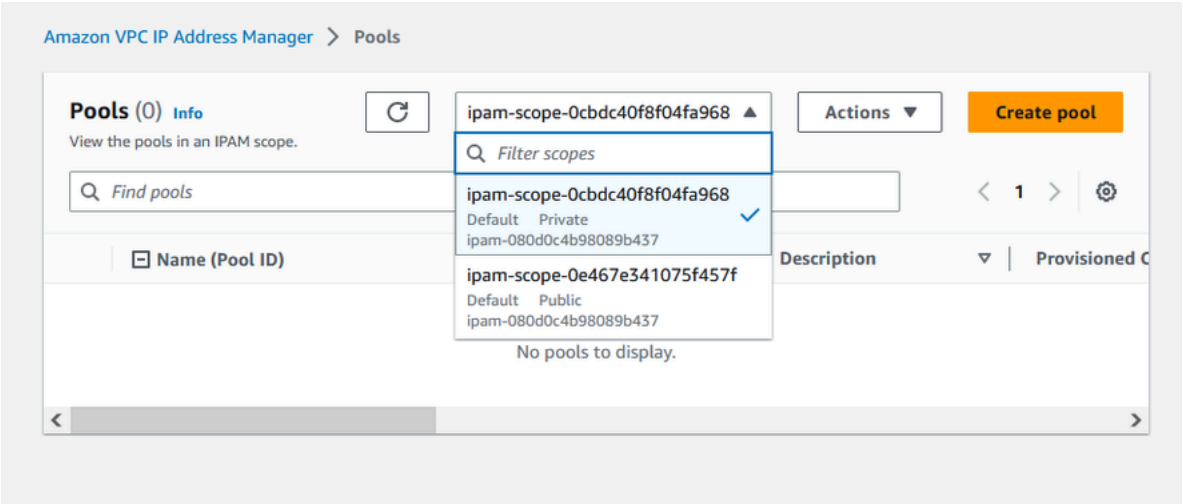
In diesem Tutorial erstellen Sie eine Poolhierarchie, wobei Sie mit dem IPAM-Pool der obersten Ebene beginnen. In den nachfolgenden Schritten erstellen Sie zwei regionale Pools und einen Entwicklungspool für die Vorproduktion in einem der regionalen Pools.

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

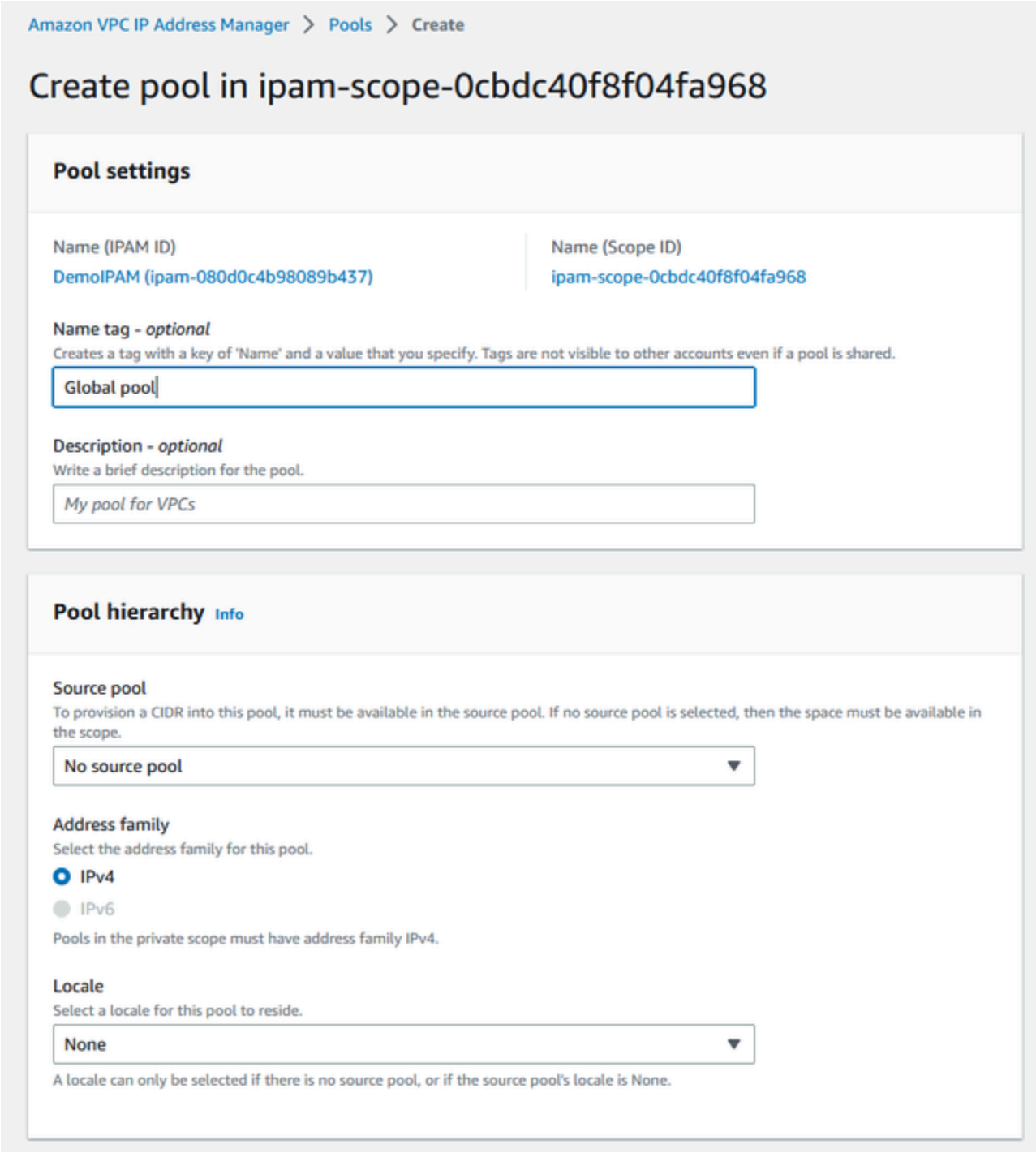
So erstellen Sie einen Pool der obersten Ebene

1. Öffnen Sie mit dem IPAM-Administratorkonto die IPAM-Konsole unter. https://console.aws.amazon.com/ipam/

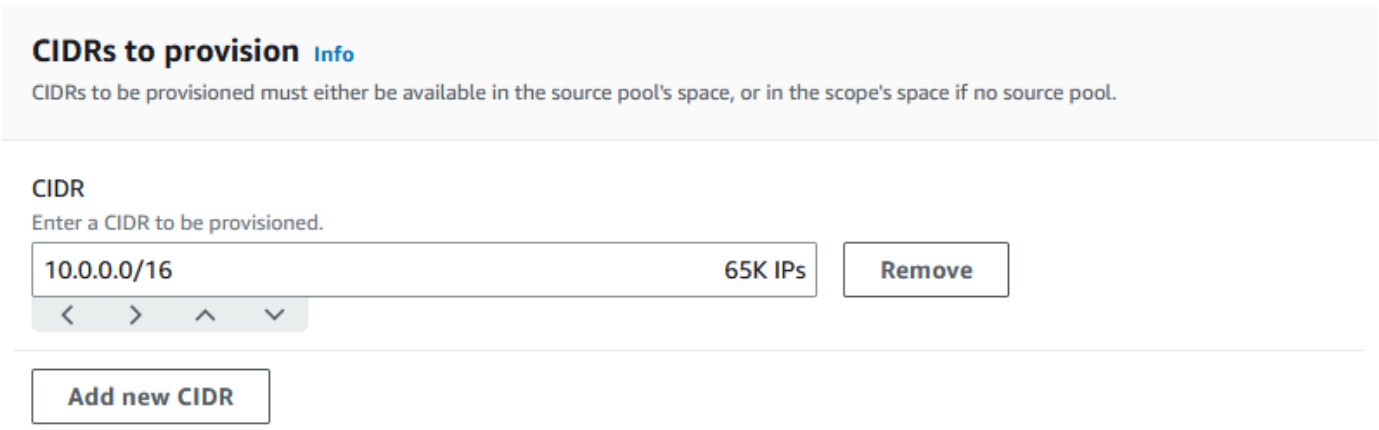
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich aus.



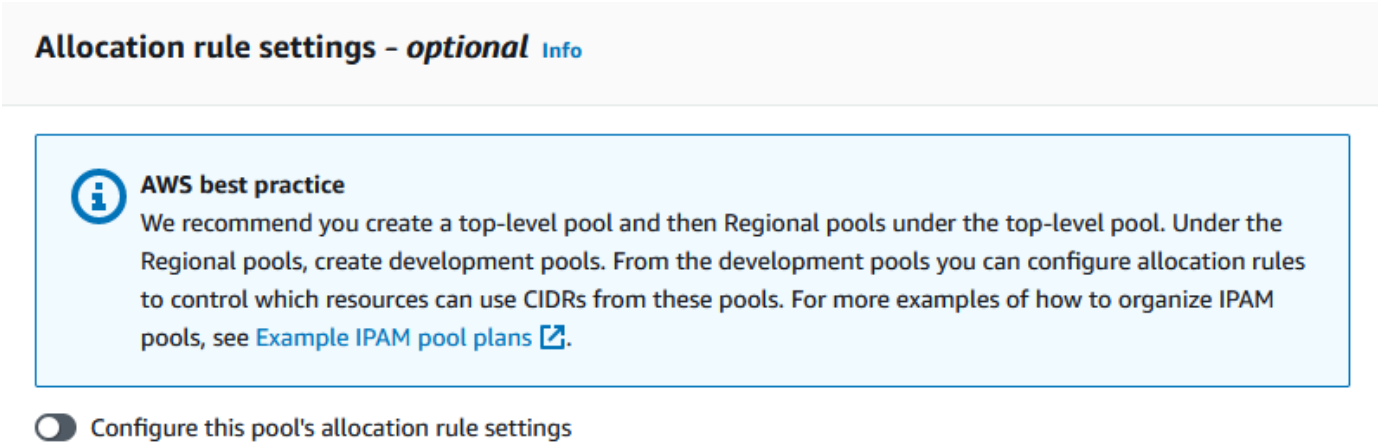
4. Wählen Sie Pool erstellen.
5. Lassen Sie unter IPAM-Bereich den privaten Bereich ausgewählt.
6. (Optional) Fügen Sie ein Namens-Tag und eine Beschreibung für den Pool hinzu, z. B. „Globaler Pool“.
7. Wählen Sie unter Quelle die Option IPAM-Bereich aus. Da es sich hierbei um den Pool der obersten Ebene handelt, verfügt er über keinen Quellpool.
8. Wählen Sie unter Adressfamilie die Option aus. IPv4
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. Gebietsschemas 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.



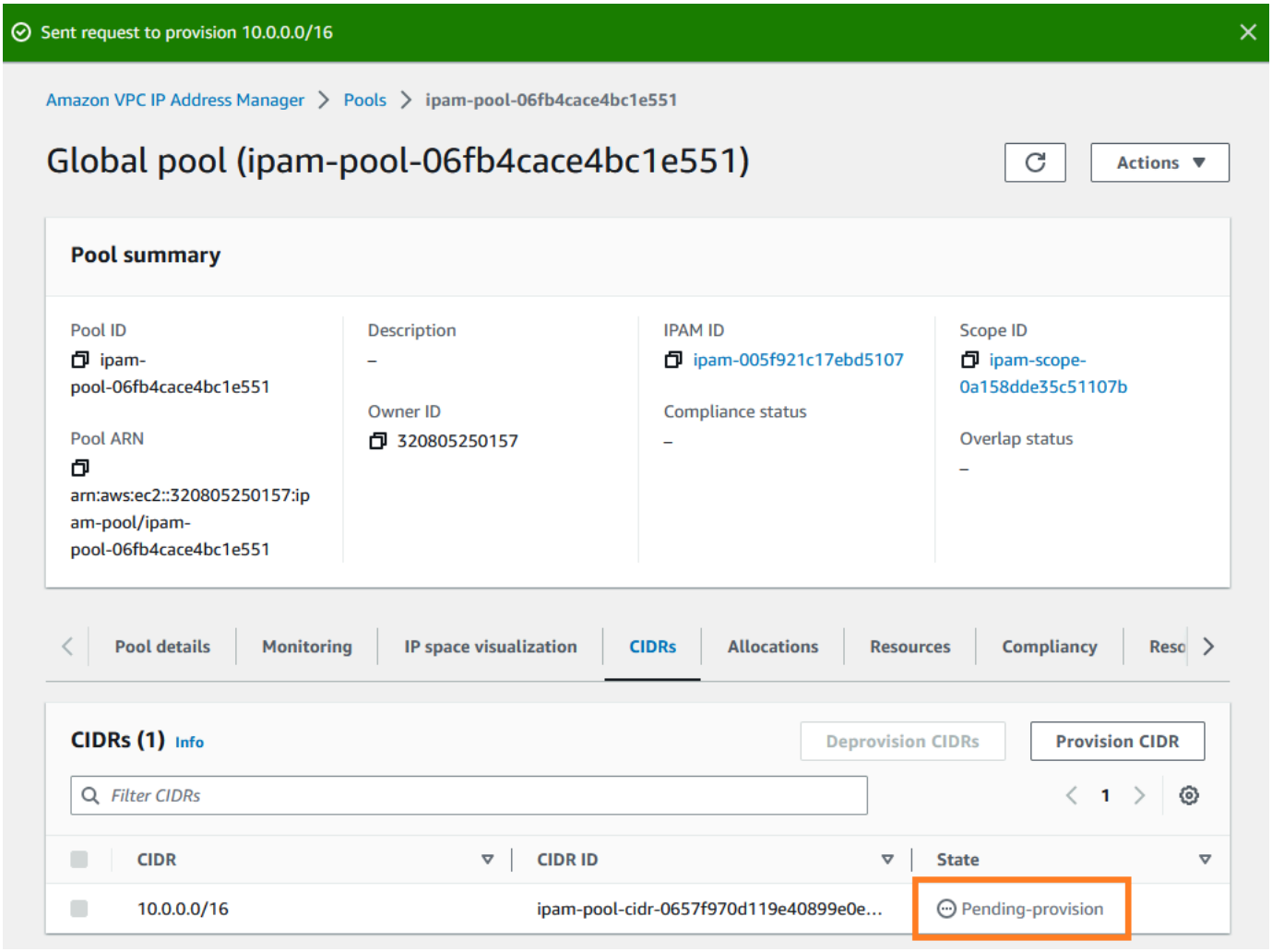
11. Wählen Sie ein CIDR aus, das für den Pool bereitgestellt werden soll. In diesem Beispiel stellen wir 10.0.0.0/16 bereit.



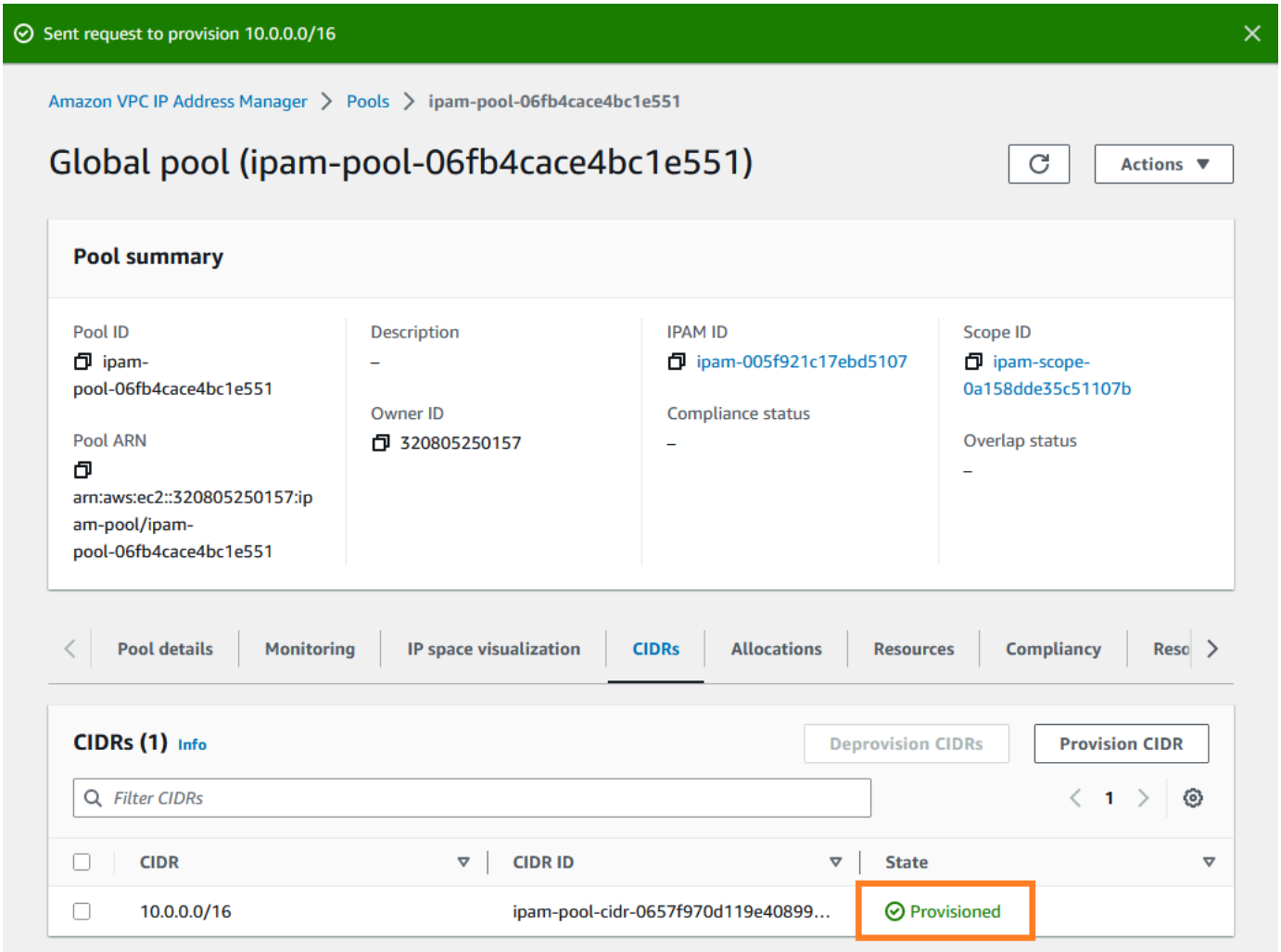
12. Lassen Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren deaktiviert. Dies ist unser Pool auf oberster Ebene, und Sie werden die Zuteilung nicht VPCs direkt von diesem Pool aus CIDRs vornehmen. Stattdessen weisen Sie sie aus einem Unterpool zu, den Sie anhand dieses Pools erstellen.



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.

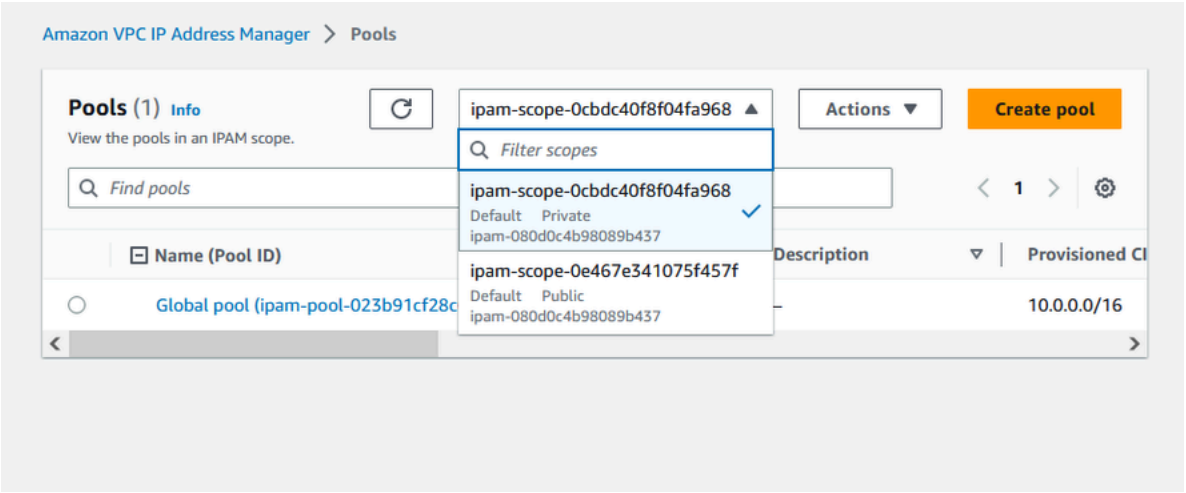
Schritt 4: Erstellen regionaler IPAM-Pools

Dieser Abschnitt veranschaulicht, wie Sie die IP-Adressen mithilfe von zwei regionalen Pools organisieren. In diesem Tutorial folgen wir einem der Beispiele für IPAM-Poolpläne und erstellen zwei regionale Pools, die von den Mitgliedskonten in Ihrer Organisation für die Zuweisung CIDRs zu ihren Pools verwendet werden können. VPCs

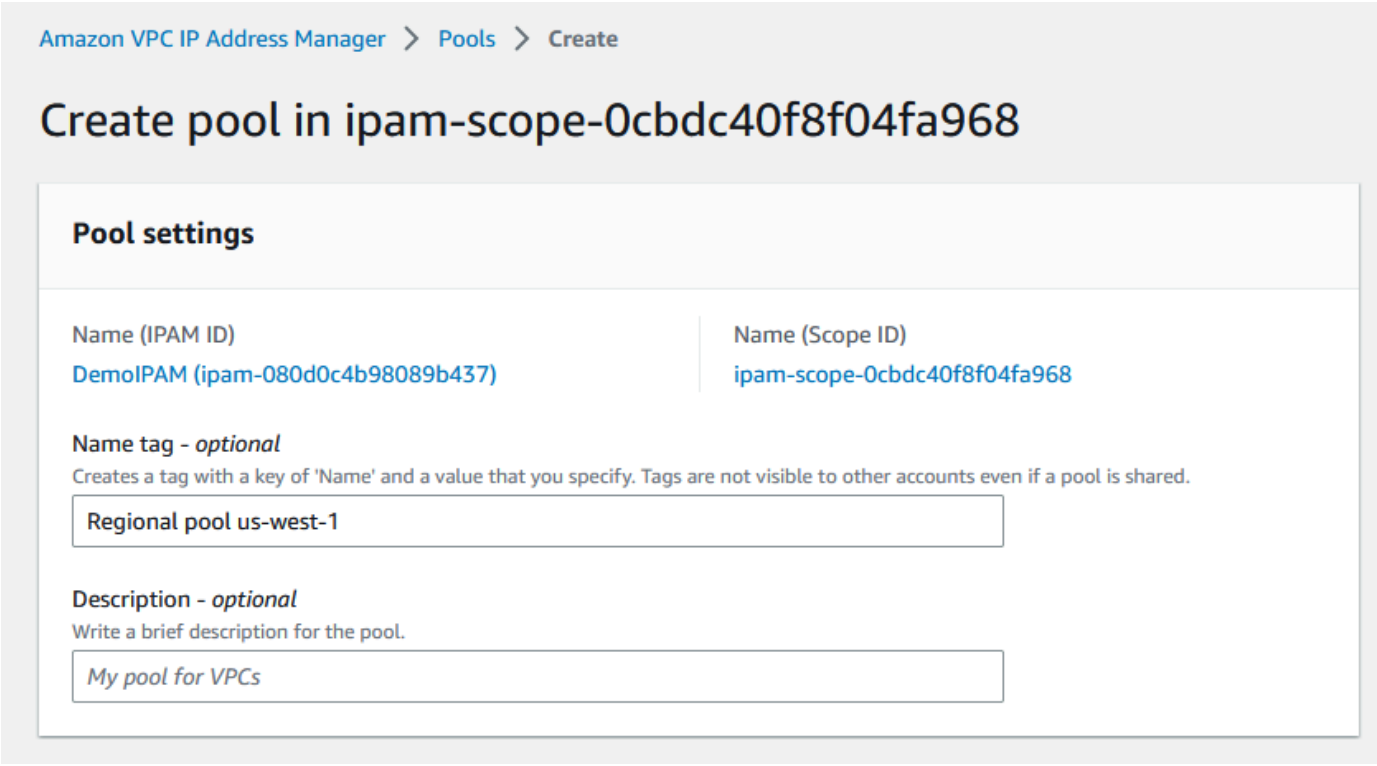
So erstellen Sie einen regionalen Pool

1. Öffnen Sie mit dem IPAM-Administratorkonto die IPAM-Konsole unter. https://console.aws.amazon.com/ipam/

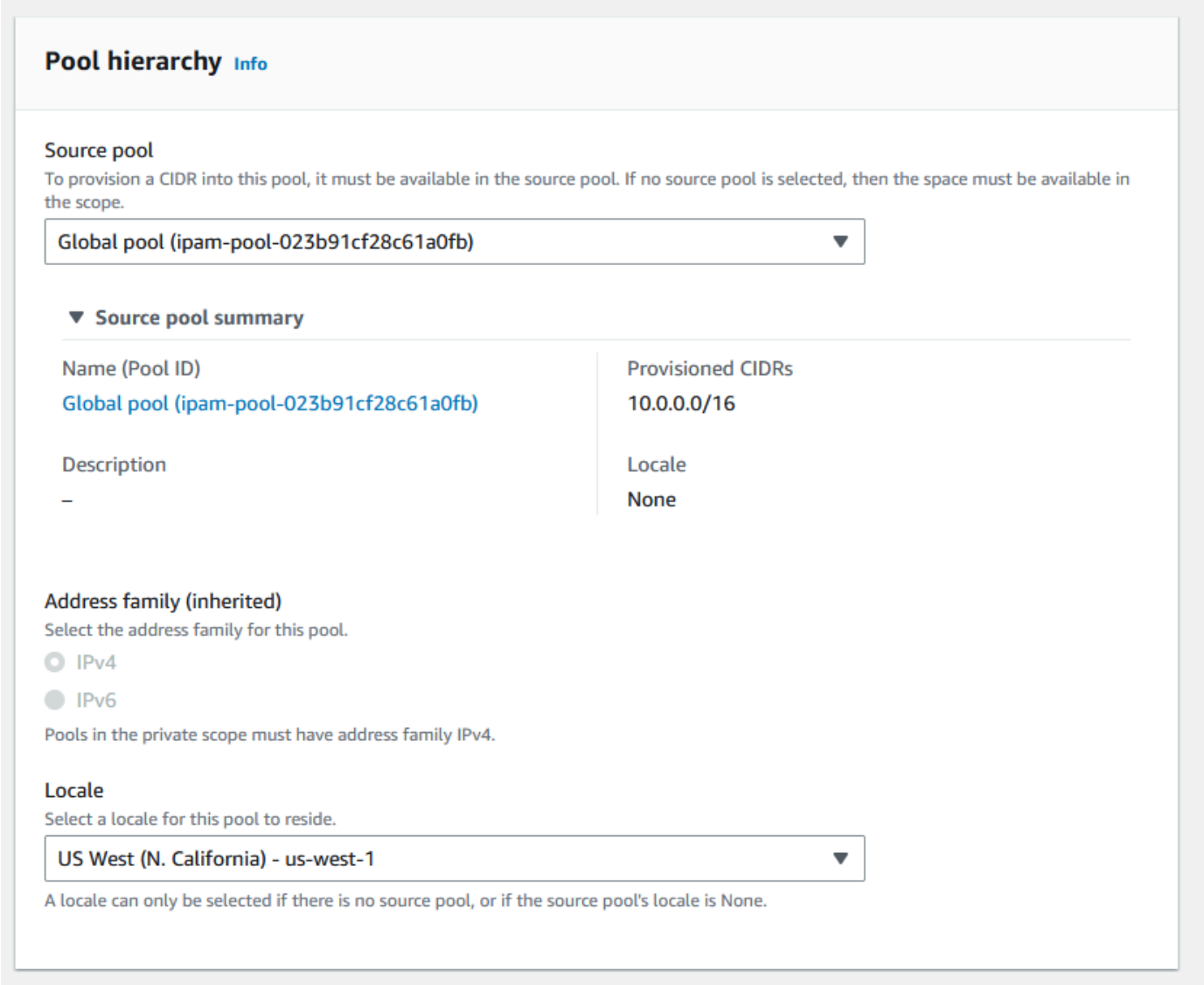
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich aus.



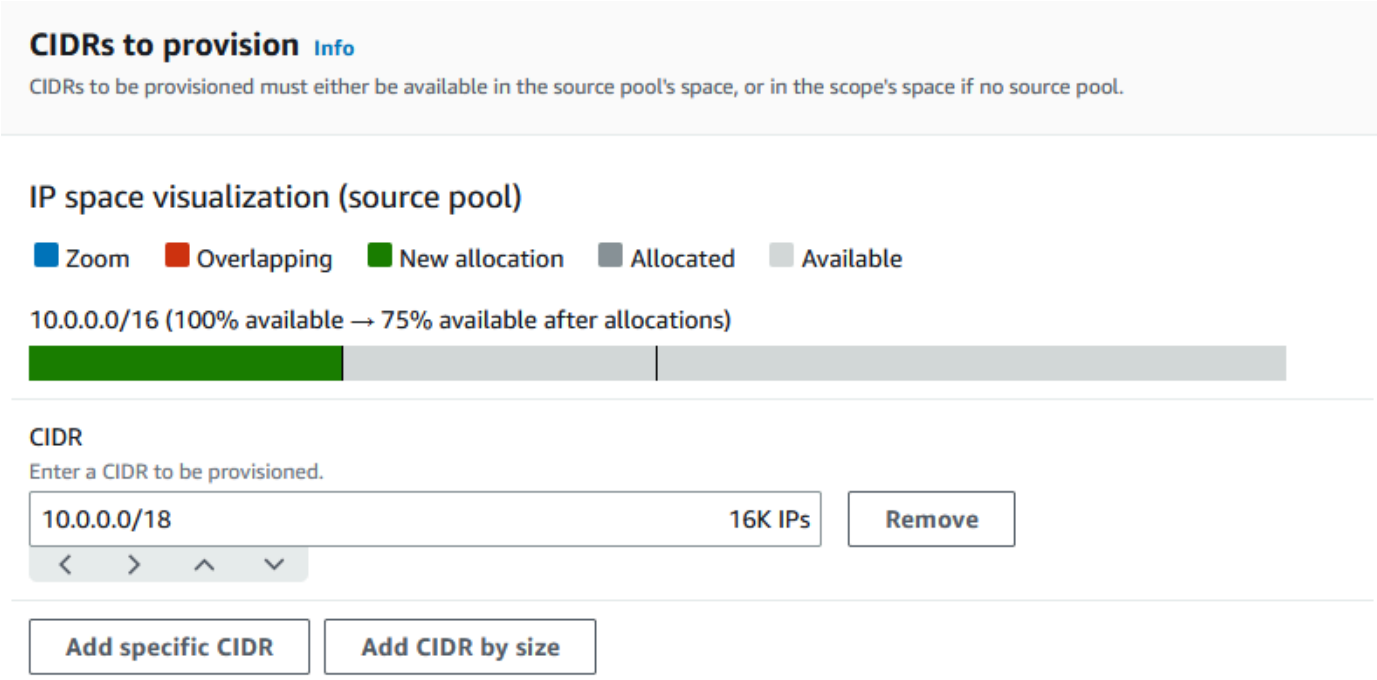
4. Wählen Sie Pool erstellen.
5. Lassen Sie unter IPAM-Bereich den privaten Bereich ausgewählt.
6. (Optional) Fügen Sie ein Namens-Tag und eine Beschreibung für den Pool hinzu, z. B. Regionaler Pool us-west-1.



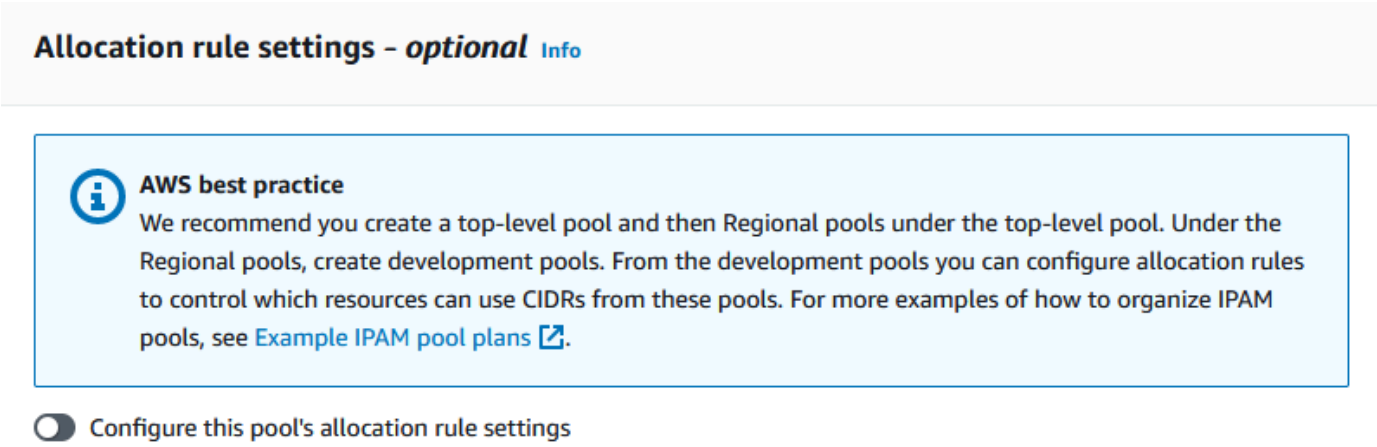
7. Wählen Sie unter Quelle die Option IPAM-Pool und den Pool der obersten Ebene aus („Globaler Pool“), den Sie in Schritt 3: Erstellen Sie einen IPAM-Pool der obersten Ebene erstellt haben. Wählen Sie dann unter Gebietsschema die Option us-west-1 aus.



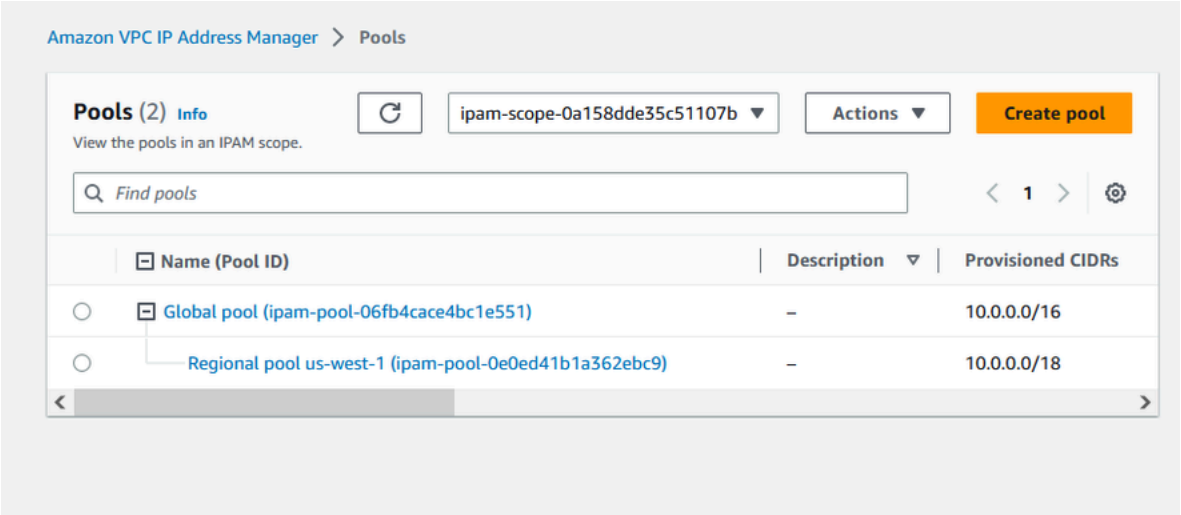
8. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt. Weitere Informationen zur Verwendung dieser Option zur Planung des Subnetz-IP-Bereichs innerhalb einer VPC finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen.
9. Geben CIDRs Sie unter Bereitstellung den Wert 10.0.0.0/18 ein, wodurch dieser Pool rund 16.000 verfügbare IP-Adressen erhält.



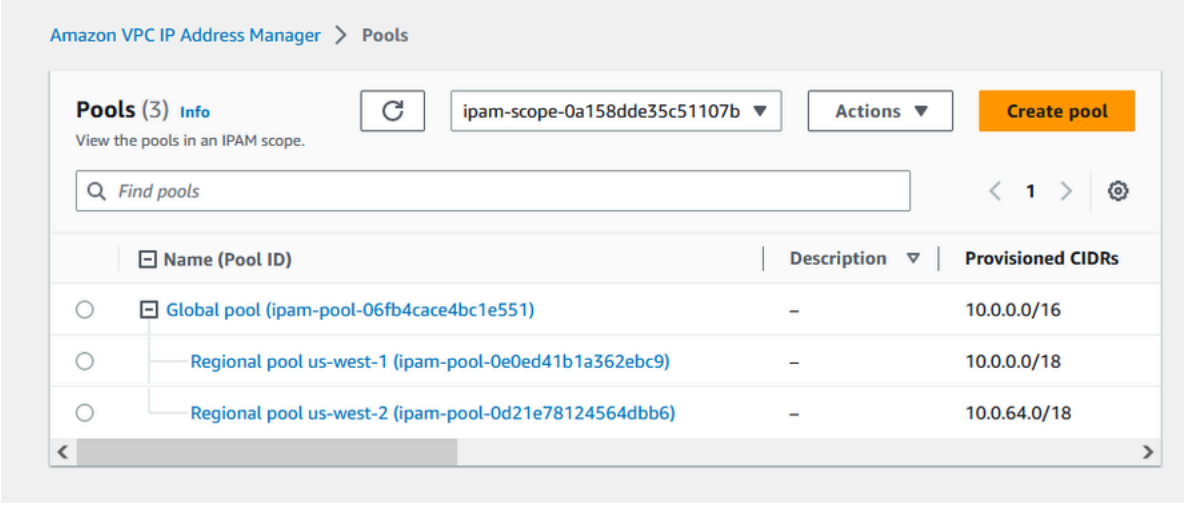
10. Lassen Sie Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren deaktiviert. Sie werden die Zuteilung CIDRs nicht VPCs direkt von diesem Pool aus vornehmen. Stattdessen weisen Sie sie aus einem Unterpool zu, den Sie anhand dieses Pools erstellen.



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:

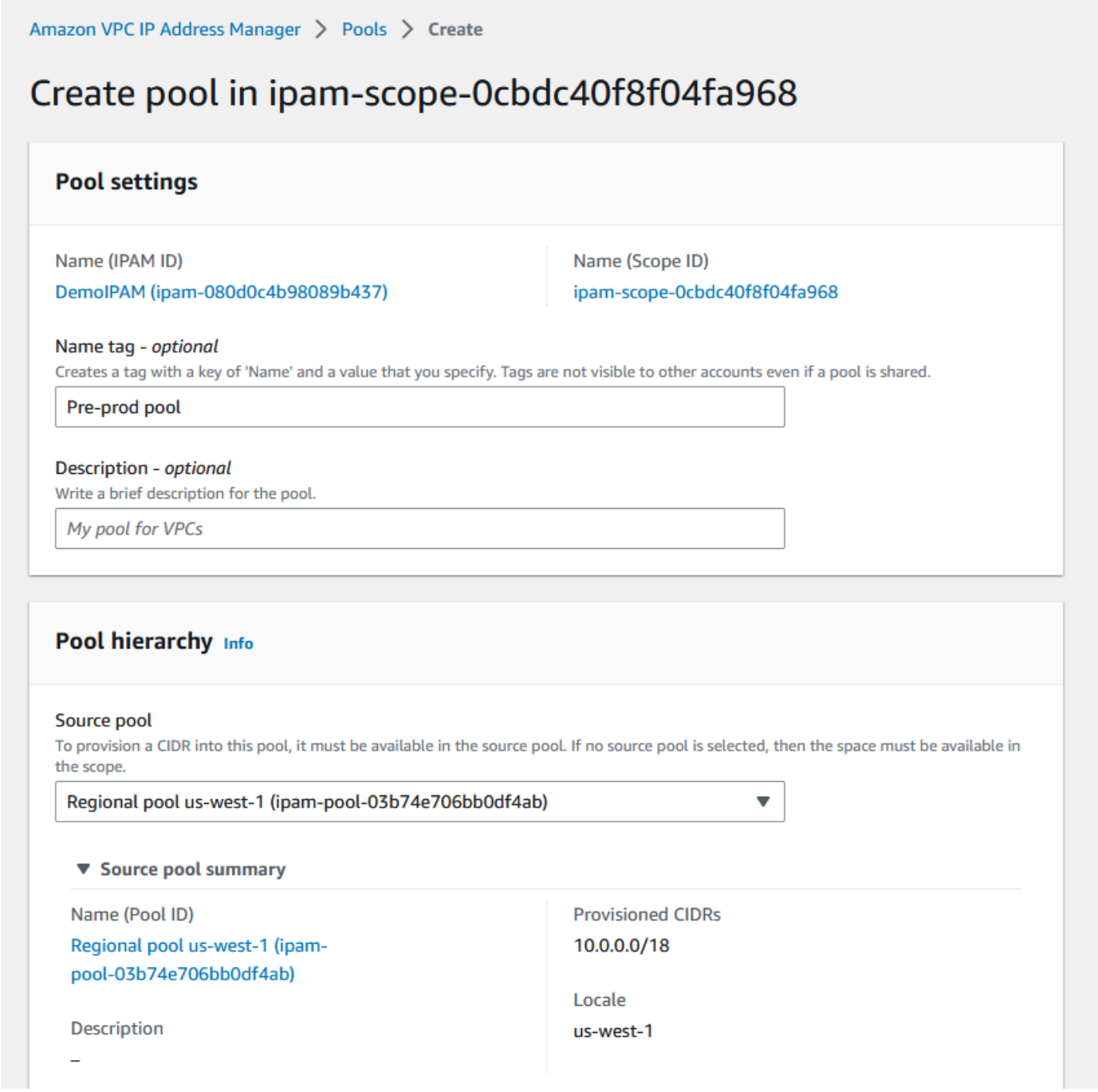


Schritt 5: Erstellen eines Entwicklungspools für die Vorproduktion

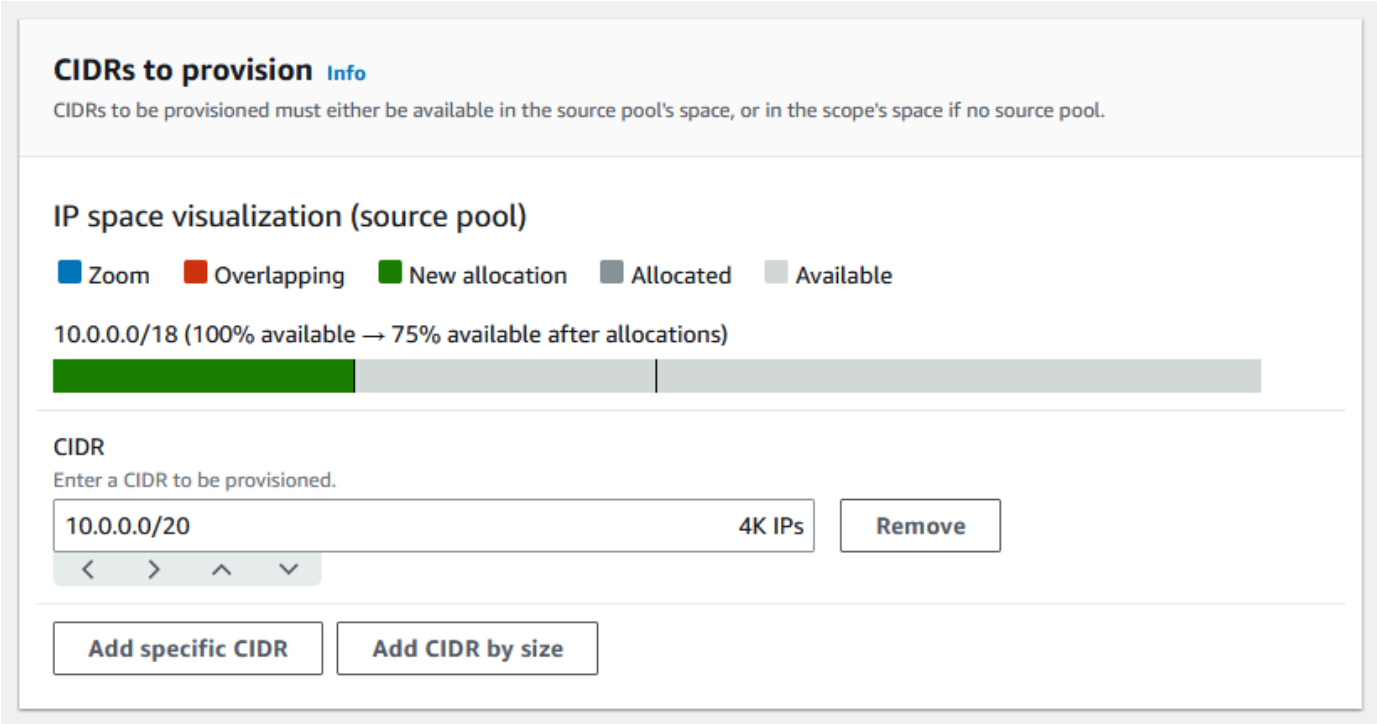
Führen Sie die Schritte in diesem Abschnitt aus, um in einem Ihrer regionalen Pools einen Entwicklungspool für Vorproduktionsressourcen zu erstellen.

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.

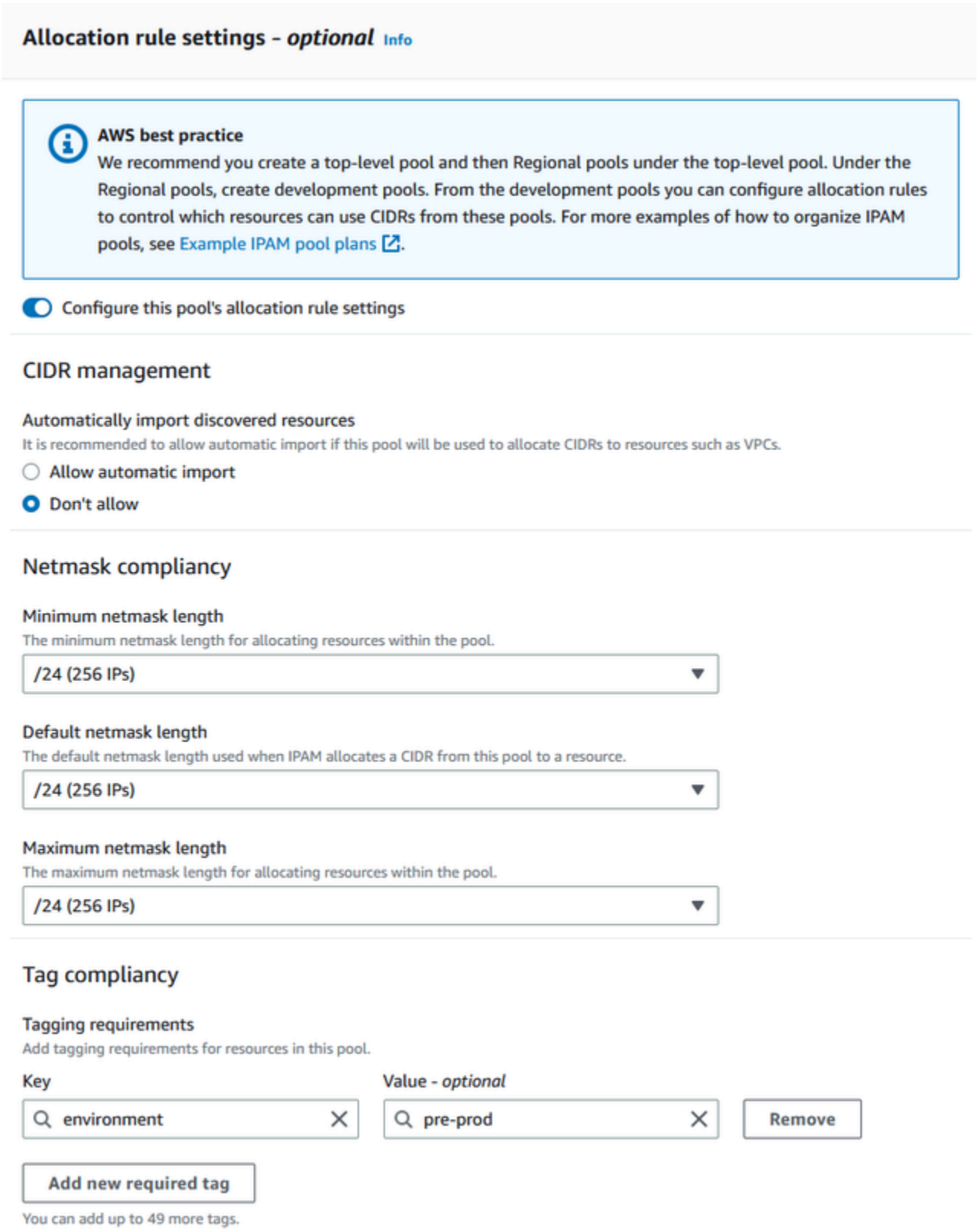


2. Geben Sie als bereitzustellenden CIDR „10.0.0.0/20“ an. Dadurch erhält dieser Pool rund 4 000 IP-Adressen.



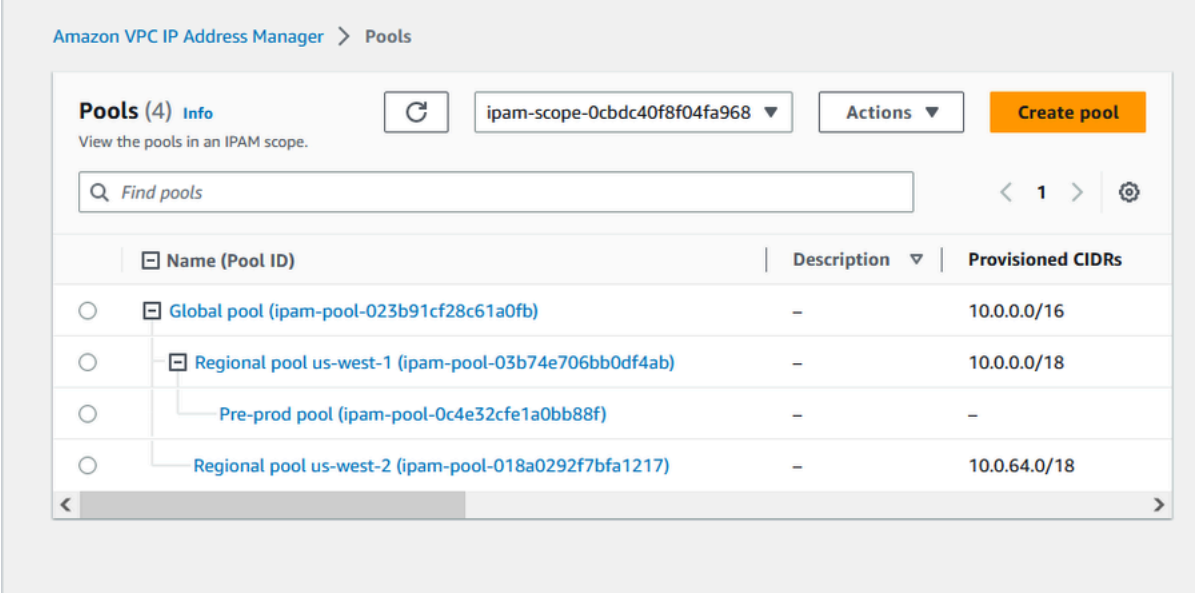
3. Schalten Sie die Option Einstellungen für die Zuweisungsregeln dieses Pools konfigurieren um. Gehen Sie wie folgt vor:

   1. Lassen Sie unter CIDR-Verwaltung für Entdeckte Ressourcen automatisch importieren die Standardoption Nicht erlauben aktiviert. Diese Option würde es IPAM ermöglichen, automatisch Ressourcen zu importieren, die CIDRs es im Gebietsschema des Pools entdeckt. Eine detaillierte Beschreibung dieser Option würde den Rahmen dieses Tutorials sprengen. Unter Erstellen Sie einen Pool auf oberster Ebene IPv4 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 Sie einen Pool auf oberster Ebene IPv4 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, um Speicherplatz aus VPCs dem Pool zuzuweisen. 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

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

Dieser Abschnitt besteht aus zwei Unterabschnitten:

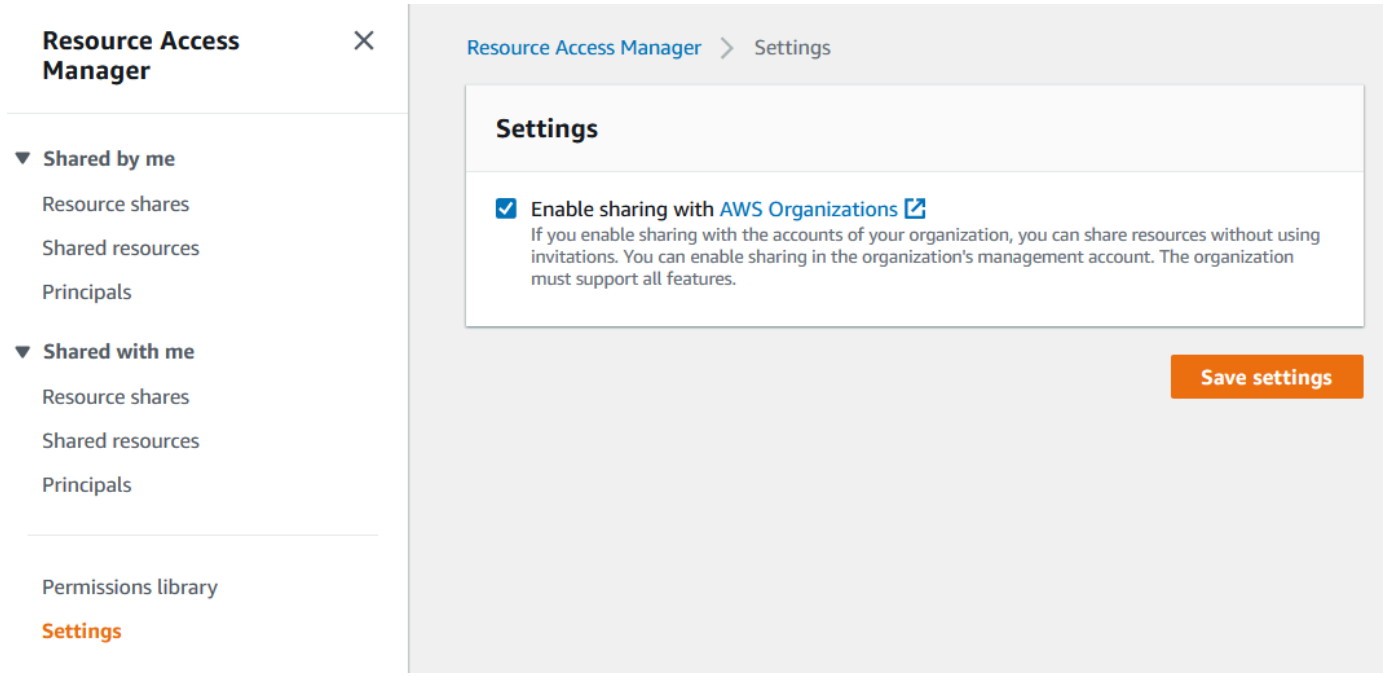
- Schritt 6.1. Aktivieren der Ressourcenfreigabe in AWS RAM: Dieser Schritt muss über das AWS Organizations -Verwaltungskonto ausgeführt werden.
- Schritt 6.2. Teilen Sie einen IPAM-Pool mit AWS RAM: Dieser Schritt muss vom IPAM-Administrator ausgeführt werden.

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. Bevor Sie einen IPAM-Pool gemeinsam nutzen, führen Sie die Schritte in diesem Abschnitt aus, um die gemeinsame Nutzung von Ressourcen für zu aktivieren. AWS RAM

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.

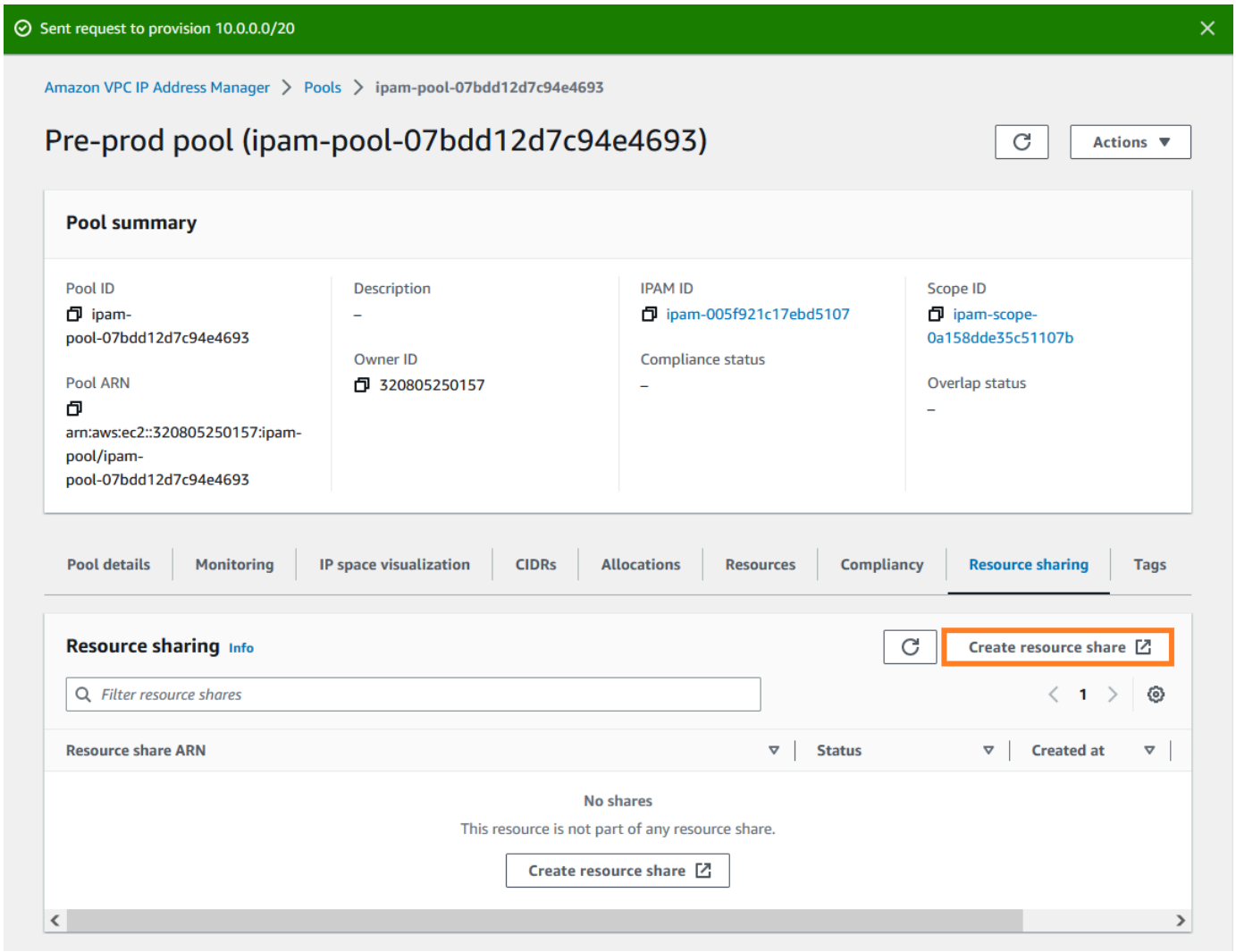
Schritt 6.2. Teilen Sie einen IPAM-Pool mit AWS RAM

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 mithilfe von RAM AWS.

Um einen IPAM-Pool gemeinsam zu nutzen mit AWS RAM

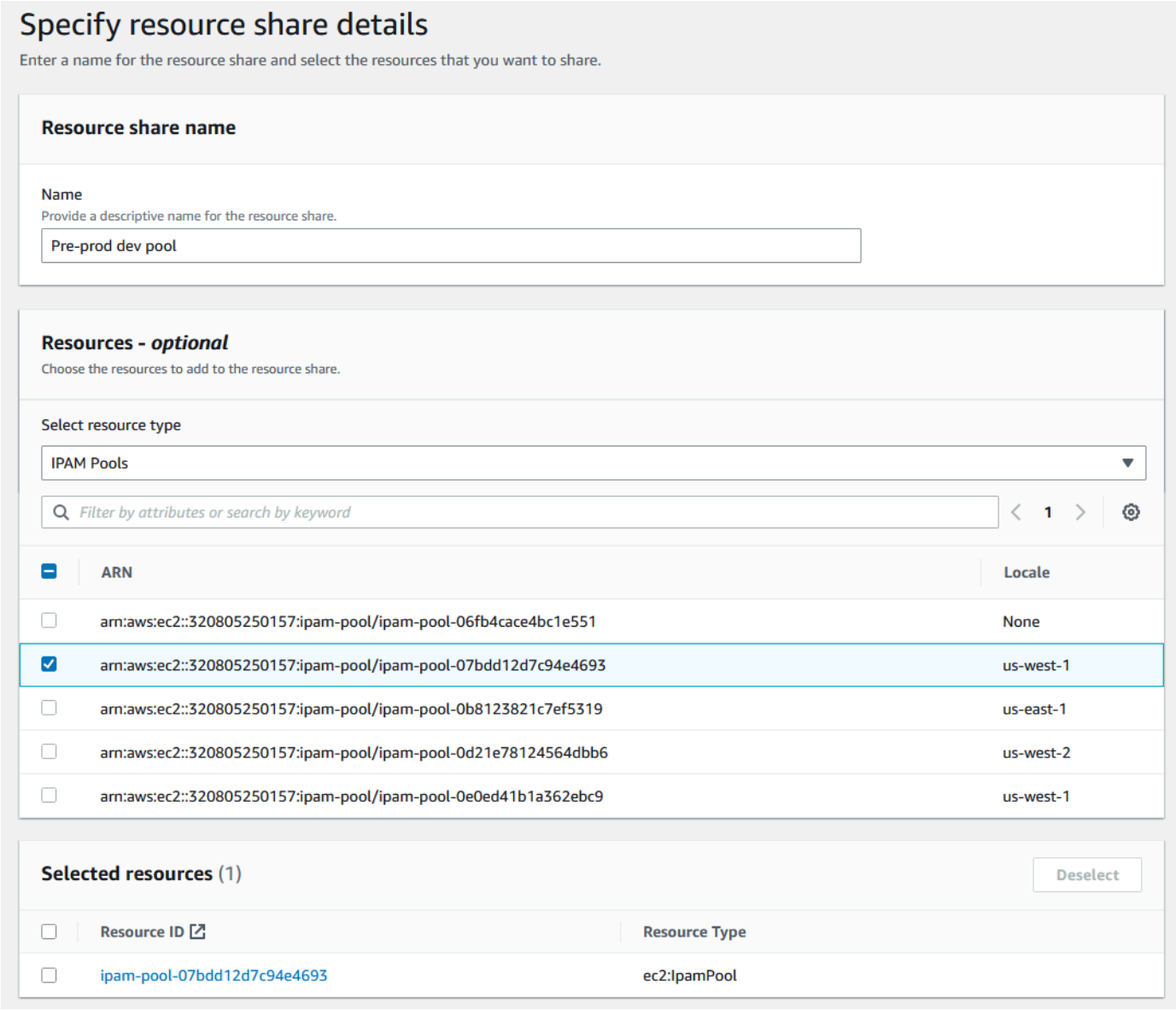
1. Öffnen Sie mit dem IPAM-Administratorkonto die IPAM-Konsole unter. https://console.aws.amazon.com/ipam/
2. Wählen Sie im Navigationsbereich Pools aus.
3. Wählen Sie den privaten Bereich und dann den IPAM-Pool für die Vorproduktion aus. Wählen Sie anschließend Aktionen > Details anzeigen aus.

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

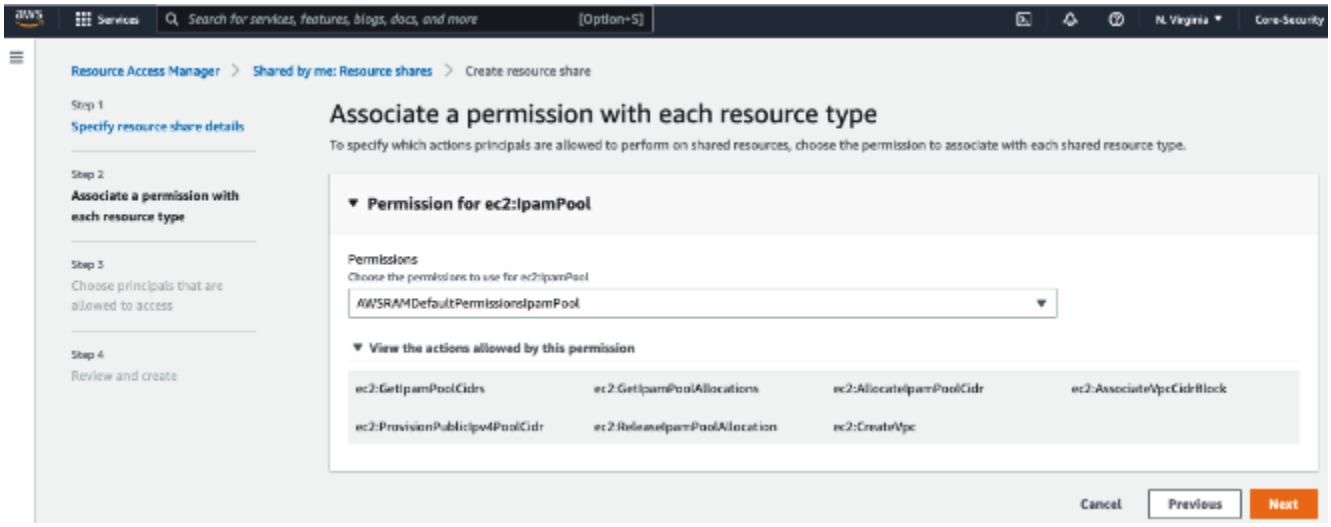


Die AWS RAM Konsole wird geöffnet.

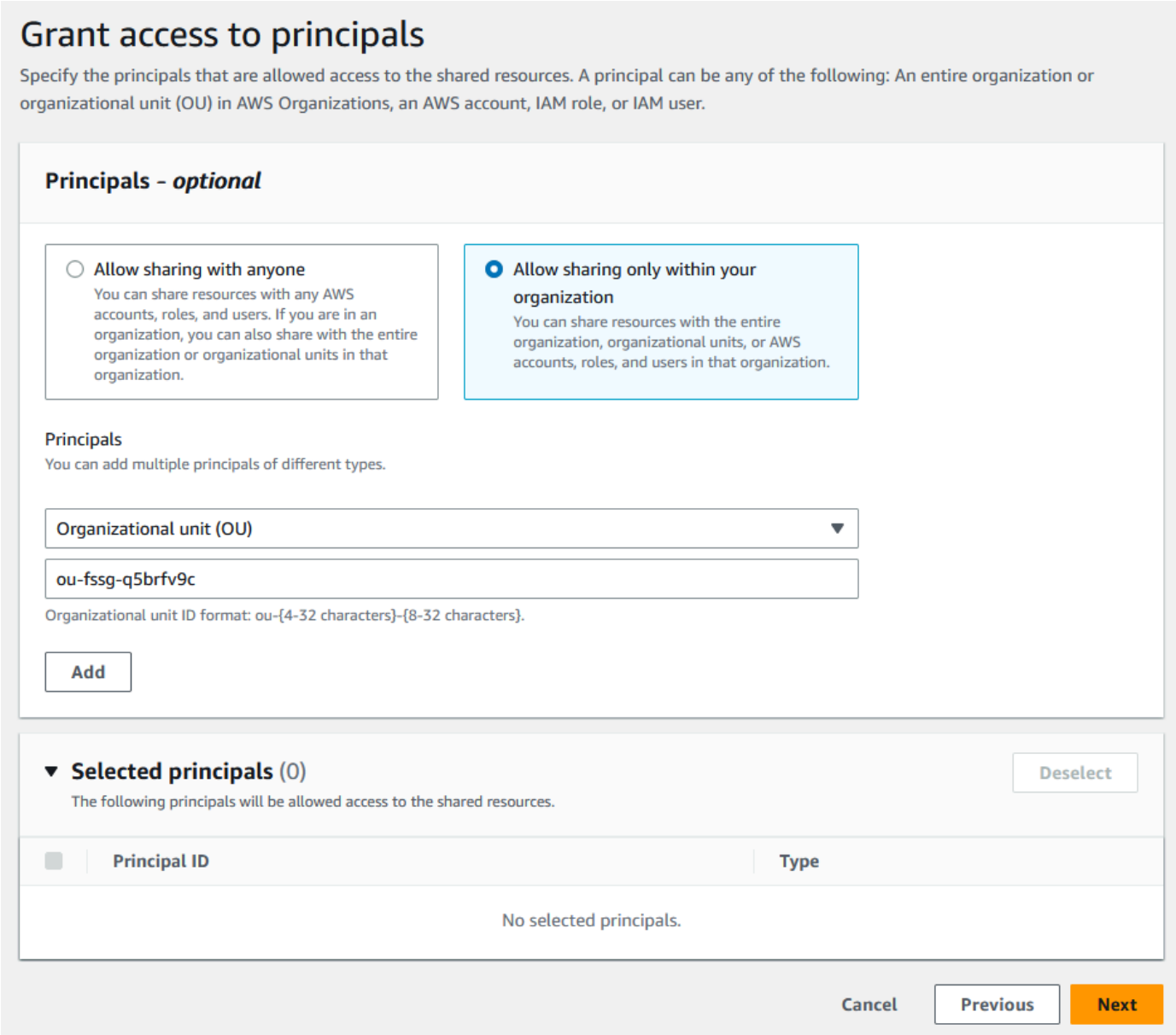
6. Wählen Sie in der AWS RAM Konsole erneut Create a resource share aus.
7. Fügen Sie einen Namen für den freigegebenen Pool hinzu.
8. Wählen Sie unter Ressourcentyp auswählen die Option IPAM-Pools und dann den ARN des Entwicklungspools für die Vorproduktion aus.



9. Wählen Sie Weiter.
10. Lassen Sie die AWSRAMDefaultPermissionsIpamPoolStandardberechtigung ausgewählt. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mithilfe von RAM AWS können Sie jedoch mehr über diese Optionen erfahren.



11. Wählen Sie Weiter.
12. Wählen Sie unter Prinzipale die Option Zulassen der Freigabe nur innerhalb der eigenen Organisation aus. Geben Sie die ID Ihrer AWS Organizations Organisationseinheit ein (wie unter beschrieben)Wie AWS Organizations lässt es sich mit IPAM integrieren, und wählen Sie dann Hinzufügen aus.



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

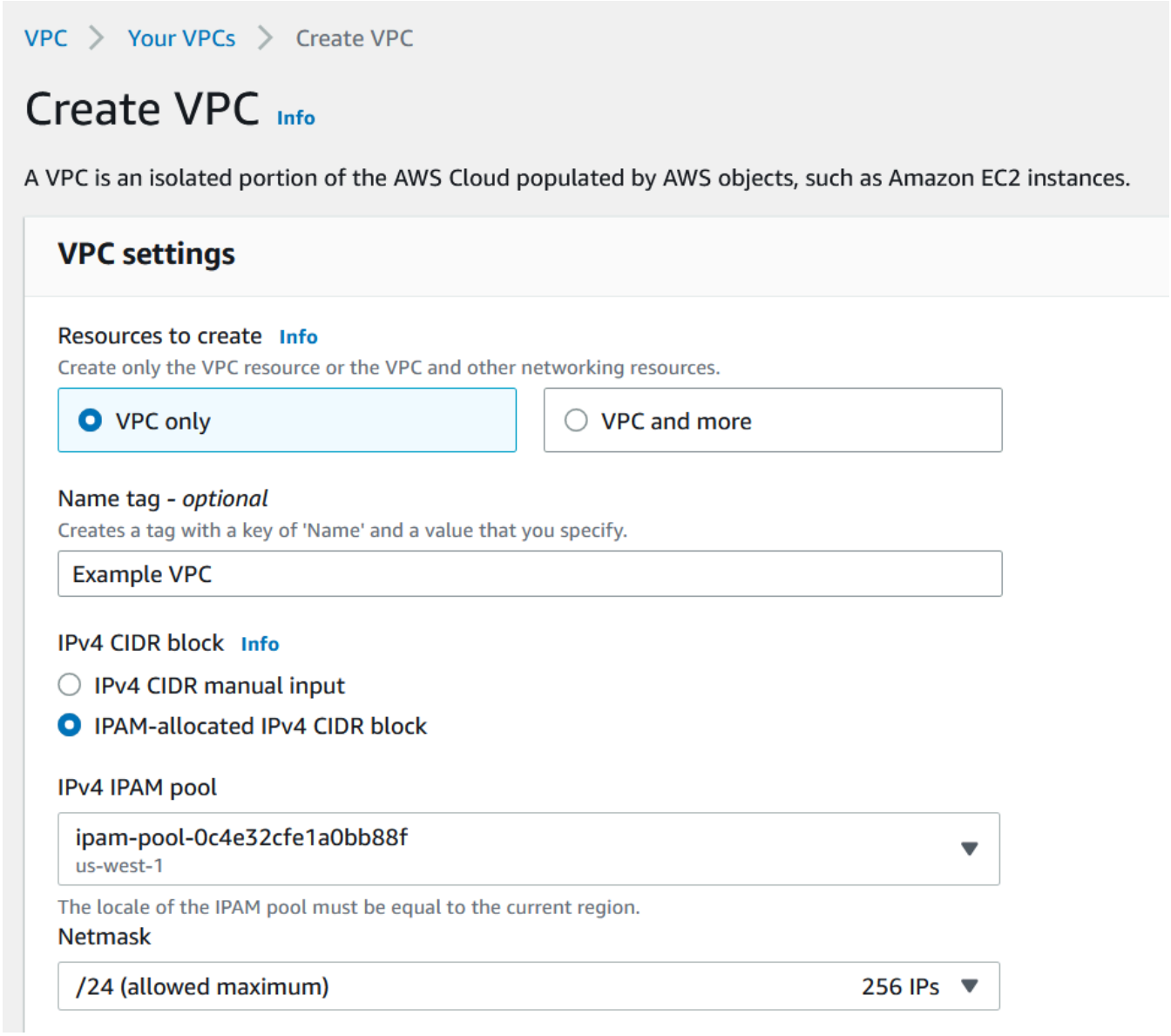
Nach der Freigabe des Pools fahren Sie mit dem nächsten Schritt fort, um eine VPC mit einem CIDR zu erstellen, das aus einem IPAM-Pool zugewiesen wird.

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 von dem Mitgliedskonto in der Organisationseinheit abgeschlossen werden, mit der der IPAM-Pool im vorherigen Abschnitt gemeinsam genutzt wurde („ example-member-account-2 in“ genanntWie AWS Organizations lässt es sich mit IPAM integrieren). Weitere Informationen zu den IAM-Berechtigungen, die für die Erstellung erforderlich sind VPCs, finden Sie in den Amazon VPC-Richtlinienbeispielen im Amazon VPC-Benutzerhandbuch.

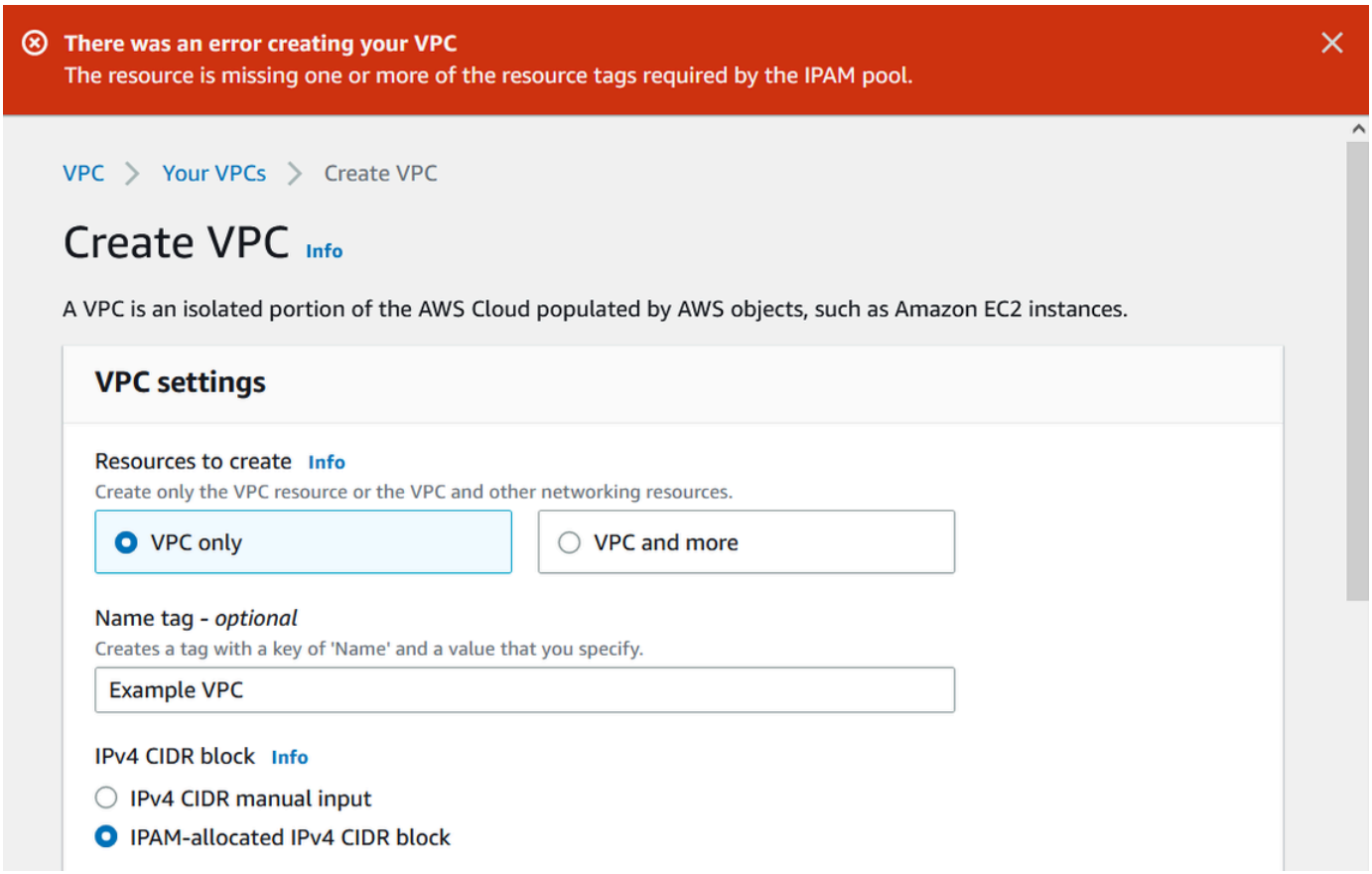
So erstellen Sie eine VPC mit einem CIDR, das aus einem IPAM-Pool zugewiesen wird

1. Öffnen Sie mit dem Mitgliedskonto die VPC-Konsole unter https://console.aws.amazon.com/vpc/dem 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 den IPAM-zugewiesenen CIDR-Block IPv4 .
    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.

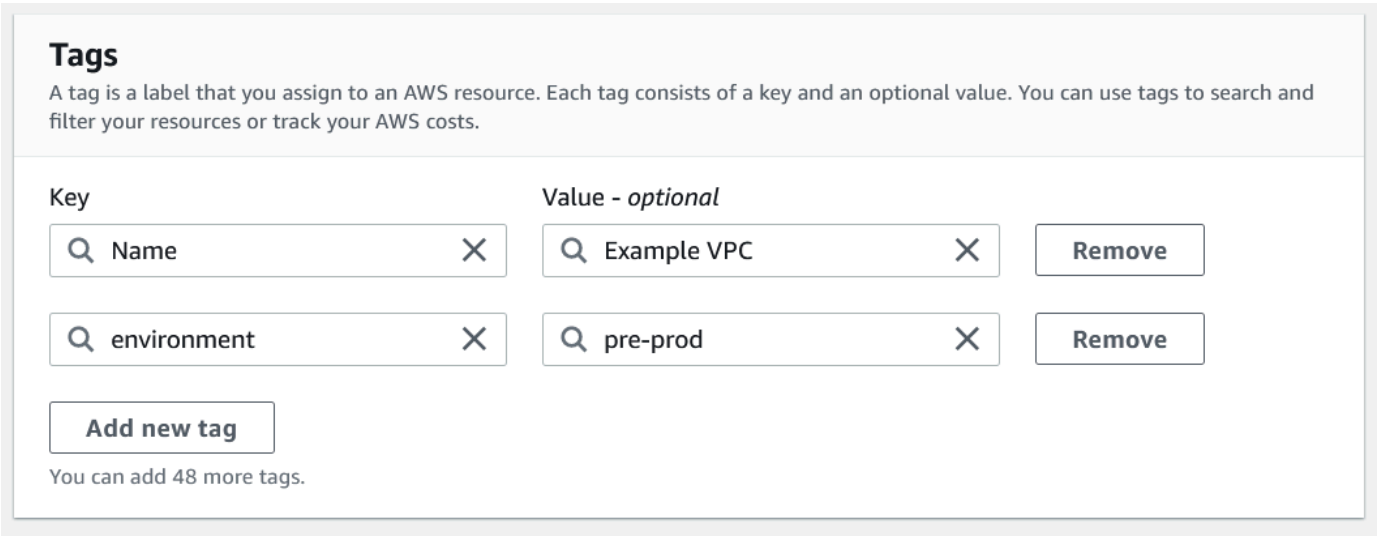


4. Fügen Sie – zu Demonstrationszwecken – unter Tags zum jetzigen Zeitpunkt keine zusätzlichen Tags hinzu. Als Sie den Pre-Prod-Pool (in Schritt 5: Erstellen eines Entwicklungspools für die Vorproduktion) erstellt haben, haben Sie eine Zuweisungsregel hinzugefügt, nach der alle VPCs , die mit CIDRs diesem Pool erstellt wurden, vorerst das Tag environment/pre-prod tag. Leave the environment/pre -prod deaktivieren müssen, sodass Sie sehen können, dass eine Fehlermeldung angezeigt wird, die Ihnen mitteilt, 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

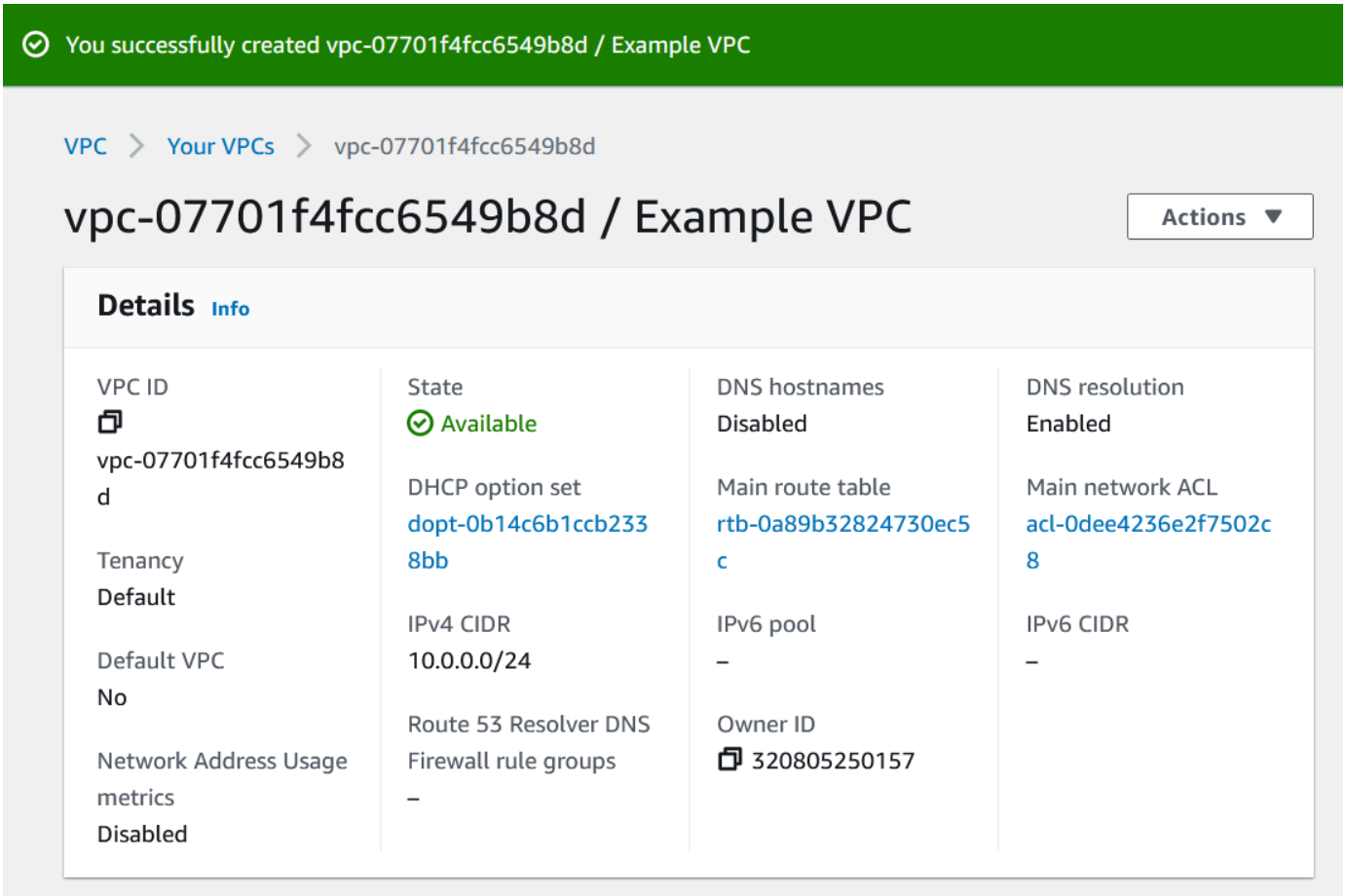
festgelegt haben. Gemäß der Zuweisungsregel müssen alle VPCs , die mit diesem Pool erstellt wurden, über ein CIDRs Umgebungs-/Pre-Prod-Tag verfügen.



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.

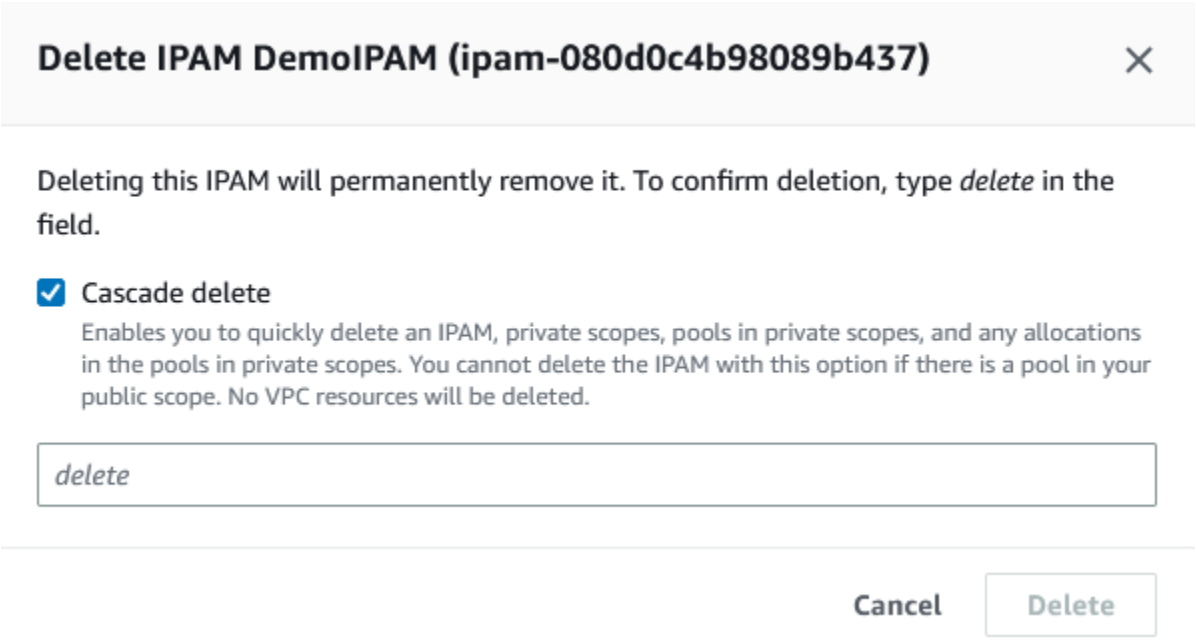
Schritt 8: Bereinigen

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 Beispiel-Ressourcenfreigabe in der Konsole. AWS RAM 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 AWS Organizations Verwaltungskonto bei der IPAM-Konsole an, wählen Sie Einstellungen und entfernen Sie das delegierte Administratorkonto.

8. (Optional) Wenn Sie IPAM mit integrieren AWS Organizations, erstellt IPAM automatisch eine dienstverknüpfte Rolle in jedem Mitgliedskonto. Melden Sie sich mit jedem AWS Organizations Mitgliedskonto bei IAM an und löschen Sie die mit dem AWSServiceRoleForIPAM-Dienst verknüpfte Rolle in jedem Mitgliedskonto.
9. Die Bereinigung ist abgeschlossen.

Tutorial: Erstellen Sie ein IPAM und Pools mit dem AWS CLI

Folgen Sie den Schritten in diesem Tutorial, um ein IPAM AWS CLI 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 Region 1, Region 2 AWS AWS
  - Privater Bereich
    - Pool auf oberster Ebene
      - Regionalpool 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 5. Erstellen Sie einen regionalen Pool mit CIDR aus dem Pool der obersten Ebene
- Schritt 6: Stellen Sie ein CIDR für den regionalen Pool bereit
- 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 CLI zu konfigurieren. AWS Weitere Informationen zur Rolle des IPAM-Kontos finden Sie unter Integrieren Sie IPAM mit Konten in einer Organisation AWS.

Diese Anfrage muss von einem Verwaltungskonto einer AWS Organizations aus gestellt 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.

Um ein IPAM mit dem zu erstellen 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, geht AWS automatisch wie folgt vor:

   - 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 Sie einen IPv4 Adresspool

Folgen Sie den Schritten in diesem Abschnitt, um einen IPv4 Adresspool zu erstellen.

> **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 das Gebietsschema von hat`None`, ist der Pool für VPC-Ressourcen in keiner AWS Region verfügbar. Sie können den IP-Adressraum im Pool nur manuell zuweisen, um Speicherplatz zu reservieren.

Um einen IPv4 Adresspool für all Ihre AWS Ressourcen zu erstellen, verwenden Sie AWS CLI

1. Führen Sie den folgenden Befehl aus, um einen IPv4 Adresspool 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 Bereitstellung CIDRs für einen Pool.

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-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 IPAM-Region. 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.

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-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 Sie IPAM mit Konten in einer Organisation AWSabgeschlossen haben.

Wenn Sie eine AWS RAM-Freigabe für den IPAM-Pool erstellen, werden IP-Zuweisungen für alle Konten aktiviert. RAM-Sharing 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 mithilfe von RAM AWS.

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 Sie die 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: IP-Adressverlauf anzeigen mit dem 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 finden Sie unter Verwenden von AWS CLI im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle. AWS CLI

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 Instanzen, die ausgeführt werden
- EC2 Netzwerkschnittstellen, die mit Instanzen verbunden sind

Important

Obwohl IPAM keine EC2 Amazon-Instances oder EC2 Netzwerkschnittstellen überwacht, die mit Instances verbunden sind, können Sie die Funktion „IP-Verlauf durchsuchen“ verwenden, um nach historischen Daten auf EC2 Instances und CIDRs Netzwerkschnittstellen zu suchen.

Note

- Die Befehle in diesem Tutorial müssen mit dem Konto ausgeführt werden, dem das IPAM gehört, und der AWS Region, in der das IPAM gehostet wird.
- Aufzeichnungen über Änderungen CIDRs werden in regelmäßigen Snapshots erfasst, was bedeutet, dass es einige Zeit dauern kann, bis die Datensätze angezeigt oder aktualisiert werden, und die Werte für SampledStartTime und SampledEndTime können sich von den tatsächlichen Zeitpunkten unterscheiden.

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 folgenden 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 der CIDR im Laufe des Zeitraums einer Netzwerkschnittstelle und einer EC2 Instanz zugewiesen. Beachten Sie, dass kein SampledEndTimeWert 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"
        }
    ]
```

```
}
```

Wenn sich die Besitzer-ID der Instanz, an die eine Netzwerkschnittstelle angeschlossen ist, von der Besitzer-ID der Netzwerkschnittstelle unterscheidet (wie dies bei NAT-Gateways, Lambda-Netzwerkschnittstellen in VPCs und anderen AWS Diensten der Fall ist), `ResourceOwnerId` ist dies und `amazon-aws` nicht 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 folgenden 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 SampledEndTimeWert 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 der CIDR im VPCs Laufe des Zeitraums in einer Region außerhalb der IPAM-Heimatregion zwei verschiedenen Gruppen zugewiesen. Beachten Sie, dass kein SampledEndTimeWert 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 folgenden 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 der CIDR im VPCs Laufe des Zeitraums zahlreichen Subnetzen zugewiesen. Beachten Sie, dass kein SampledEndTimeWert 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 folgenden 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 der CIDR im Laufe des Zeitraums einer Netzwerkschnittstelle und einer EC2 Instanz zugewiesen. Beachten Sie, dass kein SampledEndTimeWert 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 folgenden 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 SampledEndTimeWert 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 `54.0.0.9/32` wird eine Elastic IP-Adresse zugewiesen, die nicht Teil der AWS Organisation ist, die in Ihr IPAM integriert ist.

1. Führen Sie den folgenden 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 in diesem Beispiel einer Elastic IP-Adresse zugewiesen `54.0.0.9/32` ist, die nicht Teil der in das IPAM integrierten AWS Organisation 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 sie beispielsweise, ASNs um die Quelle des Netzwerkverkehrs zu identifizieren. Nicht alle

Unternehmen kaufen ihre eigenen Produkte ASNs, aber Unternehmen, die dies tun, können ihre ASN bei uns AWS einreichen.

Mit BYOASN (Bring Your Own Autonomous System Number) können Sie die IPv4 oder IPv6 Adressen, an die Sie uns senden, 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 AWS -ASN, und Ihre Workloads sind für Kunden oder Partner erreichbar, die den aufgelisteten Datenverkehr auf der Grundlage Ihrer IP-Adresse und 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 AWS und für einen Pool in Ihrem öffentlichen Bereich bereitgestellt haben. 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 beim Herstellen des CIDR-Bereichs für die IP-Adresse erstellt haben, AWS oder Sie können einen

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

- Wenn Sie einen IPv6 Adressbereich IPv4 oder angebenTutorial: Mitbringen eigener IP-Adressen in IPAM, erstellen Sie ein X.509-Zertifikat und laden das X.509-Zertifikat in den RDAP-Datensatz 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.
- Wenn Sie einen IP-Adressbereich zu IPAM hinzufügen, erstellen Sie ein ROA-Objekt, um sicherzustellen, dass Sie den IP-Adressraum kontrollieren, den Sie zu IPAM hinzufügen. Zusätzlich zu diesem ROA-Objekt müssen Sie in Ihrem RIR ein zweites ROA-Objekt mit der ASN haben, die Sie zu IPAM hinzufügen. Wenn Sie dieses zweite ROA-Objekt für die ASN nicht in Ihrem RIR haben, schließen Sie 3 ab. Erstellen Sie ein ROA-Objekt in Ihrem RIR. Ignorieren Sie die anderen Schritte.

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 aus.

3. Wählen Sie Ihren IPAM.
4. Wählen Sie die BYOASNsRegisterkarte und dann Bereitstellung BYOASNs aus.
5. Geben Sie die ASN ein. Infolgedessen wird das Nachrichtenfeld automatisch mit der Nachricht gefüllt, die Sie im nächsten Schritt signieren müssen.

   - Das Format der Nachricht ist wie folgt: 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 Eine weitere ASN bereitstellen. Sie können bis zu 5 bereitstellen. ASNs Informationen zur Erhöhung dieses Kontingents finden Sie unter Kontingente für Ihr IPAM.
10. Wählen Sie Bereitstellung.
11. Sehen Sie sich den Bereitstellungsprozess auf der BYOASNsRegisterkarte an. Warten Sie, bis der Status von Pending-provision zu Provisioned wechselt. BYOASNs wenn die Bereitstellung fehlgeschlagen ist, werden sie 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 eingestellt sein EC2und es muss ein Gebietsschema ausgewählt werden.
15. Wählen Sie die CIDRsRegisterkarte und wählen Sie ein BYOIP CIDR aus.
16. Wählen Sie Aktionen > BYOASN-Zuweisungen verwalten.

17. Wählen Sie unter Zugeordnet die ASN aus BYOASNs, zu der Sie weitergeleitet haben. AWS Wenn Sie mehrere haben ASNs, können Sie dem BYOIP CIDR mehrere ASNs zuordnen. Sie können so viele verknüpfen, ASNs wie Sie zu IPAM hinzufügen können. Beachten Sie, dass Sie standardmäßig bis zu 5 ASNs zu IPAM hinzufügen 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 CIDRsRegisterkarte Pool.
21. Wählen Sie das BYOIP CIDR und Aktionen > Werben aus. Daraufhin werden Ihre ASN-Optionen angezeigt: die Amazon ASN und alle, die ASNs Sie zu IPAM gebracht 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 BYOASNs Registerkarte die ASN aus und wählen Sie ASN deprovision aus. Aus diesem Grund wird die

Bereitstellung der ASN aufgehoben. BYOASNs im Status Deprovisioned werden automatisch nach 7 Tagen 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, sollte der Status nach einigen Minuten auf ProvisionStatus„Bereitgestellt“ gesetzt werden.

```
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 Amazon wieder zu verwenden und ASNs gleichzeitig die CIDR-Werbung 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 BYOIPs, CIDRs mit denen Sie sie verknüpft 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, wie Sie öffentlichen IP-Adressraum in AWS IPAM integrieren und ihn verwalten können.

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 Einrichtung von öffentlichem IP-Bereich AWS: Sie können IPAM verwenden, um öffentlichen IP-Adressraum einmal zu integrieren, und dann IPAM verwenden, um Ihre öffentlichen Daten IPs über Regionen auf Ressourcen wie EC2 Instances und Load Balancer für Anwendungen zu verteilen. Ohne IPAM müssen Sie Ihr Publikum IPs für jede Region einbinden. AWS

Inhalt

Überprüfen der Domain-Kontrolle

Bevor Sie einen IP-Adressbereich einrichten AWS, müssen Sie eine der in diesem Abschnitt beschriebenen Optionen verwenden, um sicherzustellen, dass Sie den IP-Adressraum kontrollieren. Später, wenn Sie den IP-Adressbereich auf ändern AWS, wird AWS bestätigt, dass Sie den IP-Adressbereich kontrollieren. Diese Überprüfung stellt sicher, dass Kunden keine IP-Bereiche verwenden können, die anderen gehören. Dadurch werden Routing- und Sicherheitsprobleme verhindert.

Sie können mit zwei Methoden überprüfen, ob Sie den Bereich kontrollieren:

- X.509-Zertifikat: Wenn Ihr IP-Adressbereich bei einem Internetregister registriert ist, das RDAP unterstützt (wie ARIN, RIPE und APNIC), können Sie ein X.509-Zertifikat verwenden, um die Eigentümerschaft Ihrer Domain zu überprüfen.

- DNS-TXT-Datensatz: Unabhängig davon, ob Ihr Internetregister RDAP unterstützt, können Sie ein Verifizierungstoken und einen DNS-TXT-Datensatz verwenden, um die Eigentümerschaft Ihrer Domain zu überprüfen.

Inhalt

Überprüfen Ihrer Domain mit einem X.509-Zertifikat

In diesem Abschnitt wird beschrieben, wie Sie Ihre Domain mit einem X.509-Zertifikat überprüfen, bevor Sie Ihren IP-Adressbereich in IPAM einbringen.

So überprüfen Sie Ihre Domain mit einem X.509-Zertifikat

1. Führen Sie die drei Schritte unter Voraussetzungen für BYOIP in Amazon EC2 im EC2 Amazon-Benutzerhandbuch durch.

   > **Note**
   >
   > Wenn Sie das erstellen ROAs, müssen IPv4 CIDRs Sie die maximale Länge eines IP-Adresspräfixes auf festlegen. `/24` Denn IPv6 CIDRs wenn Sie sie zu einem Pool mit Werbung hinzufügen, muss die maximale Länge eines IP-Adresspräfixes sein. `/48` Dies stellt sicher, dass Sie bei der Aufteilung Ihrer öffentlichen IP-Adresse auf verschiedene AWS Regionen die volle Flexibilität haben. 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 dies `/24` der kleinste IPv4 Block `/48` ist und der kleinste IPv6 Block ist, für den Sie von einer Region aus im Internet werben können.

2. Führen Sie im AWS EC2 Amazon-Benutzerhandbuch nur die Schritte 1 und 2 unter Einen öffentlich beworbenen Adressbereich bereitstellen aus und geben Sie den Adressbereich (Schritt

3) noch nicht an. Speichern Sie `text_message` und `signed_message`. Sie benötigen die Werte später in diesem Prozess.

Wenn Sie diese Schritte abgeschlossen haben, fahren Sie mit Bringen Sie mithilfe der AWS Management Console und der CLI Ihre eigene IP zu IPAM AWS oder Bringen Sie Ihr eigenes IP-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS fort.

Überprüfen Ihrer Domain mit einem DNS-TXT-Datensatz

Führen Sie die Schritte in diesem Abschnitt aus, um Ihre Domain mit einem DNS-TXT-Datensatz zu verifizieren, bevor Sie Ihren IP-Adressbereich in IPAM einbringen.

Sie können DNS-TXT-Datensätze verwenden, um zu überprüfen, ob Sie die Kontrolle über einen öffentlichen IP-Adressbereich haben. DNS-TXT-Datensätze sind eine Art von DNS-Datensätzen, die Informationen über Ihren Domain-Namen enthalten. Mit diesem Feature können Sie IP-Adressen einbringen, die bei einer beliebigen Internetregistrierung registriert sind (z. B. JPNIC, LACNIC und AFRINIC), nicht nur bei solchen, die auf RDAP-Datensätzen (Registration Data Access Protocol) basierende Validierungen unterstützen (z. B. ARIN, RIPE und APNIC).

> **Important**
>
> Bevor Sie fortfahren können, müssen Sie bereits ein IPAM für das kostenlose oder erweiterte Kontingent erstellt haben. Wenn Sie kein IPAM haben, schließen Sie Erstellen eines IPAM zuerst ab.

Inhalt

Schritt 1: Erstellen einer ROA, falls Sie noch keine haben

Sie müssen eine Route Origin Authorization (ROA) in Ihrem Regional Internet Registry (RIR) für die IP-Adressbereiche haben, die Sie bewerben möchten. Wenn Ihr RIR keine ROA enthält, führen Sie Schritt 3 aus. Erstellen Sie im EC2 Amazon-Benutzerhandbuch ein ROA-Objekt in Ihrem RIR. Ignorieren Sie die anderen Schritte.

Der spezifischste IPv4 Adressbereich, den Sie angeben können, ist /24. Der spezifischste IPv6 Adressbereich, den Sie angeben können, ist /48 für solche CIDRs , die öffentlich beworben werden können, und /60 für solche CIDRs , die nicht öffentlich beworben werden können.

Schritt 2. Erstellen eines Verifizierungstokens

Ein Überprüfungstoken ist ein zufällig AWS generierter Wert, mit dem Sie die Kontrolle über eine externe Ressource nachweisen können. Sie können beispielsweise ein Überprüfungstoken verwenden, um zu überprüfen, ob Sie die Kontrolle über einen öffentlichen IP-Adressbereich haben, wenn Sie einen IP-Adressbereich hinzufügen AWS (BYOIP).

Führen Sie die Schritte in diesem Abschnitt aus, um ein Verifizierungstoken zu erstellen, das Sie in einem späteren Schritt dieses Tutorials benötigen, um Ihren IP-Adressbereich in IPAM einzubringen. Verwenden Sie die nachstehenden Anweisungen entweder für die AWS Konsole oder für. AWS CLI

AWS Management Console

So erstellen Sie ein Verifizierungstoken

1. Öffnen Sie die IPAM-Konsole unter https://console.aws.amazon.com/ipam/.
2. Wählen Sie in der AWS Management Console die AWS Region aus, in der Sie Ihr IPAM erstellt haben.
3. Wählen Sie im linken Navigationsbereich die Option IPAMs aus.
4. Wählen Sie Ihr IPAM und dann den Tab für die Verifizierungstoken aus.
5. Wählen Sie Verifizierungstoken erstellen aus.
6. Lassen Sie diesen Browser-Tab geöffnet, nachdem Sie das Token erstellt haben. Im nächsten Schritt benötigen Sie den Token-Wert, den Token-Namen und in einem späteren Schritt die Token-ID.

Beachten Sie Folgendes:

- Sobald Sie ein Verifizierungstoken erstellt haben, können Sie das Token für mehrere BYOIPs wiederverwenden CIDRs , die Sie innerhalb von 72 Stunden von Ihrem IPAM aus bereitstellen. Wenn Sie CIDRs nach 72 Stunden mehr bereitstellen möchten, benötigen Sie ein neues Token.
- Sie können bis zu 100 Token erstellen. Wenn Sie das Limit erreichen, löschen Sie abgelaufene Token.

Command line

- Fordern Sie mit create-ipam-external-resource-verification token an, dass IPAM ein Verifizierungstoken erstellt, das Sie für die DNS-Konfiguration verwenden werden:

```
aws ec2 create-ipam-external-resource-verification-token --ipam-id ipam-id
```

Dadurch wird ein UND-Token mit IpamExternalResourceVerificationTokenId und `TokenName` und `TokenValue` der Ablaufzeit (`NotAfter`) des Tokens zurückgegeben.

```
{
    "IpamExternalResourceVerificationToken": {
        "IpamExternalResourceVerificationTokenId": "ipam-ext-res-ver-
token-0309ce7f67a768cf0",
        "IpamId": "ipam-0f9e8725ac3ae5754",
        "TokenValue": "a34597c3-5317-4238-9ce7-50da5b6e6dc8",
        "TokenName": "86950620",
        "NotAfter": "2024-05-19T14:28:15.927000+00:00",
        "Status": "valid",
        "Tags": [],
        "State": "create-in-progress" }
}
```

Beachten Sie Folgendes:

- Sobald Sie ein Verifizierungstoken erstellt haben, können Sie das Token für mehrere BYOIPs wiederverwenden CIDRs , die Sie innerhalb von 72 Stunden von Ihrem IPAM aus bereitstellen. Wenn Sie CIDRs nach 72 Stunden mehr bereitstellen möchten, benötigen Sie ein neues Token.
- Sie können Ihre Token mithilfe von describe-ipam-external-resource-verification tokens einsehen.
- Sie können bis zu 100 Token erstellen. Wenn Sie das Limit erreichen, können Sie abgelaufene Token mit -verification token löschen. delete-ipam-external-resource

Schritt 3. Einrichten der DNS-Zone und des TXT-Datensatzes

Führen Sie die Schritte in diesem Abschnitt aus, um die DNS-Zone und den TXT-Datensatz einzurichten. Wenn Sie nicht Route53 als DNS verwenden, folgen Sie der Dokumentation Ihres DNS-Anbieters, um eine DNS-Zone einzurichten und einen TXT-Datensatz hinzuzufügen.

Wenn Sie Route53 verwenden, beachten Sie Folgendes:

- Informationen zum Erstellen einer Reverse-Lookupzone in der AWS Konsole finden Sie unter Creating a public hosted zone im Amazon Route 53 Developer Guide oder verwenden Sie den AWS CLI Befehl create-hosted-zone.
- Informationen zum Erstellen eines Datensatzes in der Reverse-Lookupzone in der AWS Konsole finden Sie unter Erstellen von Datensätzen mithilfe der Amazon Route 53 53-Konsole im Amazon Route 53-Entwicklerhandbuch oder verwenden Sie den AWS CLI Befehl change-resource-record-sets.
- Nachdem Sie Ihre gehostete Zone erstellt haben, delegieren Sie die gehostete Zone von Ihrem RIR an die von Route53 bereitgestellten Namensserver (z. B. für LACNIC oder APNIC).

Unabhängig davon, ob Sie einen anderen DNS-Anbieter oder Route53 verwenden, beachten Sie bei der Einrichtung des TXT-Datensatzes das Folgende:

- Der Datensatzname muss Ihr Token-Name sein.
- Der Datensatztyp muss TXT sein.
- ResourceRecord Der Wert sollte der Token-Wert sein.

Beispiel:

- Name (Name: `86950620.113.0.203.in-addr.arpa`
- Typ: `TXT`
- ResourceRecords Value (Wert): `a34597c3-5317-4238-9ce7-50da5b6e6dc8`

Wobei gilt:

- `86950620` ist der Name des Verifizierungstokens.
- `113.0.203.in-addr.arpa` ist der Name der Reverse-Lookup-Zone.
- `TXT` ist der Datensatztyp.
- `a34597c3-5317-4238-9ce7-50da5b6e6dc8` ist der Wert des Verifizierungstokens.

Note

Abhängig von der Größe des Präfixes, das mit BYOIP zu IPAM hinzugefügt werden soll, müssen ein oder mehrere Authentifizierungsdatensätze im DNS erstellt werden. Diese Authentifizierungsdatensätze sind vom Datensatztyp TXT und müssen in der Reverse-Zone des Präfixes selbst oder seines übergeordneten Präfixes platziert werden.

- Denn IPv4 Authentifizierungsdatensätze müssen sich an Bereichen an einer Oktettgrenze orientieren, aus denen das Präfix besteht.
  - Beispiele
  - Für 198.18.123.0/24, das bereits an einer Oktettgrenze ausgerichtet ist, müssten Sie einen einzigen Authentifizierungsdatensatz erstellen unter:
    - *token-name*.123.18.198.in-addr.arpa. IN TXT “*token-value*”
  - Für 198.18.12.0/22, das selbst nicht an der Oktettgrenze ausgerichtet ist, müssten Sie vier Authentifizierungsdatensätze erstellen. Diese Datensätze müssen die Subnetze 198.18.12.0/24, 198.18.13.0/24, 198.18.14.0/24 und 198.18.15.0/24 abdecken, die an einer Oktettgrenze ausgerichtet sind. Die entsprechenden DNS-Einträge müssen wie folgt lauten:
    - *token-name*.12.18.198.in-addr.arpa. IN TXT “*token-value*”
    - *token-name*.13.18.198.in-addr.arpa. IN TXT “*token-value*”
    - *token-name*.14.18.198.in-addr.arpa. IN TXT “*token-value*”
    - *token-name*.15.18.198.in-addr.arpa. IN TXT “*token-value*”
  - Für 198.18.0.0/16, das bereits an einer Oktettgrenze ausgerichtet ist, müssen Sie einen einzigen Authentifizierungsdatensatz erstellen:
    - *token-name*.18.198.in-addr.arpa. IN TXT “*token-value*”
- Denn die IPv6 Authentifizierungsdatensätze müssen sich an den Bereichen an der Nibble-Grenze orientieren, aus denen das Präfix besteht. Gültige Nibble-Werte sind z. B. 32, 36, 40, 44, 48, 52, 56 und 60.
  - Beispiele
    - Für 2001:0db8::/40, das bereits an der Nibble-Grenze ausgerichtet ist, müssen Sie einen einzigen Authentifizierungsdatensatz erstellen:
      - *token-name*.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT “*token-value*”
    - Für 2001:0db8:80::/42, das selbst nicht an der Nibble-Grenze ausgerichtet ist, müssen Sie vier Authentifizierungsdatensätze erstellen. Diese Datensätze müssen die

Subnetze 2001:db8:80::/44, 2001:db8:90::/44, 2001:db8:a0::/44 und 2001:db8:b0::/44 abdecken, die an einer Nibble-Grenze ausgerichtet sind. Die entsprechenden DNS-Einträge müssen wie folgt lauten:

- *token-name*.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
- *token-name*.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
- *token-name*.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
- *token-name*.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"

- Für den nicht beworbenen Bereich 2001:db8:0:1000::/54, der selbst nicht an einer Nibble-Grenze ausgerichtet ist, müssen Sie vier Authentifizierungsdatensätze erstellen. Diese Datensätze müssen die Subnetze 2001:db8:0:1000::/56, 2001:db8:0:1100::/56, 2001:db8:0:1200::/56 und 2001:db8:0:1300::/56 abdecken, die an einer Nibble-Grenze ausgerichtet sind. Die entsprechenden DNS-Einträge müssen wie folgt lauten:
  - *token-name*.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
  - *token-name*.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
  - *token-name*.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
  - *token-name*.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
- Um die korrekte Anzahl der hexadezimalen Zahlen zwischen dem Token-Namen und der Zeichenfolge „ip6.arpa“ zu überprüfen, multiplizieren Sie die Zahl mit vier. Das Ergebnis muss mit der Präfixlänge übereinstimmen. Für ein /56-Präfix müssen Sie zum Beispiel 14 hexadezimale Zeichen haben.

Wenn Sie diese Schritte abgeschlossen haben, fahren Sie mit Bringen Sie mithilfe der AWS Management Console und der CLI Ihre eigene IP zu IPAM AWS oder Bringen Sie Ihr eigenes IP-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS fort.

Bringen Sie mithilfe der AWS Management Console und der CLI Ihre eigene IP zu IPAM AWS

Mit Bring Your Own IP (BYOIP) zu IPAM können Sie die vorhandenen IPv4 Adressbereiche Ihrer Organisation nutzen. IPv6 AWS So können Sie ein konsistentes Branding beibehalten, die Netzwerkleistung verbessern, die Sicherheit erhöhen und die Verwaltung vereinfachen, indem Sie On-Premises- und Cloud-Umgebungen unter Ihrem eigenen IP-Adressraum vereinheitlichen.

Gehen Sie wie folgt vor, um mithilfe der AWS Managementkonsole und der CLI ein IPv4 oder IPv6 CIDR auf IPAM zu übertragen. AWS

> **Note**
>
> Bevor Sie beginnen, müssen Sie die Domainkontrolle überprüfen.

Sobald Sie einen IPv4 Adressbereich hinzugefügt haben AWS, 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 für IPAM bereitzustellen und eine Elastic IP-Adresse (EIP) sowohl über die AWS Management Console als auch über die CLI zuzuweisen. AWS

> **Important**
>
> - In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
>   - Integrieren Sie IPAM mit Konten in einer Organisation AWS.
>   - 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 Sie IPAM mit Konten in einer Organisation AWS. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zugewiesen wird. 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

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 die Zuweisung CIDRs aus einem IPAM-Pool erfolgt.

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 die Option aus IPv4.
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.

   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 die Option BYOIP aus.
11. Führen CIDRs Sie unter Bereitstellung eine der folgenden Aktionen aus:

    - Wenn Sie Ihre Domain-Kontrolle mit einem X.509-Zertifikat verifiziert haben, müssen Sie das CIDR, die BYOIP-Nachricht und die Zertifikatssignatur angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.
    - Wenn Sie Ihre Domain-Kontrolle mit einem DNS-TXT-Datensatz verifiziert haben, müssen Sie das CIDR- und IPAM-Token angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.

    Beachten Sie, dass Sie bei der Bereitstellung eines IPv4 CIDR für einen Pool innerhalb des Pools der obersten Ebene mindestens IPv4 CIDR bereitstellen können`/24`; genauere Angaben CIDRs (z. B.`/25`) sind nicht zulässig.

    > **Important**
    >
    > Während die Bereitstellung in den meisten Fällen innerhalb von zwei Stunden abgeschlossen sein wird, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich zugängliche Bereiche abgeschlossen ist.

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 Status der Bereitstellung auf der CIDRsRegisterkarte der Pool-Detailseite 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 einer der Betriebsregionen angehören, die Sie beim Erstellen des IPAM konfiguriert haben. Beispiel: Das Gebietsschema us-east-1 bedeutet, dass us-east-1 eine Betriebsregion für das IPAM sein muss. Das Gebietsschema us-east-1-scl-1 (eine Netzwerkgrenzgruppe, die für Local Zones verwendet wird) bedeutet, dass das IPAM die Betriebsregion us-east-1 haben muss.

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 für den Pool sollte eines der folgenden sein:

   - Eine AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll.

- Die Netzwerkgrenzgruppe für eine AWS lokale Zone, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll (unterstützte Local Zones). Diese Option ist nur für IPv4 IPAM-Pools im öffentlichen Bereich verfügbar.
- Eine AWS Dedicated Local Zone. Um einen Pool innerhalb einer AWS dedizierten lokalen Zone zu erstellen, geben Sie die AWS Dedizierte lokale Zone in die Auswahleingabe ein.

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 Service die Option 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 CIDRs zugewiesenen Daten für den Amazon-Service (für Elastic IP-Adressen) und den Amazon EC2 VPC-Service (für verknüpft mit) beworben werden. CIDRs VPCs
10. Wählen Sie unter Bereitstellung CIDRs einen CIDR aus, der für den Pool bereitgestellt werden soll.

> **Note**
>
> Wenn Sie ein CIDR für einen regionalen Pool innerhalb des Pools der obersten Ebene bereitstellen, ist `/24` das spezifischste IPv4 CIDR, das Sie bereitstellen können. Spezifischere CIDRs CIDRs (z. B.`/25`) sind nicht zulässig. Nachdem Sie den regionalen Pool erstellt haben, können Sie kleinere Pools (z. B. `/25`) innerhalb desselben regionalen Pools erstellen. Wenn Sie den regionalen Pool oder die darin enthaltenen Pools teilen, können diese Pools nur in dem Gebietsschema verwendet werden, das für denselben regionalen Pool festgelegt ist.

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 Sie

einen Pool auf oberster Ebene IPv4 . 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 Status der Bereitstellung auf der CIDRsRegisterkarte der Pool-Detailseite sehen.

Schritt 4: Werben für das 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 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.

> **Note**
>
> Der Werbestatus schränkt nicht Ihre Fähigkeit ein, Elastic-IP-Adressen zuzuweisen. Auch wenn Ihr BYOIPv4 CIDR nicht beworben wird, können Sie dennoch aus dem IPAM-Pool heraus etwas erstellen. EIPs

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 aus.

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 5. 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 aus, wählen Sie 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 mithilfe von RAM AWS. 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 mit dem IPAM-Administratorkonto 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 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 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 mithilfe von RAM AWS 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 6: Zuweisen einer Elastic-IP-Adresse aus dem Pool

Führen Sie die Schritte in diesem Abschnitt aus, um eine Elastic-IP-Adresse aus dem Pool zuzuweisen. Beachten Sie, dass Sie, wenn Sie öffentliche IPv4 Pools für die Zuweisung von Elastic

IP-Adressen verwenden, die alternativen Schritte unter Alternative zu Schritt 6 anstelle der Schritte in diesem Abschnitt verwenden können.

> **Important**
>
> Wenn Sie eine Fehlermeldung erhalten, weil Sie nicht berechtigt sind, ec2: aufzurufenAllocateAddress, muss die verwaltete Berechtigung aktualisiert werden, die derzeit dem IPAM-Pool zugewiesen ist, der mit Ihnen geteilt wurde. Wenden Sie sich an die Person, die die Ressourcenfreigabe 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

Folgen Sie den Schritten unter Zuweisen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch, um die Adresse zuzuweisen. Beachten Sie dabei jedoch Folgendes:

- Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.
- Stellen Sie sicher, dass die AWS Region, in der Sie sich in der EC2 Konsole befinden, der Locale-Option entspricht, die Sie bei der Erstellung des regionalen Pools ausgewählt haben.
- Wählen Sie bei der Auswahl des Adresspools die Option „Zuweisen mithilfe eines IPv4 IPAM-Pool“ und anschließend den von Ihnen erstellten regionalen Pool aus.

Command line

Weisen Sie mit dem Befehl allocate-address eine Adresse aus dem Pool zu. Der von Ihnen verwendete `--region` muss mit der Option `-locale` übereinstimmen, die Sie bei der Erstellung des Pools in Schritt 2 ausgewählt haben. Geben Sie in `--ipam-pool-id` die ID des IPAM-Pools an, den Sie in Schritt 2 erstellt haben. Optional können Sie auch einen bestimmten `/32` in Ihrem IPAM-Pool auswählen, indem Sie die Option `--address` verwenden.

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

Beispielantwort:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

Weitere Informationen finden Sie unter Zuweisen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch.

Schritt 7: Ordnen Sie die Elastic IP-Adresse einer Instance zu EC2

Führen Sie die Schritte in diesem Abschnitt aus, um die Elastic IP-Adresse einer EC2 Instance zuzuordnen.

AWS Management Console

Folgen Sie den Schritten unter Elastic IP-Adresse zuordnen im EC2 Amazon-Benutzerhandbuch, um eine Elastic IP-Adresse aus dem IPAM-Pool zuzuweisen. Beachten Sie jedoch Folgendes: Wenn Sie die Option AWS Management Console verwenden, muss die AWS Region, der Sie die Elastic IP-Adresse zuordnen, der Locale-Option entsprechen, die Sie bei der Erstellung des regionalen Pools ausgewählt haben.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

Command line

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden. Verwenden Sie die Option `--profile` **`member-account`**.

Verknüpfen Sie mit dem Befehl associate-address die Elastic-IP-Adresse mit einer Instance. Der `--region`, dem Sie die Elastic-IP-Adresse zuordnen, muss mit der Option `--locale` übereinstimmen, die Sie bei der Erstellung des regionalen Pools ausgewählt haben.

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

Beispielantwort:

```
{
```

```
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

Weitere Informationen finden Sie im EC2 Amazon-Benutzerhandbuch unter Eine Elastic IP-Adresse mit einer Instance oder Netzwerkschnittstelle verknüpfen.

Schritt 8: 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 aus.
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 die verwenden AWS CLI, verwenden Sie die `--profile` **`member-account`** Option.

- Führen Sie die Schritte unter Trennen einer Elastic IP-Adresse im EC2 Amazon-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, 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.

Schritt 3: Geben Sie die elastische IP-Adresse frei

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

- Führen Sie die Schritte unter Elastic IP-Adresse veröffentlichen im EC2 Amazon-Benutzerhandbuch aus, um eine Elastic IP-Adresse (EIP) aus dem öffentlichen IPv4 Pool freizugeben. Beim Öffnen EC2 in der AWS Management-Konsole 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: 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 zum Löschen der RAM-Shares und zum Deaktivieren der RAM-Integration verwenden, verwenden Sie die Optionen und. `--profile` **`ipam-account`** `--profile` **`management-account`**

- 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 5: Trennen Sie die Bereitstellung CIDRs von aus dem regionalen Pool und dem Pool der obersten Ebene

Dieser Schritt muss vom IPAM-Konto ausgeführt werden. Wenn Sie den verwenden, AWS CLI um den Pool gemeinsam zu nutzen, verwenden Sie die `--profile` **`ipam-account`** Option.

- Gehen Sie in dieser Reihenfolge wie Deprovisionierung CIDRs aus einem Pool unter beschrieben CIDRs vor, um die Bereitstellung für den Regionalpool und dann für den Pool der obersten Ebene aufzuheben.

Schritt 8: Löschen des regionalen Pools und des Pools auf oberster Ebene

Dieser Schritt muss vom IPAM-Konto ausgeführt werden. Wenn Sie den verwenden, AWS CLI um den Pool gemeinsam zu nutzen, 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.

Alternative zu Schritt 6

Wenn Sie öffentliche IPv4 Pools verwenden, um Elastic IP-Adressen zuzuweisen, können Sie die Schritte in diesem Abschnitt anstelle der Schritte unter verwenden. Schritt 6: Zuweisen einer Elastic-IP-Adresse aus dem Pool

Inhalt

Schritt 1: Erstellen Sie einen öffentlichen Pool IPv4

Dieser Schritt sollte von dem Mitgliedskonto durchgeführt werden, das eine elastische IP-Adresse bereitstellt.

> **Note**
>
> - Dieser Schritt muss vom Mitgliedskonto mit der AWS CLI durchgeführt werden.
> - Öffentliche IPv4 Pools und IPAM-Pools werden von unterschiedlichen Ressourcen in AWS verwaltet. Öffentliche IPv4 Pools sind Ressourcen mit einem einzigen Konto, mit denen Sie Ihre öffentlichen IP-Adressen in Elastic CIDRs umwandeln können. IPAM-Pools können verwendet werden, um Ihren öffentlichen Speicherplatz öffentlichen Pools zuzuweisen. IPv4

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 ID des öffentlichen IPv4 Pools. Sie benötigen diese ID im nächsten Schritt.

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

Schritt 2: Stellen Sie den öffentlichen IPv4 CIDR für Ihren öffentlichen Pool bereit IPv4

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. Die unspezifischste `--netmask-length`, die Sie definieren 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.
> - 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": []
        }
    ]
```

```
}
```

Nachdem Sie den öffentlichen IPv4 Pool erstellt haben, öffnen Sie die IPAM-Konsole und sehen Sie sich die Zuweisung im regionalen Pool unter Zuweisungen oder Ressourcen an, um den im regionalen Pool zugewiesenen öffentlichen IPv4 Pool anzuzeigen.

Schritt 3: Weisen Sie eine Elastic IP-Adresse aus dem öffentlichen Pool zu IPv4

Führen Sie die Schritte unter Zuweisen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch aus, um eine EIP aus dem öffentlichen Pool zuzuweisen. IPv4 Beim Öffnen EC2 in der AWS Management-Konsole muss die AWS Region, in 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.

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

Wenn Sie diese drei Schritte abgeschlossen haben, kehren Sie zu Schritt 7: Ordnen Sie die Elastic IP-Adresse einer Instance zu EC2 zurück und fahren Sie fort, bis Sie das Tutorial abgeschlossen haben.

Alternative zur Bereinigung in Schritt 6

Gehen Sie wie folgt vor, um öffentliche IPv4 Pools zu bereinigen, die mit der Alternative zu Schritt 9 erstellt wurden. Sie sollten diese Schritte ausführen, nachdem Sie die Elastic-IP-Adresse während des Standardbereinigungsvorgangs in Schritt 8: Bereinigen freigegeben haben.

Schritt 1: Trennen Sie die Bereitstellung des öffentlichen IPv4 CIDR aus Ihrem öffentlichen Pool IPv4

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

1. Sehen Sie sich Ihre BYOIP an. CIDRs

   ```
   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 den CIDR aus dem öffentlichen Pool freizugeben. IPv4

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-2 --pool-id ipv4pool-ec2-09037ce61cf068f9a --cidr 130.137.245.0/24 --profile member-account
```

3. Sehen Sie sich Ihre BYOIP CIDRs erneut an und stellen Sie sicher, dass keine Adressen mehr bereitgestellt wurden. 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 Pool. IPv4

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
```

```
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

> **Note**
>
> Es kann einige Zeit dauern, bis IPAM feststellt, dass Zuweisungen für öffentliche 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 2: Löschen Sie den öffentlichen Pool IPv4

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

- Führen Sie den folgenden Befehl aus, um den öffentlichen IPv4 Pool, den 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.

Bringen Sie mithilfe der Management Console Ihr eigenes IPv6 CIDR auf IPAM AWS

Folgen Sie den Schritten in diesem Tutorial, um ein IPv6 CIDR auf IPAM zu übertragen und dem CIDR mithilfe der Management Console und der eine VPC zuzuweisen. AWS AWS CLI

Wenn Sie Ihre IPv6 Adressen nicht über das Internet bekannt geben müssen, können Sie einem IPAM eine private IPv6 GUA-Adresse bereitstellen. Weitere Informationen finden Sie unter Bereitstellung von privater IPv6 GUA aktivieren CIDRs.

Important

- In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
  - Integrieren Sie IPAM mit Konten in einer Organisation AWS.
  - 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 Sie IPAM mit Konten in einer Organisation AWS. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zugewiesen wird. 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 auf oberster Ebene mit einem darin enthaltenen regionalen Pool erstellen und einer Ressource aus dem regionalen Pool Speicherplatz zuweisen, legen Sie das Gebietsschema für den regionalen Pool und nicht für den Pool auf oberster 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 die Option aus IPv6.
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. 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.

10. Unter Öffentliche IP-Quelle ist BYOIP standardmäßig ausgewählt.
11. Führen CIDRs Sie unter Bereitstellung einen der folgenden Schritte aus:

    - Wenn Sie Ihre Domain-Kontrolle mit einem X.509-Zertifikat verifiziert haben, müssen Sie das CIDR, die BYOIP-Nachricht und die Zertifikatssignatur angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.
    - Wenn Sie Ihre Domain-Kontrolle mit einem DNS-TXT-Datensatz verifiziert haben, müssen Sie das CIDR- und IPAM-Token angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.

    Beachten Sie, dass bei der Bereitstellung eines IPv6 CIDR für einen Pool innerhalb des Pools der obersten Ebene der spezifischste IPv6 Adressbereich, den Sie angeben können, /48 für solche, die öffentlich beworben werden können, und /60 für solche CIDRs , die nicht öffentlich beworben werden können, ist. CIDRs

    > **Important**
    >
    > Während die Bereitstellung in den meisten Fällen innerhalb von zwei Stunden abgeschlossen sein wird, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich zugängliche Bereiche abgeschlossen ist.

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 Status der Bereitstellung auf der Registerkarte auf der Seite mit den Pool-Details sehen. CIDRs

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 Service die Option 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 CIDRs zugewiesenen Daten für den EC2 Amazon-Service und den Amazon VPC-Service (für verknüpft mit) beworben werden können. CIDRs VPCs
10. Wählen Sie unter Bereitstellung CIDRs einen CIDR aus, der für den Pool bereitgestellt werden soll. 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 solche, die öffentlich beworben werden können, und /60 für CIDRs solche, die nicht öffentlich beworben werden können, ist. CIDRs
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 Ressourcen, die diesen Ressourcen zugewiesen werden CIDRs , dürfen nicht bereits anderen Ressourcen zugewiesen 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 CIDRs dieser Überschneidungen feststellt, importiert IPAM nur den größten CIDR.
        - Wenn IPAM mehrere CIDRs mit übereinstimmendem Ergebnis entdeckt CIDRs, importiert IPAM nach dem Zufallsprinzip 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.
- Gebietsschema: Das Gebietsschema, das für Ressourcen benötigt wird, die diesen Pool verwenden CIDRs . 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 Status der Bereitstellung auf der CIDRsRegisterkarte der Pool-Detailseite sehen.

Schritt 3. 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 aus, wählen Sie 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 mithilfe von RAM AWS. 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 mit dem IPAM-Administratorkonto 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 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 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.
10. Wählen Sie die AWSRAMPermissionIpamPoolByoipCidrImportBerechtigung aus. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mithilfe von RAM AWS können Sie jedoch mehr über diese Optionen erfahren.

11. Wählen Sie Weiter.
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.
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 Dienst 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 aus.
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 aus.
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: Trennen Sie die Bereitstellung CIDRs von aus dem regionalen Pool und dem Pool der obersten Ebene

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

- Führen Sie die Schritte unter ausDeprovisionierung CIDRs aus einem Pool, um die Bereitstellung CIDRs von aus dem Regionalpool und dann vom Pool der obersten Ebene aufzuheben, und zwar in dieser Reihenfolge.

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 IP-CIDR zu IPAM, indem Sie nur die CLI verwenden AWS

Mit Bring Your Own IP (BYOIP) zu IPAM können Sie die vorhandenen IPv4 Adressbereiche Ihrer Organisation nutzen. IPv6 AWS So können Sie ein konsistentes Branding beibehalten, die Netzwerkleistung verbessern, die Sicherheit erhöhen und die Verwaltung vereinfachen, indem Sie On-Premises- und Cloud-Umgebungen unter Ihrem eigenen IP-Adressraum vereinheitlichen.

Gehen Sie wie folgt vor, um ein IPv4 oder IPv6 CIDR nur mit der CLI auf IPAM zu übertragen. AWS

> **Note**
>
> Bevor Sie beginnen, müssen Sie die Domainkontrolle überprüfen.

Sobald Sie einen IPv4 Adressbereich hinzugefügt haben AWS, 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

Gehen Sie wie folgt vor, um ein IPv4 CIDR auf IPAM zu übertragen und dem CIDR eine Elastic IP-Adresse (EIP) zuzuweisen, indem Sie nur die verwenden. AWS CLI

Important

- In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
  - Integrieren Sie IPAM mit Konten in einer Organisation AWS.
  - 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 Sie IPAM mit Konten in einer Organisation AWS. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zugewiesen wird. In diesem Tutorial wird dieses Konto als Mitgliedskonto bezeichnet.

Inhalt

- Schritt 11: Bereinigen
- Alternative zu Schritt 9

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

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 die Zuweisung CIDRs aus einem IPAM-Pool erfolgt.

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, weil BYOIP öffentliche IP-Adressen CIDRs sind, wofür der öffentliche Bereich gedacht 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 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 Sie bei der Bereitstellung eines IPv4 CIDR für einen Pool innerhalb des Pools der obersten Ebene mindestens IPv4 CIDR bereitstellen können. Spezifischere `/24` CIDRs CIDRs (z. B.`/25`) sind nicht zulässig.

> **Note**
>
> - Wenn Sie Ihre Domain-Kontrolle mit einem X.509-Zertifikat verifiziert haben, müssen Sie das CIDR, die BYOIP-Nachricht und die Zertifikatssignatur angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.
> - Wenn Sie Ihre Domain-Kontrolle mit einem DNS-TXT-Datensatz verifiziert haben, müssen Sie das CIDR- und IPAM-Token angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.

Sie müssen die Domain-Kontrolle nur verifizieren, wenn Sie das BYOIP CIDR für den Pool der obersten Ebene bereitstellen. Für den Regionalpool im Pool der obersten Ebene können Sie die Option zur Domäneneigentumsüberprüfung auslassen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

> **Important**
>
> Sie müssen die Domain-Kontrolle nur verifizieren, wenn Sie das BYOIP CIDR für den Pool der obersten Ebene bereitstellen. Für den Regionalpool im Pool der obersten Ebene können Sie die Option zur Domain-Kontrolle 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. Verwenden Sie das folgende Befehlsbeispiel, um dem CIDR Zertifikatsinformationen zur Verfügung zu stellen. Achten Sie nicht nur darauf, die Werte wie im Beispiel angegeben zu ersetzen, sondern ersetzen Sie auch die Werte `Message` und `Signature` durch die Werte `text_message` und `signed_message`, die Sie in Überprüfen Ihrer Domain mit einem X.509-Zertifikat erhalten haben.

   ```
   aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-
   pool-id ipam-pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --
   verification-method remarks-x509 --cidr-authorization-context
    Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
   RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsMaU0P7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
   hApR89Kt6GxRYOdRaNx8yt-uoZWzxct2yIhWngy-
   du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
   oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
   C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
   ```

   Verwenden Sie das folgende Befehlsbeispiel, um dem CIDR Verifizierungstoken-Informationen zur Verfügung zu stellen. Achten Sie nicht nur darauf, die Werte wie im Beispiel angegeben zu ersetzen, sondern ersetzen Sie `ipam-ext-res-ver-token-0309ce7f67a768cf0` und durch die Token-ID `IpamExternalResourceVerificationTokenId`, die Sie in Überprüfen Ihrer Domain mit einem DNS-TXT-Datensatz erhalten haben.

   ```
   aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
   pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --verification-method dns-
   token --ipam-external-resource-verification-token-id ipam-ext-res-ver-
   token-0309ce7f67a768cf0 --profile ipam-account
   ```

In der Konsolenausgabe 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 Bereitstellung in den meisten Fällen innerhalb von zwei Stunden abgeschlossen sein wird, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich zugängliche 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.

Das Gebietsschema für den Pool sollte eines der folgenden sein:

- Eine AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll.
- Die Netzwerkgrenzgruppe für eine AWS lokale Zone, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll (unterstützte Local Zones). Diese Option ist nur für IPv4 IPAM-Pools im öffentlichen Bereich verfügbar.
- Eine AWS Dedicated Local Zone. Um einen Pool innerhalb einer AWS dedizierten lokalen Zone zu erstellen, geben Sie die AWS Dedizierte lokale Zone in die Auswahleingabe ein.

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.

Wenn Sie die Befehle in diesem Abschnitt ausführen, muss der Wert für `--region` die `--locale`-Option enthalten, die Sie eingegeben haben, als Sie den Pool erstellt haben, der für das BYOIP CIDR verwendet wird. Wenn Sie beispielsweise den BYOIP-Pool mit dem Gebietsschema us-east-1 erstellt haben, sollte `--region` den Wert us-east-1 haben. Wenn Sie den BYOIP-Pool mit dem Gebietsschema us-east-1-scl-1 (einer Netzwerkgrenzgruppe, die für Local Zones verwendet wird) erstellt haben, sollte `--region` den Wert us-east-1 haben, weil diese Region das Gebietsschema us-east-1-scl-1 verwaltet.

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 CIDRs zugewiesenen Daten für den Amazon-Service (für Elastic IP-Adressen) und den Amazon EC2 VPC-Service (für CIDRs Associated with) beworben werden können. VPCs

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.

> **Note**
>
> Wenn Sie ein CIDR für einen regionalen Pool innerhalb des Pools der obersten Ebene bereitstellen, ist das spezifischste IPv4 CIDR, das Sie bereitstellen können. Spezifischere CIDRs CIDRs (z. `/24` B.) sind nicht zulässig. `/25` Nachdem Sie den regionalen Pool erstellt haben, können Sie kleinere Pools (z. B. `/25`) innerhalb desselben regionalen Pools erstellen. Wenn Sie den regionalen Pool oder die darin enthaltenen Pools teilen, können diese Pools nur in dem Gebietsschema verwendet werden, das für denselben regionalen Pool festgelegt 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-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: Werben für das 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.

> **Note**
>
> Der Werbestatus schränkt nicht Ihre Fähigkeit ein, Elastic-IP-Adressen zuzuweisen. Auch wenn Ihr BYOIPv4 CIDR nicht beworben wird, können Sie dennoch aus dem IPAM-Pool heraus etwas erstellen EIPs .

Beginnen Sie mit der Werbung für CIDR mit dem 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 8: Teilen des regionalen Pools

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 mithilfe von RAM AWS. 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 mit dem IPAM-Administratorkonto 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 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 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 mithilfe von RAM AWS 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 9: Zuweisen einer Elastic-IP-Adresse aus dem Pool

Führen Sie die Schritte in diesem Abschnitt aus, um eine Elastic-IP-Adresse aus dem Pool zuzuweisen. Beachten Sie, dass Sie, wenn Sie öffentliche IPv4 Pools für die Zuweisung von Elastic IP-Adressen verwenden, die alternativen Schritte unter Alternative zu Schritt 9 anstelle der Schritte in diesem Abschnitt verwenden können.

> **Important**
>
> Wenn Sie eine Fehlermeldung erhalten, weil Sie nicht berechtigt sind, ec2: aufzurufenAllocateAddress, muss die verwaltete Berechtigung aktualisiert werden, die derzeit dem IPAM-Pool zugewiesen ist, der mit Ihnen geteilt wurde. Wenden Sie sich an die Person, die die Ressourcenfreigabe 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

Folgen Sie den Schritten unter Zuweisen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch, um die Adresse zuzuweisen. Beachten Sie dabei jedoch Folgendes:

- Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.
- Stellen Sie sicher, dass die AWS Region, in der Sie sich in der EC2 Konsole befinden, der Locale-Option entspricht, die Sie bei der Erstellung des regionalen Pools ausgewählt haben.
- Wählen Sie bei der Auswahl des Adresspools die Option „Zuweisen mithilfe eines IPv4 IPAM-Pool“ und anschließend den von Ihnen erstellten regionalen Pool aus.

Command line

Weisen Sie mit dem Befehl allocate-address eine Adresse aus dem Pool zu. Der von Ihnen verwendete `--region` muss mit der Option `-locale` übereinstimmen, die Sie bei der Erstellung des Pools in Schritt 2 ausgewählt haben. Geben Sie in `--ipam-pool-id` die ID des IPAM-Pools an, den Sie in Schritt 2 erstellt haben. Optional können Sie auch einen bestimmten `/32` in Ihrem IPAM-Pool auswählen, indem Sie die Option `--address` verwenden.

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

Beispielantwort:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

Weitere Informationen finden Sie unter Zuweisen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch.

Schritt 10: Ordnen Sie die Elastic IP-Adresse einer Instance zu EC2

Führen Sie die Schritte in diesem Abschnitt aus, um die Elastic IP-Adresse einer EC2 Instance zuzuordnen.

AWS Management Console

Folgen Sie den Schritten unter Elastic IP-Adresse zuordnen im EC2 Amazon-Benutzerhandbuch, um eine Elastic IP-Adresse aus dem IPAM-Pool zuzuweisen. Beachten Sie jedoch Folgendes: Wenn Sie die Option AWS Management Console verwenden, muss die AWS Region, der Sie die Elastic IP-Adresse zuordnen, der Locale-Option entsprechen, die Sie bei der Erstellung des regionalen Pools ausgewählt haben.

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden.

Command line

Dieser Schritt muss vom Mitgliedskonto durchgeführt werden. Verwenden Sie die Option `--profile` **`member-account`**.

Verknüpfen Sie mit dem Befehl associate-address die Elastic-IP-Adresse mit einer Instance. Der `--region`, dem Sie die Elastic-IP-Adresse zuordnen, muss mit der Option `--locale` übereinstimmen, die Sie bei der Erstellung des regionalen Pools ausgewählt haben.

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

Beispielantwort:

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

Weitere Informationen finden Sie im EC2 Amazon-Benutzerhandbuch unter Eine Elastic IP-Adresse mit einer Instance oder Netzwerkschnittstelle verknüpfen.

Schritt 11: 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` die `--locale`-Option enthalten, 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. Hören Sie auf, für das IPv4 CIDR zu werben.

   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. 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` die `--locale`-Option enthalten, 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.

```
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": []
}
```

5. 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"

    }

}
```

6. 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.

7. 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"
    }
}
```

8. 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"

    }

}
```

9. 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"
    }
}
```

10. 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"
            }
        ],
    }
```

```
}
```

Alternative zu Schritt 9

Wenn Sie öffentliche IPv4 Pools verwenden, um Elastic IP-Adressen zuzuweisen, können Sie die Schritte in diesem Abschnitt anstelle der Schritte unter verwenden. Schritt 9: Zuweisen einer Elastic-IP-Adresse aus dem Pool

Inhalt

Schritt 1: Erstellen Sie einen öffentlichen Pool IPv4

Dieser Schritt wird normalerweise von einem anderen AWS Konto ausgeführt, das eine Elastic IP-Adresse bereitstellen möchte, z. B. das Mitgliedskonto.

> **Important**
>
> Öffentliche IPv4 Pools und IPAM-Pools werden von unterschiedlichen Ressourcen in AWS verwaltet. Öffentliche IPv4 Pools sind Ressourcen mit einem einzigen Konto, mit denen Sie Ihre öffentlichen IP-Adressen in Elastic CIDRs umwandeln können. IPAM-Pools können verwendet werden, um Ihren öffentlichen Speicherplatz öffentlichen Pools zuzuweisen. IPv4

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 ID des öffentlichen IPv4 Pools. Sie benötigen diese ID im nächsten Schritt.

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

Schritt 2: Stellen Sie den öffentlichen IPv4 CIDR für Ihren öffentlichen Pool bereit IPv4

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. Die unspezifischste `--netmask-length`, die Sie definieren können, ist 24.

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 3: Erstellen Sie eine Elastic IP-Adresse aus dem öffentlichen Pool IPv4

Erstellen Sie eine Elastic 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"
        }
    ]
}
```

Alternative zu Schritt 9 – Bereinigung

Gehen Sie wie folgt vor, um öffentliche IPv4 Pools zu bereinigen, die mit der Alternative zu Schritt 9 erstellt wurden. Sie sollten diese Schritte ausführen, nachdem Sie die Elastic-IP-Adresse während des Standardbereinigungsvorgangs in Schritt 10: Bereinigen freigegeben haben.

1. Sehen Sie sich Ihr 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": []
        }
    ]
}
```

2. Geben Sie das CIDR aus dem öffentlichen Pool frei. IPv4 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 130.137.245.0/24 --profile member-account
   ```

3. Sehen Sie sich Ihre BYOIP CIDRs erneut an und stellen Sie sicher, dass keine Adressen mehr bereitgestellt wurden. 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 Pool. IPv4

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
   ```

```
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

Bringen Sie Ihr eigenes IPv6 CIDR zu IPAM, indem Sie nur die CLI verwenden AWS

Gehen Sie wie folgt vor, um ein IPv6 CIDR auf IPAM zu übertragen und eine VPC zuzuweisen, indem Sie nur die verwenden. AWS CLI

Wenn Sie Ihre IPv6 Adressen nicht über das Internet bekannt geben müssen, können Sie einem IPAM eine private IPv6 GUA-Adresse bereitstellen. Weitere Informationen finden Sie unter Bereitstellung von privater IPv6 GUA aktivieren CIDRs.

Important

- In diesem Tutorial wird davon ausgegangen, dass Sie die Schritte in den folgenden Abschnitten bereits ausgeführt haben:
  - Integrieren Sie IPAM mit Konten in einer Organisation AWS.
  - 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 Sie IPAM mit Konten in einer Organisation AWS. In diesem Tutorial wird dieses Konto als IPAM-Konto bezeichnet.
  - Das Mitgliedskonto in Ihrer Organisation, das CIDRs aus einem IPAM-Pool zugewiesen wird. 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

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 die Zuweisung CIDRs aus einem IPAM-Pool erfolgt.

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 diejenigen ist, die öffentlich beworben werden können, und /60 für solche CIDRs , die nicht öffentlich beworben werden können. CIDRs

> **Note**
>
> - Wenn Sie Ihre Domain-Kontrolle mit einem X.509-Zertifikat verifiziert haben, müssen Sie das CIDR, die BYOIP-Nachricht und die Zertifikatssignatur angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.

- Wenn Sie Ihre Domain-Kontrolle mit einem DNS-TXT-Datensatz verifiziert haben, müssen Sie das CIDR- und IPAM-Token angeben, die Sie in diesem Schritt erstellt haben, damit wir überprüfen können, ob Sie den öffentlichen Raum kontrollieren.

Sie müssen die Domain-Kontrolle nur verifizieren, wenn Sie das BYOIP CIDR für den Pool der obersten Ebene bereitstellen. Für den Regionalpool im Pool der obersten Ebene können Sie die Option für den Domainbesitz weglassen.

Dieser Schritt muss vom IPAM-Konto ausgeführt werden.

Um einen CIDR-Block für den Pool bereitzustellen, verwenden Sie AWS CLI

1. Verwenden Sie das folgende Befehlsbeispiel, um dem CIDR Zertifikatsinformationen zur Verfügung zu stellen. Achten Sie nicht nur darauf, die Werte wie im Beispiel angegeben zu ersetzen, sondern ersetzen Sie auch die Werte `Message` und `Signature` durch die Werte `text_message` und `signed_message`, die Sie in Überprüfen Ihrer Domain mit einem X.509-Zertifikat erhalten haben.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-
x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|
20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

   Verwenden Sie das folgende Befehlsbeispiel, um dem CIDR Verifizierungstoken-Informationen zur Verfügung zu stellen. Achten Sie nicht nur darauf, die Werte wie im Beispiel angegeben zu ersetzen, sondern ersetzen Sie `ipam-ext-res-ver-token-0309ce7f67a768cf0` und durch die Token-ID `IpamExternalResourceVerificationTokenId`, die Sie in Überprüfen Ihrer Domain mit einem DNS-TXT-Datensatz erhalten haben.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method
 dns-token --ipam-external-resource-verification-token-id ipam-ext-res-ver-
token-0309ce7f67a768cf0 --profile ipam-account
```

   In der Konsolenausgabe 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 Bereitstellung in den meisten Fällen innerhalb von zwei Stunden abgeschlossen sein wird, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich zugängliche 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 ausgewählte Dienst bestimmt den AWS Dienst, bei dem der CIDR beworben wird. Derzeit ist die einzige Option`ec2`, was bedeutet, dass die aus diesem Pool CIDRs zugewiesenen Daten für den EC2 Amazon-Service und den Amazon VPC-Service (für CIDRs verknüpft mit) beworben werden können. VPCs

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 Pools der obersten Ebene der spezifischste IPv6 Adressbereich, den Sie angeben können, /48 für öffentlich beworbene Bereiche und /60 für solche CIDRs , die nicht öffentlich beworben werden können, ist. CIDRs

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 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 mithilfe von RAM AWS. 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 mit dem IPAM-Administratorkonto 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 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 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.
10. Wählen Sie die AWSRAMPermissionIpamPoolByoipCidrImportBerechtigung aus. Die Details der Berechtigungsoptionen würden den Rahmen dieses Tutorials sprengen. Unter Teilen Sie einen IPAM-Pool mithilfe von RAM AWS können Sie jedoch mehr über diese Optionen erfahren.
11. Wählen Sie Weiter.
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.

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 Sie eine VPC mithilfe des CIDR IPv6

Erstellen Sie eine VPC mithilfe der IPAM-Pool-ID. Mithilfe der `--cidr-block` Option müssen Sie der VPC auch einen IPv4 CIDR-Block zuordnen, da die Anfrage sonst fehlschlägt. 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 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 den 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 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.

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: Eine BYOIP IPv4 CIDR auf IPAM übertragen

Gehen Sie wie folgt vor, um ein vorhandenes IPv4 CIDR auf IPAM zu übertragen. Wenn Sie bereits über ein IPv4 BYOIP-CIDR verfügen AWS, können Sie das CIDR von einem öffentlichen Pool zu IPAM verschieben. IPv4 Sie können einen CIDR nicht auf IPAM verschieben. IPv6

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 beschriebenen Prozesses hinzugefügt haben EC2 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 auf IPAM übertragen, hat dies keine Auswirkungen auf bestehende Zuweisungen. Sobald Sie einen öffentlichen IPv4 Pool an IPAM übertragen haben, können Sie je nach Ressourcentyp möglicherweise die vorhandenen Zuweisungen überwachen. Weitere Informationen finden Sie unter Überwachen Sie die CIDR-Nutzung nach Ressourcen.

> **Note**
>
> - 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

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 CIDRs zugewiesenen Daten für den Amazon-Service (für Elastic IP-Adressen) und den Amazon EC2 VPC-Service (für CIDRs Associated with) beworben werden können. VPCs

Um einen IPv4 Adresspool für das übertragene BYOIP CIDR zu erstellen, verwenden Sie 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 IPV4 BYOIP-CIDR in den IPAM-Pool übertragen und den IPAM-Pool verwenden kann. Dieser Schritt sollte vom **`ipam-account`**-Konto ausgeführt werden.

Um einen Adresspool gemeinsam zu nutzen, verwenden Sie IPv4 AWS CLI

1. Sehen Sie sich die für IPAM-Pools verfügbaren AWS RAM Berechtigungen an. Sie benötigen beide ARNs , um die Schritte in diesem Abschnitt auszuführen.

```
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 **`byoip-owner-account`** Konto BYOIP CIDRs nach 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 dem **`byoip-owner-account`** Konto ermöglichen möchten, nach Abschluss der Übertragung 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"

        }

}
```

Nachdem Sie die Ressourcenfreigabe im RAM erstellt haben, kann das byoip-owner-account Konto jetzt zu IPAM verschoben CIDRs werden.

Schritt 5: Übertragen Sie ein vorhandenes IPV4 BYOIP-CIDR auf IPAM

Folgen Sie den Schritten in diesem Abschnitt, um ein vorhandenes IPV4 BYOIP-CIDR auf IPAM zu übertragen. Dieser Schritt sollte vom **`byoip-owner-account`**-Konto ausgeführt werden.

> **Important**
>
> Sobald Sie einen IPv4 Adressbereich hinzugefügt 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/dem **`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 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 den CIDR aus dem öffentlichen Pool frei. IPv4 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 130.137.249.0/24
   ```

6. Sehen Sie sich Ihre BYOIP CIDRs erneut an und stellen Sie sicher, dass keine Adressen mehr bereitgestellt wurden. 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 Pool. IPv4

   ```
   {
       "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 Subnetzen VPCs . Sie können dieses Tutorial auch mithilfe eines IPv6 CIDR-Bereichs abschließen, indem Sie die VPC mit einer 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 für die Zuweisung CIDRs zu Subnetzen oder 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 für die Erstellung erforderlich sind VPCs, finden Sie in den Amazon VPC-Richtlinienbeispielen im Amazon VPC-Benutzerhandbuch.

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 mit dem IPAM-Administratorkonto 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 IPv4 CIDR Manual Input und geben Sie einen CIDR-Block ein IPv4 . 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 mit dem IPAM-Administratorkonto 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 mit dem IPAM-Administratorkonto 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 für den Pool 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 für die Bereitstellung für CIDRs den Ressourcenplanungspool verwendet wird.
9. Wählen Sie unter CIDRs Zur Bereitstellung die VPC-CIDR aus, die 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 mit dem IPAM-Administratorkonto 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 für den Pool 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 Zur Bereitstellung den CIDR aus, der 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 „“ zu erstellen. prod-subnet-pool

Wenn Sie diesen Subnetzpool nun für andere AWS Konten verfügbar machen möchten, können Sie den Subnetzpool gemeinsam nutzen. Anweisungen dazu finden Sie unter Teilen Sie einen IPAM-Pool mithilfe von RAM AWS. 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 mit dem entsprechenden Konto 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 Instance in einem der Subnetze starten. EC2

IPAM veröffentlicht Metriken zur Nutzung von IP-Adressen in Subnetzen. Sie können CloudWatch Alarme für die IPUsage Subnetz-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% davon genutzt IPs 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 mit dem IPAM-Administratorkonto 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 werden weiterhin für sie CIDRs bereitgestellt, obwohl sie nicht mehr aus einem IPAM-Pool stammen. CIDRs
6. Wählen Sie Löschen.
7. Löschen Sie die Subnetze.
8. Löschen Sie die VPC.

Die Bereinigung ist abgeschlossen.

Zuweisen von sequentiellen Elastic-IP-Adressen aus einem IPAM-Pool

Mit IPAM können Sie öffentliche IPv4 Blöcke, die Amazon gehören, für IPAM-Pools bereitstellen und sequentielle Elastic IP-Adressen aus diesen Pools Ressourcen zuweisen. AWS

Fortlaufend zugewiesene Elastic IP-Adressen sind öffentliche Adressen, die sequentiell zugewiesen werden. IPv4 Wenn Amazon Ihnen beispielsweise einen öffentlichen IPv4 CIDR-Block von zur Verfügung stellt `192.0.2.0/30` und Sie die vier verfügbaren öffentlichen IPv4 Adressen aus diesem CIDR-Block zuweisen, ist ein Beispiel für vier sequentielle Elastic IP-Adressen`192.0.2.0`,, `192.0.2.1` und. `192.0.2.2` `192.0.2.3`

Mit zusammenhängend zugewiesenen Elastic-IP-Adressen können Sie Ihre Sicherheits- und Netzwerkregeln auf folgende Weise vereinfachen:

- Sicherheitsadministration: Die Verwendung sequentieller IPv4 Adressen reduziert den Verwaltungsaufwand für Ihre Firewall. Sie können ein ganzes Präfix mit einer einzigen Regel hinzufügen und bei der Skalierung IPs von demselben Präfix aus zuordnen, was Zeit und Mühe spart.

- Zugriff für Unternehmen: Sie können den mit Ihren Kunden gemeinsam genutzten Adressraum vereinfachen, indem Sie statt einer langen Liste einzelner öffentlicher IPv4 Adressen einen kompletten CIDR-Block verwenden. Auf diese Weise müssen Sie nicht ständig IP-Änderungen mitteilen, wenn Ihre Anwendung auf AWS skaliert wird.
- Vereinfachtes IP-Management: Die Verwendung sequentieller IPv4 Adressen vereinfacht die Verwaltung öffentlicher IP-Adressen für Ihr zentrales Netzwerkteam, da so die Notwendigkeit reduziert wird, einzelne öffentliche IPs IP-Adressen zu verfolgen, sodass sie sich stattdessen auf eine begrenzte Anzahl von IP-Präfixen konzentrieren können.

In diesem Tutorial gehen Sie die Schritte durch, die für die Zuweisung sequentieller Elastic-IP-Adressen aus einem IPAM-Pool erforderlich sind. Sie erstellen einen IPAM-Pool mit einem von Amazon bereitgestellten zusammenhängenden öffentlichen IPv4 CIDR-Block, weisen Elastic IP-Adressen aus dem Pool zu und lernen, wie Sie die IPAM-Poolzuweisungen überwachen.

> **Note**
>
> - Für die Bereitstellung von öffentlichen IPv4 CIDR-Blöcken, die sich im Besitz von Amazon befinden, fallen Gebühren an. Weitere Informationen finden Sie auf der Amazon VPC-Preisseite auf der Amazon VPC-Preisseite auf der Registerkarte „zusammenhängende IPv4 Blöcke“.
> - In diesem Tutorial wird davon ausgegangen, dass Sie ein IPAM mithilfe von IPAM mit einem einzigen Konto erstellen möchten. Wenn Sie zusammenhängende öffentliche IPv4 Blöcke, die sich im Besitz von Amazon befinden, für mehrere Konten gemeinsam nutzen möchten, zuerst und dann. Integrieren Sie IPAM mit Konten in einer Organisation AWS Teilen Sie einen IPAM-Pool mithilfe von RAM AWS Wenn Sie mit AWS Organizations integrieren, haben Sie die Möglichkeit, eine Dienststeuerungsrichtlinie zu erstellen, um die Deprovisionierung der dem Pool zugewiesenen IPv4 Contig-Blöcke zu verhindern.
> - Sie können keine sequentiellen Elastic-IP-Adressen, die von einem IPAM-Pool zugewiesen wurden, an andere AWS -Konten übertragen. Stattdessen können Sie mit IPAM IPAM-Pools für mehrere AWS Konten gemeinsam nutzen, indem Sie IPAM in AWS Organizations integrieren (wie oben erwähnt).
> - Die Anzahl der öffentlichen IPv4 CIDR-Blöcke, die sich im Besitz von Amazon befinden, die Sie bereitstellen können, und deren Größe sind begrenzt. Weitere Informationen finden Sie unter Kontingente für Ihr IPAM.

Inhalt

Schritt 1: Erstellen von einem IPAM

Führen Sie die Schritte in diesem Abschnitt durch, um ein IPAM zu erstellen.

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 Management Console die AWS Region aus, 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, ist standardmäßig als eine der Betriebsregionen ausgewählt. Wenn Sie dieses IPAM beispielsweise in AWS Region erstellen, `us-east-1` aber später regionale IPAM-Pools erstellen möchten, die Zugriff CIDRs darauf VPCs bieten, wählen Sie hier aus. `us-west-2` `us-west-2` 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.

Erstellen Sie das IPAM mit dem Befehl create-ipam:

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

Beispielantwort:

```
{
    "Ipam": {
        "OwnerId": "320805250157",
        "IpamId": "ipam-0755477df834ea06b",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-01bc7290e4a9202f9",
        "PrivateDefaultScopeId": "ipam-scope-0a50983b97a7a583a",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "State": "create-in-progress",
```

```
        "Tags": [],
        "DefaultResourceDiscoveryId": "ipam-res-disco-02cc5b34cc3f04f09",
        "DefaultResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-06b3a4dccfc81f7c1",
        "ResourceDiscoveryAssociationCount": 1,
        "Tier": "advanced"
    }
}
```

Sie benötigen die PublicDefaultScopeId im nächsten Schritt. Weitere Informationen zu Bereichen finden Sie unter Funktionsweise von IPAM.

Schritt 2: Erstellen eines IPAM-Pools und Bereitstellen eines CIDR

Führen Sie die Schritte in diesem Abschnitt aus, um einen IPAM-Pool zu erstellen, aus dem Sie die Elastic-IP-Adressen zuweisen.

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 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 die Option aus IPv4.
8. Belassen Sie unter Ressourcenplanung den IP-Bereich für den Plan innerhalb des ausgewählten Bereichs ausgewählt.
9. Wählen Sie unter Gebietsschema das Gebietsschema für den Pool aus. Das Gebietsschema ist die AWS Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Die verfügbaren Optionen stammen aus den Betriebsregionen, die Sie beim Erstellen Ihres IPAM ausgewählt haben.

10. Wählen Sie unter Service die Option 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 CIDRs zugewiesenen Daten für den EC2 Amazon-Service (für Elastic IP-Adressen) beworben werden.
11. Wählen Sie unter Öffentliche IP-Quelle die Option Amazon-eigen aus.
12. Wählen Sie unter CIDR für die Bereitstellung die Option Öffentliches CIDR im Besitz von Amazon hinzufügen aus. Wählen Sie eine Länge der Netzmaske zwischen `/29` (8 IP-Adressen) und `/30` (4 IP-Adressen). Sie können standardmäßig bis zu 2 hinzufügen. CIDRs Informationen zur Erhöhung der Grenzwerte für von Amazon bereitgestellte zusammenhängende öffentliche Inhalte finden Sie unter. IPv4 CIDRs Kontingente für Ihr IPAM
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 Status der Bereitstellung auf der CIDRsRegisterkarte auf der Seite mit den Pool-Details sehen.

Command line

So erstellen Sie einen Pool

1. Erstellen Sie mit dem Befehl einen IPAM-Pool. create-ipam-pool Das Gebietsschema AWS -Region, in der dieser IPAM-Pool für Zuweisungen verfügbar sein soll. Die verfügbaren Optionen stammen aus den Betriebsregionen, die Sie beim Erstellen Ihres IPAM ausgewählt haben.

```
aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-
scope-01bc7290e4a9202f9 --address-family ipv4 --locale us-east-1 --aws-service
 ec2 --public-ip-source amazon
```

Beispielantwort mit Status `create-in-progress`:

```
{

    "IpamPool": {
```

```
        "OwnerId": "320805250157",

        "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",

        "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-07ccc86aa41bef7ce",
        "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-01bc7290e4a9202f9",
        "IpamScopeType": "public",

        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",

        "IpamRegion": "us-east-1",

        "Locale": "us-east-1",

        "PoolDepth": 1,

        "State": "create-in-progress",

        "AutoImport": false,

        "AddressFamily": "ipv4",

        "Tags": [],

        "AwsService": "ec2",

        "PublicIpSource": "amazon"

    }

}
```

2. Überprüfen Sie mit dem describe-ipam-poolsBefehl, ob der Pool erfolgreich erstellt wurde.

```
aws ec2 describe-ipam-pools --region us-east-1 --ipam-pool-ids ipam-
pool-07ccc86aa41bef7ce
```

Beispielantwort mit Status `create-complete`:

```
{
```

```
    "IpamPools": [
        {
            "OwnerId": "320805250157",
            "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",
            "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-07ccc86aa41bef7ce",
            "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-01bc7290e4a9202f9",
            "IpamScopeType": "public",
            "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
            "IpamRegion": "us-east-1",
            "Locale": "us-east-1",
            "PoolDepth": 1,
            "State": "create-complete",
            "AutoImport": false,
            "AddressFamily": "ipv4",
            "Tags": [],
            "AwsService": "ec2",
            "PublicIpSource": "amazon"
        }
    ]
}
```

3. Stellen Sie mit dem provision-ipam-pool-cidrBefehl ein CIDR für den Pool bereit. Wählen Sie eine `--netmask-length` zwischen `/29` (8 IP-Adressen) und `/30` (4 IP-Adressen). Sie können CIDRs standardmäßig bis zu 2 hinzufügen. Informationen zur Erhöhung der Grenzwerte für von Amazon bereitgestellte zusammenhängende öffentliche Inhalte finden Sie unter. IPv4 CIDRs Kontingente für Ihr IPAM

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce --netmask-length 29
```

Beispielantwort mit Status `pending-provision`:

```
{

    "IpamPoolCidr": {
        "State": "pending-provision",
        "IpamPoolCidrId": "ipam-pool-cidr-01856e43994df4913b7bc6aac47adf983",
        "NetmaskLength": 29
    }
}
```

4. Stellen Sie sicher, dass dieses CIDR bereitgestellt wurde, bevor Sie fortfahren. Sie können den Status der Bereitstellung mithilfe des Befehls anzeigen. get-ipam-pool-cidrs

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

Beispielantwort mit Status `provisioned`:

```
{

    "IpamPoolCidrs": [
        {
            "Cidr": "18.97.0.40/29",
            "State": "provisioned",
            "IpamPoolCidrId": "ipam-pool-
cidr-01856e43994df4913b7bc6aac47adf983",
            "NetmaskLength": 29
        }
    ]
}
```

Schritt 3: Zuweisen einer Elastic-IP-Adresse aus dem Pool

Führen Sie die Schritte in diesem Abschnitt aus, um eine Elastic-IP-Adresse aus dem Pool zuzuweisen.

AWS Management Console

Folgen Sie den Schritten unter Zuweisen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch, um die Adresse zuzuweisen. Beachten Sie dabei jedoch Folgendes:

- Stellen Sie sicher, dass die AWS Region, in der Sie sich in der EC2 Konsole befinden, der Locale-Option entspricht, die Sie bei der Erstellung des Pools in Schritt 2 ausgewählt haben.
- Wählen Sie bei der Auswahl des Adresspools die Option Zuweisen mithilfe eines IPv4 IPAM-Pool und dann den Pool aus, den Sie in Schritt 1 erstellt haben.

Command line

Weisen Sie mit dem Befehl allocate-address eine Adresse aus dem Pool zu. Der von Ihnen verwendete `--region` muss mit der Option `-locale` übereinstimmen, die Sie bei der Erstellung des Pools in Schritt 2 ausgewählt haben. Geben Sie in `--ipam-pool-id` die ID des IPAM-Pools an, den Sie in Schritt 2 erstellt haben.

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

Beispielantwort:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

Optional können Sie auch einen bestimmten /32 in Ihrem IPAM-Pool auswählen, indem Sie die Option `--address` verwenden.

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce --address 18.97.0.41
```

Beispielantwort:

```
{
    "PublicIp": "18.97.0.41",
    "AllocationId": "eipalloc-056cdd6019c0f4b46",
    "PublicIpv4Pool": "ipam-pool-07ccc86aa41bef7ce",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

Weitere Informationen finden Sie unter Zuweisen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch.

Schritt 4: Ordnen Sie die Elastic IP-Adresse einer Instance zu EC2

Führen Sie die Schritte in diesem Abschnitt aus, um die Elastic IP-Adresse einer EC2 Instance zuzuordnen.

AWS Management Console

Folgen Sie den Schritten unter Elastic IP-Adresse zuordnen im EC2 Amazon-Benutzerhandbuch, um eine Elastic IP-Adresse aus dem IPAM-Pool zuzuweisen. Beachten Sie jedoch Folgendes: Wenn Sie die Option AWS Management Console verwenden, muss die AWS Region, der Sie die Elastic IP-Adresse zuordnen, der Locale-Option entsprechen, die Sie bei der Erstellung des Pools in Schritt 2 ausgewählt haben.

Command line

Verknüpfen Sie mit dem Befehl associate-address die Elastic-IP-Adresse mit einer Instance. Der `--region`, dem Sie die Elastic-IP-Adresse zuordnen, muss mit der Option `--locale` übereinstimmen, die Sie bei der Erstellung des Pools in Schritt 2 ausgewählt haben.

```
aws ec2 associate-address --region us-east-1 --instance-id i-07459a6fca5b35823 --
public-ip 18.97.0.41
```

Beispielantwort:

```
{
    "AssociationId": "eipassoc-06aa85073d3936e0e"
}
```

Weitere Informationen finden Sie im EC2 Amazon-Benutzerhandbuch unter Eine Elastic IP-Adresse mit einer Instance oder Netzwerkschnittstelle verknüpfen.

Schritt 5: Verfolgen und Überwachen der Poolnutzung

Sobald Sie Elastic-IP-Adressen aus dem IPAM-Pool zugewiesen haben, können Sie die IPAM-Pool-Zuweisungen nachverfolgen und überwachen.

AWS Management Console

- Zeigen Sie die IPAM-Pool-Details auf der Registerkarte Zuweisungen der IPAM-Konsole an. Alle Elastic-IP-Adressen, die aus dem IPAM-Pool zugewiesen werden, haben den Ressourcentyp EIP.
- Verwendung von Einblicke in öffentliche IPs:
  - Filtern Sie unter Öffentliche IP-Typen nach EIPsAmazon-Eigentum. Dies zeigt die Gesamtzahl der öffentlichen IPv4 Adressen, die Amazon-eigenen Elastic IP-Adressen zugewiesen wurden. Wenn Sie nach dieser Kennzahl filtern und unten auf der Seite zu Öffentliche IP-Adressen scrollen, sehen Sie die von Ihnen zugewiesenen Elastic-IP-Adressen.
  - Filtern Sie unter EIP-Nutzung nach Associated Amazon-Owned EIPs oder Unassociated Amazon-Owned. EIPs Hier wird die Gesamtzahl der Elastic IP-Adressen angezeigt, die Sie in Ihrem AWS Konto zugewiesen haben und die Sie mit einer EC2 Instance, Netzwerkschnittstelle oder Ressource verknüpft haben oder nicht. AWS Wenn Sie nach dieser Kennzahl filtern und unten auf der Seite zu Öffentliche IP-Adressen scrollen, sehen Sie Details zu den gefilterten Ressourcen.
  - Überwachen Sie unter Amazon-eigener IPv4 zusammenhängender Nutzung die sequentielle IPs Nutzung öffentlicher IPv4 Adressen im Laufe der Zeit und die damit verbundenen IPAM-Pools im Besitz von Amazon. IPv4
- Verwenden Sie Amazon CloudWatch , um Metriken zu verfolgen und zu überwachen, die sich auf von Amazon bereitgestellte zusammenhängende öffentliche IPv4 Blöcke beziehen, die für IPAM-Pools bereitgestellt wurden. Die verfügbaren Metriken für zusammenhängende IPv4 Blöcke finden Sie unter Öffentliche IP-Metriken unter. IPAM-Metriken Zusätzlich zur Anzeige von Kennzahlen können Sie in Amazon Alarme erstellen, um Sie CloudWatch zu benachrichtigen, wenn Schwellenwerte erreicht werden. Das Erstellen von Alarmen und das Einrichten von Benachrichtigungen bei Amazon CloudWatch würde den Rahmen dieses Tutorials sprengen. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

Command line

- Zeigen Sie die IPAM-Pool-Zuweisungen mit dem get-ipam-pool-allocationsBefehl an. Alle Elastic-IP-Adressen, die aus dem IPAM-Pool zugewiesen werden, haben den Ressourcentyp EIP.

```
aws ec2 get-ipam-pool-allocations --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce
```

Beispielantwort:

```
{
     "IpamPoolAllocations": [
        {
            "Cidr": "18.97.0.40/32",
            "IpamPoolAllocationId": "ipam-pool-
alloc-0bd07df786e8148aba2763e2b6c1c44bd",
            "ResourceId": "eipalloc-0c9decaa541d89aa9",
            "ResourceType": "eip",
            "ResourceRegion": "us-east-1",
            "ResourceOwner": "320805250157"
        }
    ]
}
```

- Verwenden Sie Amazon CloudWatch , um Metriken zu verfolgen und zu überwachen, die sich auf von Amazon bereitgestellte zusammenhängende öffentliche IPv4 Blöcke beziehen, die für IPAM-Pools bereitgestellt wurden. Die verfügbaren Metriken für zusammenhängende IPv4 Blöcke finden Sie unter Öffentliche IP-Metriken unter. IPAM-Metriken Zusätzlich zur Anzeige von Kennzahlen können Sie in Amazon Alarme erstellen, um Sie CloudWatch zu benachrichtigen, wenn Schwellenwerte erreicht werden. Das Erstellen von Alarmen und das Einrichten von Benachrichtigungen bei Amazon CloudWatch würde den Rahmen dieses Tutorials sprengen. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

Das Tutorial ist nun abgeschlossen. Sie haben einen IPAM-Pool mit einem von Amazon bereitgestellten zusammenhängenden öffentlichen IPv4 CIDR-Block erstellt, Elastic IP-Adressen aus dem Pool zugewiesen und gelernt, wie Sie IPAM-Poolzuweisungen überwachen können. Fahren Sie mit dem nächsten Abschnitt fort, um die Ressourcen zu löschen, die Sie in diesem Tutorial erstellt haben.

Bereinigen

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

Schritt 1: Aufheben der Zuweisung der Elastic-IP-Adresse

Führen Sie die Schritte unter Trennen einer Elastic IP-Adresse im EC2 Amazon-Benutzerhandbuch aus, um die Elastic IP-Adresse zu trennen.

Schritt 2: Freigeben der Elastic-IP-Adresse

Führen Sie die Schritte unter Elastic IP Address veröffentlichen im EC2 Amazon-Benutzerhandbuch aus, um eine Elastic IP-Adresse aus dem öffentlichen IPv4 Pool freizugeben.

Schritt 3: Aufheben der Bereitstellung des CIDR aus dem IPAM-Pool

Führen Sie die Schritte unter Deprovisionierung CIDRs aus einem Pool aus, um die Bereitstellung des Amazon-eigenen öffentlichen CIDR aus dem IPAM-Pool aufzuheben. Dieser Schritt ist für das Löschen eines Pools erforderlich. Ihnen wird der von Amazon bereitgestellte zusammenhängende IPv4 Block in Rechnung gestellt, bis dieser Schritt abgeschlossen ist.

Schritt 4: Löschen des IPAM-Pools

Führen Sie die Schritte unter Einen Pool löschen aus, um den IPAM-Pool zu löschen.

Schritt 5: Löschen des IPAM

Führen Sie die Schritte unter Löschen Sie ein IPAM aus, um das IPAM zu löschen.

Das Tutorial zur Bereinigung ist abgeschlossen.

Identity and Access Management in IPAM

AWS verwendet Sicherheitsanmeldedaten, 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, Diensten und Anwendungen die vollständige oder eingeschränkte Nutzung Ihrer AWS Ressourcen zu ermöglichen, ohne Ihre Sicherheitsanmeldeinformationen weiterzugeben.

In diesem Abschnitt werden die AWS dienstbezogenen Rollen beschrieben, die speziell für IPAM erstellt wurden, sowie die verwalteten Richtlinien, die den dienstbezogenen IPAM-Rollen zugeordnet sind. Weitere Informationen zu AWS -IAM-Rollen und -Richtlinien finden Sie unter Rollenbegriffe und -Konzepte im IAM-Benutzerhandbuch.

Weitere Informationen zur Identitäts- und Zugriffsverwaltung für VPC finden Sie unter Identitäts- und Zugriffsmanagement für Amazon VPC im Amazon VPC-Benutzerhandbuch.

Inhalt

Serviceverknüpfte Rollen für IPAM

IPAM verwendet AWS Identity and Access Management dienstverknüpfte Rollen (IAM). Eine dienstverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle. Dienstbezogene Rollen sind von IPAM vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstverknüpfte Rolle erleichtert die Einrichtung von IPAM, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. IPAM definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur IPAM seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Berechtigungen von serviceverknüpften Rollen

IPAM verwendet die dienstverknüpfte AWSServiceRoleForIPAM-Rolle, um die Aktionen in der angehängten verwalteten Richtlinie aufzurufen. AWSIPAMServiceRolePolicy Weitere Informationen zu den zulässigen Aktionen in dieser Richtlinie finden Sie unter AWS verwaltete Richtlinien für IPAM.

Der dienstbezogenen Rolle ist auch eine IAM-Vertrauensrichtlinie beigefügt, die es dem Dienst ermöglicht, die `ipam.amazonaws.com` dienstverknüpfte Rolle zu übernehmen.

Erstellen der serviceverknüpften Rolle

IPAM überwacht die IP-Adressnutzung in einem oder mehreren Konten, indem es die dienstbezogene Rolle in einem Konto übernimmt, die Ressourcen und ihre CIDRs Ressourcen ermittelt und die Ressourcen in IPAM integriert.

Die serviceverknüpfte Rolle wird auf zwei Arten erstellt:

- Wenn Sie sich mit AWS -Organisationen integrieren

  Wenn Sie Integrieren Sie IPAM mit Konten in einer Organisation AWS die IPAM-Konsole oder den `enable-ipam-organization-admin-account` AWS CLI Befehl verwenden, wird die mit dem AWSServiceRoleForIPAM-Dienst verknüpfte Rolle automatisch in jedem Mitgliedskonten Ihrer AWS Organizations erstellt. Infolgedessen sind die Ressourcen in allen Mitgliedskonten von IPAM auffindbar.

  > **Important**
  >
  > Damit IPAM die serviceverknüpfte Rolle in Ihrem Namen erstellen kann:
  >
  > - Dem AWS Organisationsverwaltungskonto, das die IPAM-Integration mit AWS Organizations ermöglicht, muss eine IAM-Richtlinie angehängt sein, die die folgenden 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

  Falls SieVerwenden Sie IPAM mit einem einzigen Konto, wird die mit dem AWSServiceRoleForIPAM-Dienst verknüpfte Rolle automatisch erstellt, wenn Sie ein IPAM als dieses Konto erstellen.

  > **Important**
  >
  > Wenn Sie IPAM mit einem einzigen AWS Konto verwenden, müssen Sie vor der Erstellung eines IPAM sicherstellen, dass dem AWS Konto, das Sie verwenden, eine IAM-Richtlinie zugeordnet ist, die die Aktion zulässt. `iam:CreateServiceLinkedRole` Wenn Sie das IPAM erstellen, erstellen Sie automatisch die mit dem IPAM-Dienst verknüpfte Rolle. AWSService RoleFor Weitere Informationen zur Verwaltung von IAM-Richtlinien finden Sie unter Bearbeiten einer Beschreibung einer dienstbezogenen Rolle im IAM-Benutzerhandbuch.

Bearbeiten der serviceverknüpften Rolle

Sie können die dienstverknüpfte AWSServiceRoleForIPAM-Rolle nicht bearbeiten.

Löschen der serviceverknüpften Rolle

Wenn Sie IPAM nicht mehr verwenden müssen, empfehlen wir Ihnen, die dienstverknüpfte AWSServiceRoleForIPAM-Rolle 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.

Gehen Sie wie folgt vor, um die serviceverknüpfte Rolle über die AWS CLI zu löschen:

1. Löschen Sie Ihre IPAM-Ressourcen mithilfe von deprovision-ipam-pool-cidrund delete-ipam. Weitere Informationen erhalten Sie unter Deprovisionierung CIDRs aus einem Pool und Löschen Sie ein IPAM.
2. Deaktivieren Sie das IPAM-Konto mit -account. disable-ipam-organization-admin

3. Deaktivieren Sie den IPAM-Dienst disable-aws-service-accessmit der Option. `--service-principal ipam.amazonaws.com`
4. Löschen Sie die mit dem Dienst verknüpfte 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 ein IPAM erstellen, wird die AWSIPAMServiceRolePolicyverwaltete Richtlinie automatisch in Ihrem IAM-Konto erstellt und an die mit dem AWSService RoleFor IPAM-Dienst verknüpfte Rolle angehängt.

Wenn Sie die IPAM-Integration mit AWS Organizations aktivieren, wird die AWSIPAMServiceRolePolicyverwaltete Richtlinie automatisch in Ihrem IAM-Konto und in jedem Ihrer Organisations-Mitgliedskonten erstellt, und die verwaltete Richtlinie wird der mit dem AWSServiceRoleForIPAM-Dienst verknüpften Rolle angehängt. AWS

Mit dieser verwalteten Richtlinie hat IPAM folgende Möglichkeiten:

- Überwachung CIDRs der Netzwerkressourcen aller Mitglieder Ihrer Organisation. AWS
- Speichern Sie Metriken zu 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.

JSON

```
{
    "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",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsPublishActions",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

Die erste Aussage im vorherigen Beispiel ermöglicht es IPAM, die CIDRs Nutzung durch Ihr einzelnes AWS Konto oder die Mitglieder Ihrer Organisation zu überwachen. AWS

Die zweite Anweisung im vorherigen Beispiel verwendet den `cloudwatch:PutMetricData` Bedingungsschlüssel, um es IPAM zu ermöglichen, IPAM-Metriken in Ihrem `AWS/IPAM` CloudWatch Amazon-Namespace zu speichern. Diese Metriken werden von der verwendet AWS Management Console , um Daten über die Zuweisungen in Ihren IPAM-Pools und -Bereichen anzuzeigen. Weitere Informationen finden Sie unter Überwachen der CIDR-Nutzung mit dem IPAM-Dashboard.

Aktualisierungen der verwalteten Richtlinie AWS

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien für IPAM, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen.

Änderung	Beschreibung	Datum
AWSIPAMServiceRolePolicy	Der AWSIPAMService RolePolicy verwalteten Richtlinie (`organizations:ListChildren` , `undorganizations:DescribeOrganizationalUnit`) wurden Aktionen hinzugefügt`organizations:ListParents` , damit IPAM die Details von Organisationseinheiten (OUs) in AWS Organizations abrufen kann, sodass Kunden IPAM auf OU-Ebene verwenden können.	21. November 2024
AWSIPAMServiceRolePolicy	Der AWSIPAMService RolePolicy verwalteten Richtlinie (`ec2:GetIpamDiscoveredPublicAddresses`) wurde eine Aktion hinzugefügt, damit IPAM während der Ressource	13. November 2023

Änderung	Beschreibung	Datum
	nerkennung öffentliche IP-Adressen abrufen kann.	
AWSIPAMServiceRolePolicy	Der AWSIPAMService RolePolicy verwaltet en Richtlinie wurden Aktionen hinzugefügt (`ec2:DescribeAccountAttributes` ,`ec2:DescribeNetworkInterfaces` ,`ec2:DescribeSecurityGroups` , `ec2:DescribeSecurityGroupRules` `ec2:DescribeVpnConnections` , und`globalaccelerator:ListByoipCidrs`)`globalaccelerator:ListAccelerators` , damit IPAM während der Ressource nsuche öffentliche IP-Adressen abrufen kann.	1. November 2023

Änderung	Beschreibung	Datum
AWSIPAMServiceRolePolicy	Der AWSIPAMService RolePolicy verwaltet en Richtlinie wurden zwei Aktionen hinzugefü gt (`ec2:GetIp amDiscoveredAccoun ts` und`ec2:GetIp amDiscoveredResour ceCidrs`), damit IPAM die AWS Konten und Ressource n abrufen kann, die bei der CIDRs Ressourcensuche überwacht werden.	25. Januar 2023
IPAM hat mit der Verfolgung von Änderungen begonnen	IPAM begann, Änderungen für seine AWS verwalteten Richtlinien nachzuverfolgen.	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 umfassende Nutzung der IPAM-Konsole müssen Sie möglicherweise zusätzliche IAM-Aktionen für Dienste wie AWS Organizations, AWS Resource Access Manager(RAM) und hinzufügen. Amazon CloudWatch

JSON

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIpamByoasn",
```

```
                "ec2:DeprovisionIpamByoasn",
                "ec2:DescribeIpamByoasn",
                "ec2:DisassociateIpamByoasn",
                "ec2:ProvisionIpamByoasn",
                "ec2:CreateIpam",
                "ec2:DescribeIpams",
                "ec2:ModifyIpam",
                "ec2:DeleteIpam",
                "ec2:CreateIpamScope",
                "ec2:DescribeIpamScopes",
                "ec2:ModifyIpamScope",
                "ec2:DeleteIpamScope",
                "ec2:CreateIpamPool",
                "ec2:DescribeIpamPools",
                "ec2:ModifyIpamPool",
                "ec2:DeleteIpamPool",
                "ec2:ProvisionIpamPoolCidr",
                "ec2:GetIpamPoolCidrs",
                "ec2:DeprovisionIpamPoolCidr",
                "ec2:AllocateIpamPoolCidr",
                "ec2:GetIpamPoolAllocations",
                "ec2:ReleaseIpamPoolAllocation",
                "ec2:CreateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveries",
                "ec2:ModifyIpamResourceDiscovery",
                "ec2:DeleteIpamResourceDiscovery",
                "ec2:AssociateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveryAssociations",
                "ec2:DisassociateIpamResourceDiscovery",
                "ec2:GetIpamResourceCidrs",
                "ec2:ModifyIpamResourceCidr",
                "ec2:GetIpamAddressHistory",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
            "Condition": {
```

```
                "StringLike": {
                    "iam:AWSServiceName": "ipam.amazonaws.com"
                }
            }
        }
    ]
}
```

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 zusammenhängende öffentliche CIDR-Blöcke IPv4	2	Ja. Wenden Sie sich an das AWS Support Center, wie unter AWS Servicequotas in der beschrieben Allgemeine AWS-Referenz.
Von Amazon bereitgestellte zusammenhängende öffentliche IPv4 CIDR-Blocknetzmaskenlänge	/29	Die zulässige Größe liegt zwischen /29 und /30. Um eine Erhöhung zu beantragen, wenden Sie sich an das AWS Support Center, wie unter AWS Servicekontingenten in der beschrieben Allgemeine AWS-Referenz.
Von Amazon bereitgestellte IPv6 CIDR-Blocknetzmaskenlänge	/52	Ja. Wenden Sie sich an das AWS Support Center, wie unter AWS Servicequotas in der beschrieben

Name	Standard	Anpassbar
		Allgemeine AWS-Referenz.
Von Amazon bereitgestellte IPv6 CIDR-Blöcke pro Regionalpool	1	Ja. Wenden Sie sich an das AWS Support Center, wie unter AWS Servicequotas in der beschrieben Allgemeine AWS-Referenz.
Autonome Systemnummern (ASNs), die Sie zu IPAM bringen können	5	Ja. Wenden Sie sich an das AWS Support Center, wie unter AWS Servicequotas in der beschrieben Allgemeine AWS-Referenz.
CIDRs pro Pool	50	Ja
IPAM-Administratoren pro Organisation	1	Nein
IPAMs pro Region	1	Nein
Ausschlüsse von Organisationseinheiten pro Ressourcenerkennung	10	Ja. Wenden Sie sich an das AWS Support Center, wie unter AWS Servicequotas in der beschrieben Allgemeine AWS-Referenz.
Pooltiefe (Anzahl der Pools innerhalb von Pools)	10	Ja
Pools pro Bereich	50	Ja

Name	Standard	Anpassbar
Zuordnungen zur Ressourcenerkennung pro IPAM	5	Ja
Ressourcenergebnisse pro Region	1	Nein
Metriken zur Ressourcenauslastung	50	Ja. Wenden Sie sich an das AWS Support Center, wie unter AWS Servicequotas in der beschrieben Allgemeine AWS-Referenz.
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

Amazon VPC IP Address Manager (IPAM) ist ein Service, der Sie bei der Verwaltung Ihres IP-Adressraums in Ihren AWS Ressourcen und lokalen Netzwerken unterstützt. IPAM bietet eine zentrale Möglichkeit zur Planung, Überwachung und Steuerung der IP-Adressen, die von Ihren AWS und lokalen Ressourcen verwendet werden.

In diesem Abschnitt wird beschrieben, wie Sie preisbezogene Informationen und Ihre aktuellen IPAM-Kosten anzeigen.

Inhalt

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 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 zu https://console.aws.amazon.com/cost-management/Hause.
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- IPAddress Manager-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 beispielsweise 18 Stunden beträgt, bedeutet dies, dass Sie 1 aktive IP-Adresse für 18 Stunden, 3 IP-Adressen in 3 verschiedenen Regionen, die jeweils für 6 Stunden aktiv sind, oder eine beliebige Kombination dieser Adressen haben könnten, die zusammen 18 Stunden ergeben.

Weitere Informationen zu finden Sie unter Analysieren AWS Cost Explorer Ihrer Kosten mit im Benutzerhandbuch. AWS Cost ExplorerAWS Cost Management

Ähnliche Informationen

Die Website mit der AWS technischen Dokumentation ist zwar eine umfassende Ressource, aber es gibt viele andere Orte, an denen Sie Informationen zu AWS Dienstleistungen finden können. AWS Blogs, Whitepapers, Fallstudien und Community-Foren können wertvolle Einblicke, Beispiele aus der Praxis und alternative Perspektiven bieten, die über die offiziellen technischen Details hinausgehen. Die Erkundung dieser verschiedenen Quellen kann Ihnen ein umfassenderes Verständnis der Angebote vermitteln. AWS

Die folgenden verwandten Ressourcen bieten Ihnen nützliche Informationen für die Arbeit mit Amazon VPC IP Address Manager.

- Bewährte Methoden für Amazon VPC IP Address Manager: Ein AWS Blog über bewährte Methoden für die Planung und Erstellung eines skalierbaren Adressschemas mit Amazon VPC IP Address Manager.
- Netzwerkadressverwaltung und -überwachung im großen Maßstab mit Amazon VPC IP Address Manager: Ein AWS Blog, der Amazon VPC IP Address Manager vorstellt und Ihnen zeigt, wie Sie den Service in der AWS Konsole verwenden können.
- Konfigurieren Sie den detaillierten Zugriff auf Ihre gemeinsam genutzten Ressourcen mithilfe von AWS Resource Access Manager: Ein AWS Blog, in dem erklärt wird, wie Sie einen IPAM-Pool mit den Konten in einer AWS Organisationseinheit teilen.
- Visualisieren Sie die Verwaltung und Planung von Unternehmens-IP-Adressen mit CIDR-Map: Ein AWS Blog, in dem erklärt wird, wie Sie Ihre gesamte IPv4 IPv6 IT-Landschaft mithilfe der IPAM-CIDR-Map in der IPAM-Konsole visualisieren können.

Dokumentverlauf für IPAM

Die folgende Tabelle beschreibt die Versionen für IPAM.

Funktion	Beschreibung	Veröffentlichungsdatum
Kostenverteilung aktivieren	Wenn Sie die Kostenverteilung aktivieren, verteilen Sie die Gebühren für aktive IP-Adressen auf die Konten, die die IP-Adressen verwenden, und nicht auf den IPAM-Besitzer. Dies ist nützlich für große Organisationen, in denen der delegierte IPAM-Administrator die IP-Adressen zentral mithilfe von IPAM verwaltet und jedes Konto für seine eigene Nutzung verantwortlich ist, sodass keine manuellen Abrechnungsberechnungen erforderlich sind.	1. Mai 2025
Ausschließen von Organisationseinheiten von IPAM	Wenn Ihr IPAM in AWS Organizations integriert ist, können Sie jetzt Organisationseinheiten von IPAM ausschließen. IPAM verwaltet keine IP-Adressen in Konten, die von Organisationseinheiten ausgeschlossen sind.	21. November 2024
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer vorhandenen Richtlinie	Bestehende AWSIPAMService RolePolicy aktualisiert.	21. November 2024
Zuweisen von sequentiellen Elastic-IP-Adressen aus einem IPAM-Pool	Mit IPAM können Sie jetzt öffentliche IPv4 Blöcke, die Amazon gehören, für IPAM-Pools bereitstellen und sequentielle Elastic IP-Adressen aus diesen Pools Ressourcen zuweisen. AWS Sequentielle Elastic-IP-	28. August 2024

Funktion	Beschreibung	Veröffentlichungsdatum
	Adressen ermöglichen es Ihnen, Ihre Netzwerk- und Sicherheitsanforderungen zu vereinfachen.	
Private GUA und IPv6 ULAs	Sie können jetzt private IPv6 GUA- und ULA-Bereiche für einen IPAM-Pool in einem privaten Bereich bereitstellen. Private IPv6 Adressen sind nur in IPAM verfügbar. Weitere Informationen IPv6 zur privaten Adressierung finden Sie unter Private IPv6 Adressen im Amazon VPC-Benutzerhandbuch.	8. August 2024
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 IP-Adressen in Amazon einsehen CloudWatch.	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) zu AWS mitbringen.	17. November 2023

Funktion	Beschreibung	Veröffentlichungsdatum
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Bestehende AWSIPAMService RolePolicy aktualisiert.	17. November 2023
AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Bestehende AWSIPAMService RolePolicy aktualisiert.	1. November 2023
Metriken zur Ressourcenauslastung	IPAM veröffentlicht jetzt IP-Nutzungsmetriken für Ressourcen, die das IPAM überwacht, für Amazon. CloudWatch	2. August 2023
Einblicke in öffentliche IP-Adressen	Public IP Insights zeigt Ihnen in Ihrem Konto alle öffentlichen IPv4 Adressen, die von Diensten in dieser Region verwendet werden. Sie können diese Erkenntnisse nutzen, um die Nutzung öffentlicher IPv4 Adressen zu ermitteln und Empfehlungen zur Freigabe ungenutzter Elastic IP-Adressen einzusehen.	28. Juli 2023
AWS verwaltete Policy-Updates — Aktualisierung einer bestehenden Policy	Bestehende AWSIPAMService RolePolicy 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

Funktion	Beschreibung	Veröffentlichungsdatum
Von Amazon bereitgestellter IPv6 zusammenhängender CIDR-Block für IPAM-Pools	Wenn Sie einen IPAM-Pool im öffentlichen Bereich erstellen, können Sie jetzt einen von Amazon bereitgestellten IPv6 zusammenhängenden CIDR-Block für den Pool bereitstellen. Weitere Informationen finden Sie unter Erstellen Sie IPv6 Adresspools in Ihrem IPAM.	25. Januar 2023
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.