aws

IP Address Manager

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: IP Address Manager

Table of Contents

Qu'est-ce qu'IPAM ? 1
Fonctionnement d'IPAM 2
Démarrage avec IPAM 4
Accès à IPAM 4
Configuration des autorisations pour votre IPAM 5
Intégrer l'IPAM aux comptes d'une organisation AWS 6
Intégration d'IPAM à des comptes extérieurs à votre organisation 8
Utilisation d'IPAM avec un seul compte 11
Création d'un IPAM 12
Planification de l'approvisionnement des adresses IP 14
Exemples de plans de groupes IPAM 16
Création de groupes IPv4 18
Création de groupes IPv6 28
Allocation de CIDR 36
Création d'un VPC qui utilise un CIDR de groupe IPAM 37
Allocation manuelle d'un CIDR à un groupe pour réserver de l'espace d'adresse IP 37
Gestion de l'espace d'adressage IP dans IPAM 39
Application de l'utilisation d'IPAM pour la création de VPC 39
Appliquer IPAM lors de la création de VPC 40
Appliquer un groupe IPAM lors de la création de VPC 40
Appliquer IPAM à toutes les unités d'organisation à l'exception d'une liste donnée 41
Partage d'un groupe IPAM à l'aide d'AWS RAM 42
Approvisionnement de CIDR à un groupe 45
Pour désapprovisionner un CIDR de groupe 46
Modification d'un groupe 48
Suppression d'un groupe 48
Utilisation des découvertes de ressources 50
Créer une découverte de ressources 50
Afficher les détails d'une découverte de ressources 52
Partage d'une découverte de ressources 54
Associer une découverte de ressources à un IPAM 56
Dissocier une découverte de ressources 58
Supprimer une découverte de ressources 59
Création de portées supplémentaires 59

Déplacez des CIDR VPC entre les portées 61
Modifiez l'état de contrôle des CIDR VPC 62
Suppression d'une portée 64
Libération d'une allocation 65
Modifier un IPAM 67
Modifier un niveau IPAM 67
Modifiez les régions d'exploitation IPAM 68
Suppression d'un IPAM 69
Suivi de l'utilisation des adresses IP dans IPAM 72
Contrôle de l'utilisation des CIDR à l'aide du tableau de bord IPAM 72
Contrôle de l'utilisation du CIDR par ressource 75
Surveiller l'IPAM avec Amazon CloudWatch 79
Métriques relatives aux groupes et champs d'application IPAM 79
Métriques d'utilisation des ressources 81
Afficher l'historique des adresses IP 87
Affichage de Public IP Insights 91
Didacticiels 96
Créer un IPAM et des groupes à l'aide de la console 96
Prérequis 97
Comment AWS Organizations s'intègre à IPAM 97
Étape 1 : délégation d'un administrateur IPAM 99
Étape 2 : création d'un IPAM 100
Étape 3 : Création d'un groupe IPAM de niveau supérieur 103
Étape 4 : création de groupes IPAM régionaux 108
Étape 5 : création d'un groupe de développement de pré-production 112
Étape 6 : partage du groupe IPAM 116
Étape 7 : création d'un VPC avec un CIDR alloué à partir d'un groupe IPAM 121
Étape 8 : nettoyage 125
Créer un IPAM et des groupes en utilisant la AWS CLI 127
Étape 1 : activation d'IPAM dans votre organisation 128
Étape 2 : création d'un IPAM 128
Étape 3 : création d'un groupe d'adresses IPv4 130
Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur 132
Étape 5. Création d'un groupe régional avec un CIDR provenant du groupe de niveau supérieur 133
Étape 6 : approvisionnement d'un CIDR au groupe régional 135

Étape 7. Création d'un partage RAM pour activer les attributions IP entre les comptes 137
Étape 8. Création d'un VPC 138
Étape 9. Nettoyage 139
Afficher l'historique des adresses IP à l'aide de la AWS CLI 139
Présentation 140
Scénarios 140
Apporter votre ASN à l'IPAM 148
Conditions préalables à l'onboarding de votre ASN 149
Étapes du didacticiel 150
Apporter vos adresses IP à IPAM 154
AWS console et CLI 155
AWS CLI uniquement 182
Transfert d'un CIDR IPv4 BYOIP vers IPAM 227
Étape 1 : Création de profils AWS CLI nommés et de rôles IAM 228
Étape 2 : obtention de l'ID de portée publique de votre IPAM 229
Étape 3 : création d'un groupe IPAM 229
Étape 4 : partager le pool IPAM à l'aide de AWS RAM 231
Étape 5 : transfert d'un CIDR IPV4 BYOIP existant vers IPAM 234
Étape 6 : affichage du CIDR dans IPAM 236
Étape 7 : nettoyage 237
Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau 241
Étape 1 : Créer un VPC 242
Étape 2 : créer un groupe de planification des ressources 243
Étape 3 : créer des groupes de sous-réseaux 244
Étape 4 : créer des sous-réseaux 245
Étape 5 : nettoyage 245
Gestion des identités et des accès dans IPAM 247
Rôles liés à un service pour IPAM 247
Autorisations accordées au rôle lié à un service 247
Création du rôle lié à un service 248
La modification du rôle lié à un service 249
La suppression du rôle lié à un service 249
Stratégies gérées pour IPAM 249
Mises à jour de la stratégie gérée AWS 251
Exemple de stratégie 253
Quotas 256

Tarification 259
Afficher les informations sur la tarification 259
Consultez vos coûts et votre utilisation actuels à l'aide de AWS Cost Explorer 259
Informations connexes 260
Historique de document 261
..... cclxiv

Qu'est-ce qu'IPAM ?

Amazon VPC IP Address Manager (IPAM) est une fonction VPC qui facilite la planification, le suivi et le contrôle des adresses IP pour vos charges de travail AWS. Vous pouvez utiliser les flux de travail automatisés IPAM pour gérer plus efficacement les adresses IP.

Vous pouvez utiliser IPAM pour effectuer les tâches suivantes :

- Organiser l'espace d'adressage IP dans des domaines de routage et de sécurité.
- Contrôler l'espace d'adressage IP utilisé et contrôler les ressources qui utilisent l'espace par rapport aux règles métier.
- Afficher l'historique des affectations d'adresses IP dans votre organisation.
- Allouer automatiquement des CIDR aux VPC à l'aide de règles métier spécifiques.
- Résoudre les problèmes de connectivité réseau.
- Activer le partage entre Régions et entre comptes de vos adresses BYOIP (Bring Your Own IP).
- Provisionner des blocs CIDR IPv6 contigus fournis par Amazon dans des groupes pour la création de VPC

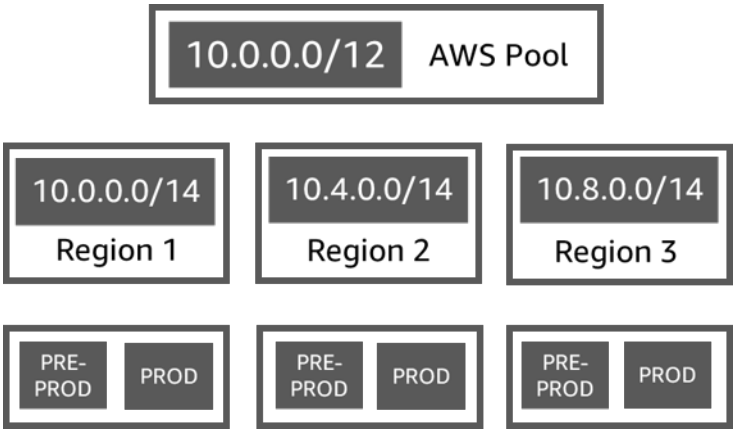
Ce guide comprend les sections suivantes :

- Fonctionnement d'IPAM : concepts et terminologie d'IPAM.
- Démarrage avec IPAM : étapes pour activer la gestion des adresses IP à l'échelle de l'entreprise avec AWS Organizations, créer un IPAM et planifier l'utilisation des adresses IP.
- Gestion de l'espace d'adressage IP dans IPAM : étapes pour gérer l'IPAM, les portées, les groupes et les allocations.
- Suivi de l'utilisation des adresses IP dans IPAM : étapes pour contrôler et suivre l'utilisation des adresses IP avec IPAM.
- Didacticiels pour Amazon VPC IP Address Manager (IPAM): Didacticiels détaillés, étape par étape, pour créer un IPAM et des groupes, allouer des CIDR de VPC et fournir vos propres CIDR d'adresses IP publiques à IPAM.

Fonctionnement d'IPAM

Pour vous aider à démarrer avec IPAM, cette rubrique explique certains des concepts clés.

Le diagramme suivant montre une hiérarchie de groupes IPAM pour plusieurs Régions AWS dans un groupe IPAM de niveau supérieur. Chaque groupe régional AWS comprend deux groupes de développement IPAM, un groupe pour la préproduction et un groupe de ressources de production. Pour plus d'informations sur les concepts d'IPAM, consultez les descriptions sous le diagramme.



Pour utiliser Amazon VPC IP Address Manager, vous devez d'abord créer un IPAM.

Lorsque vous créez l'IPAM, vous sélectionnez son nom et une Région AWS pour sa création. Lorsque vous créez un IPAM, AWS VPC IPAM crée automatiquement deux portées pour l'IPAM. Les portées, ainsi que les groupes et les allocations, sont des composants clés de votre IPAM.

- Une portée est le conteneur de niveau le plus élevé d'IPAM. Un IPAM contient deux portées par défaut. Chaque portée représente l'espace IP d'un réseau unique. La portée privée est destinée à tous les espaces privés. La portée publique est destinée à tous les espaces publics. Les portées vous permettent de réutiliser les adresses IP sur plusieurs réseaux non connectés sans provoquer de chevauchement ou de conflit d'adresses IP. Dans une portée, vous créez des groupes IPAM.
- Un groupe est un ensemble de plages d'adresses IP contiguës (ou CIDR). Les groupes IPAM vous permettent d'organiser vos adresses IP selon vos besoins de routage et de sécurité. Vous pouvez avoir plusieurs groupes au sein d'un groupe de niveau supérieur. Par exemple, si vous avez des besoins de routage et de sécurité distincts pour les applications de développement et de production, vous pouvez créer un groupe pour chacune d'elles. Dans les groupes IPAM, vous allouez des CIDR aux ressources AWS.
- Une allocation est une affectation CIDR d'un groupe IPAM vers un autre groupe de ressources ou IPAM. Lorsque vous créez un VPC et que vous choisissez un groupe IPAM pour le CIDR du VPC,

le CIDR est alloué à partir du CIDR provisionné au groupe IPAM. Vous pouvez contrôlez et gérer l'allocation à l'aide d'IPAM.

IPAM peut gérer et contrôler les CIDR IPv4 privés, les CIDR IPv4 ou IPv6 publics que vous possédez et l'espace IPv6 public appartenant à Amazon.

Pour commencer et créer un IPAM, consultez Démarrage avec IPAM.

Démarrage avec IPAM

Suivez les étapes de cette section pour démarrer avec IPAM. Vous commencerez par accéder à IPAM et par décider si vous souhaitez déléguer un compte IPAM. À la fin de cette section, vous aurez créé un IPAM, créé plusieurs groupes d'adresses IP et alloué un CIDR d'un groupe à un VPC.

Table des matières

- Accès à IPAM
- Configuration des autorisations pour votre IPAM
- Création d'un IPAM
- Planification de l'approvisionnement des adresses IP
- Allocation de CIDR

Accès à IPAM

Comme avec d'autres services AWS, vous pouvez créer votre IPAM, y accéder et le gérer à l'aide des méthodes suivantes :

- Console de gestion AWS : offre une interface web que vous pouvez utiliser pour créer et gérer votre IPAM. Reportez-vous à https://console.aws.amazon.com/.
- Interface de ligne de commande AWS (AWS CLI) : propose des commandes pour une large gamme de services AWS, notamment Amazon VPC. L'AWS CLI est prise en charge sur Windows, macOS et Linux. Pour obtenir l'AWS CLI, consultez AWS Command Line Interface.
- Kits AWS SDK : fournissent des API spécifiques aux langages. Les kits de développement (SDK) AWS prennent en charge la plupart des détails de connexion, notamment le calcul des signatures, le traitement des nouvelles tentatives de demande et le traitement des erreurs. Pour plus d'informations, consultez Kits AWS SDK.
- API de requête : fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de l'API de requête est le moyen le plus direct d'accéder à IPAM. Toutefois, il faut alors que votre application gère les détails de bas niveau, notamment la génération du hachage pour signer la demande et la gestion des erreurs. Pour plus d'informations, consultez les actions IPAM dans la Référence API d'Amazon EC2.

Ce guide se concentre principalement sur l'utilisation de la Console de gestion AWS pour créer votre IPAM, y accéder et le gérer. Dans chaque description sur la façon de terminer un processus dans la console, nous incluons des liens vers la documentation relative à l'AWS CLI, qui vous montre comment effectuer la même chose à l'aide de l'AWS CLI.

Si vous utilisez IPAM pour la première fois, consultez Fonctionnement d'IPAM pour en savoir plus sur le rôle d'IPAM dans Amazon VPC, puis suivez les instructions dans Configuration des autorisations pour votre IPAM.

Configuration des autorisations pour votre IPAM

Avant de commencer à utiliser IPAM, vous devez choisir l'une des options de cette section pour permettre à IPAM de contrôler les CIDR associés aux ressources des réseaux EC2 et de stocker des métriques :

- Afin de garantir l'intégration d'IPAM à AWS Organizations et permettre au service IPAM d'Amazon VPC de gérer et contrôler les ressources réseau créées par l'ensemble des comptes membres d'AWS Organizations, veuillez consulter la section Intégrer l'IPAM aux comptes d'une organisation AWS (français non garanti).
- Après avoir intégréAWS Organizations, pour intégrer IPAM à des comptes extérieurs à votre organisation, consultezIntégration d'IPAM à des comptes extérieurs à votre organisation.
- Pour utiliser un compte AWS unique avec IPAM et permettre au service IPAM d'Amazon VPC de gérer et de contrôler les ressources des réseaux que vous créez avec le compte unique, consultez Utilisation d'IPAM avec un seul compte.

Si vous ne choisissez pas l'une de ces options, vous pouvez toujours créer des ressources IPAM, telles que des groupes, mais vous ne verrez pas de métriques dans votre tableau de bord et vous ne pourrez pas contrôler l'état des ressources.

Table des matières

- Intégrer l'IPAM aux comptes d'une organisation AWS
- Intégration d'IPAM à des comptes extérieurs à votre organisation
- Utilisation d'IPAM avec un seul compte

Intégrer l'IPAM aux comptes d'une organisation AWS

Vous pouvez également suivre les étapes décrites dans cette rubrique pour intégrer IPAM à AWS Organizations et déléguer un compte membre comme compte IPAM.

Le compte IPAM est responsable de la création d'un IPAM et de son utilisation pour gérer et contrôler l'utilisation des adresses IP.

L'intégration d'IPAM aux AWS Organizations et la délégation d'un administrateur IPAM présentent les avantages suivants :

- Partagez vos pools IPAM avec votre organisation : Lorsque vous déléguez un compte IPAM, IPAM permet aux comptes membres d'autres AWS Organizations de l'organisation d'allouer des CIDR à partir de pools IPAM partagés à l'aide de AWS Resource Access Manager (RAM). Pour plus d'informations sur la configuration d'une organisation, consultez Qu'est-ce qu' AWS Organizations ? dans le Guide de l'utilisateur AWS Organizations.
- Contrôlez l'utilisation des adresses IP dans votre organisation : lorsque vous déléguez un compte IPAM, vous autorisez IPAM à contrôler l'utilisation de l'IP sur tous vos comptes. Par conséquent, IPAM importe automatiquement dans IPAM les CIDR utilisés par les VPC existants sur les comptes membres d'autres AWS Organizations.

Si vous ne déléguez pas un compte membre d' AWS Organizations en tant que compte IPAM, IPAM surveillera les ressources uniquement dans le AWS compte que vous utilisez pour créer l'IPAM.

Important

- Vous devez activer l'intégration avec AWS Organizations en utilisant IPAM dans la console AWS de gestion ou la enable-ipam-organization-admincommande -account AWS CLI. Cela garantit que le`AWSServiceRoleForIPAM` rôle lié à un service est créé. Si vous activez l'accès sécurisé avec AWS Organizations à l'aide de la console AWS Organizations ou de la commande register-delegated-administrator AWS CLI, le rôle `AWSServiceRoleForIPAM` lié au service n'est pas créé et vous ne pouvez ni gérer ni surveiller les ressources au sein de votre organisation.

Note

Lors de l'intégration à des AWS Organizations :

- IPAM vous facture chaque adresse IP active qu'il contrôle dans vos comptes membres de votre organisation. Pour plus d'informations sur la tarification, consultez Tarification IPAM.
- Vous devez disposer d'un compte dans AWS Organizations et d'un compte de gestion configuré avec un ou plusieurs comptes membres. Pour plus d'informations sur les différents types de comptes, consultez Terminologie et concepts dans le Guide de l'utilisateur AWS Organizations. Pour plus d'informations sur la configuration d'une organisation, consultez Prise en main d' AWS Organizations.
- Le compte IPAM doit être un compte membre d' AWS Organizations. Vous ne pouvez pas utiliser le compte de gestion AWS Organizations comme compte IPAM.
- Le compte IPAM doit utilisé un rôle IAM avec une politique IAM, qui lui est attachée, qui autorise l'action `iam:CreateServiceLinkedRole`. Lorsque vous créez l'IPAM, vous créez automatiquement le rôle lié au AWSServiceRoleForIPAM service.
- L'utilisateur associé au compte de gestion des AWS Organizations doit utiliser un rôle IAM auquel sont associées les actions de politique IAM suivantes :
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`
  - `iam:CreateServiceLinkedRole`

  Pour en savoir plus sur la création de rôles IAM, consultez la section Création d'un rôle pour la délégation d'autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM.
- L'utilisateur associé au compte de gestion des AWS Organizations peut utiliser un rôle IAM auquel sont associées les actions de politique IAM suivantes pour répertorier vos administrateurs délégués AWS Orgs actuels : `organizations:ListDelegatedAdministrators`

AWS Management Console

Sélection d'un compte IPAM

1. À l'aide du compte de gestion AWS Organizations, ouvrez la console IPAM à l'adresse https://console.aws.amazon.com/ipam/.
2. Dans la console AWS de gestion, choisissez la AWS région dans laquelle vous souhaitez travailler avec IPAM.

3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation).
4. L'option Delegate n'est disponible que si vous vous êtes connecté à la console en tant que compte de gestion des AWS Organizations. Choisisssez Delegate (Déléguer).
5. Entrez l'identifiant d'un AWS compte IPAM. L'administrateur IPAM doit être membre d'un compte AWS Organizations.
6. Sélectionnez Enregistrer les modifications.

Command line

Les commandes de cette section renvoient à la documentation de référence de la AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Pour déléguer un compte administrateur IPAM à l'aide de AWS CLI, utilisez la commande suivante : -account enable-ipam-organization-admin

Lorsque vous déléguez un compte membre Organizations comme compte IPAM, IPAM crée automatiquement un rôle IAM lié au service dans tous les comptes membres de votre organisation. IPAM contrôle l'utilisation des adresses IP dans ces comptes en assumant le rôle IAM lié au service dans chaque compte membre, en découvrant les ressources et leurs CIDR et en les intégrant à IPAM. Les ressources de tous les comptes membres pourront être découvertes par IPAM, quelle que soit leur unité organisationnelle. Si des comptes membres ont créé un VPC, par exemple, vous verrez le VPC et son CIDR dans la section Ressources de la console IPAM.

> **Important**
>
> Le rôle du compte de AWS Organizations gestion qui a délégué l'administrateur IPAM est désormais complet. Pour poursuivre l'utilisation d'IPAM, le compte administrateur IPAM doit se connecter à Amazon VPC IPAM et créer un IPAM.

Intégration d'IPAM à des comptes extérieurs à votre organisation

Cette section explique comment intégrer votre IPAM à des comptes AWS extérieurs à votre organisation. Afin d'exécuter la procédure indiquée dans cette section, vous devez avoir déjà effectué

les étapes décrites dans la section Intégrer l'IPAM aux comptes d'une organisation AWS et délégué un compte IPAM.

L'intégration d'IPAM à des comptes AWS extérieurs à votre organisation vous permet d'effectuer les opérations suivantes :

- Gérer les adresses IP extérieures à votre organisation à partir d'un seul compte IPAM.
- Partager des groupes IPAM avec des services tiers hébergés par d'autres comptes AWS sur d'autres AWS Organizations.

Après avoir intégré IPAM à des comptes AWS extérieurs à votre organisation, vous pouvez partager un groupe IPAM directement avec les comptes souhaités d'autres organisations.

Table des matières

- Considérations et restrictions
- Présentation du processus

Considérations et restrictions

Cette section contient des considérations et des limites relatives à l'intégration d'IPAM à des comptes extérieurs à votre organisation :

- Lorsque vous partagez une découverte de ressources avec un autre compte, les seules données échangées sont l'adresse IP et les données de surveillance de statut de compte. Vous pouvez consulter ces données avant de les partager à l'aide des commandes CLI get-ipam-discovered-resource-cidrs et get-ipam-discovered-accounts, ou des API GetIpamDiscoveredResourceCidrs et GetIpamDiscoveredAccounts. Pour les découvertes de ressources qui surveillent les ressources d'une organisation, aucune donnée d'organisation (telle que les noms des unités organisationnelles de votre organisation) n'est partagée.
- Lorsque vous créez une découverte de ressources, celle-ci surveille toutes les ressources visibles dans le compte propriétaire. Si le compte propriétaire est un compte de service AWS tiers qui crée des ressources pour plusieurs de ses propres clients, ces ressources seront découvertes lors de la découverte de ressources. Si le compte de service AWS tiers partage la découverte de ressources avec un compte AWS d'utilisateur final, l'utilisateur final aura une visibilité sur les ressources des autres clients du service AWS tiers. Ainsi, le service AWS tiers doit faire preuve de prudence lors de la création et du partage des découvertes de ressources, ou utiliser un compte AWS distinct pour chaque client.

Présentation du processus

Cette section explique comment intégrer votre IPAM à des comptes AWS extérieurs à votre organisation. Dans cette section, plusieurs références à des sujets abordés dans d'autres sections de ce guide sont présentes. Afin de conserver cette page et les instructions qu'elle contient visibles, cliquez sur les liens ci-dessous dirigeant vers d'autres sections de manière à les ouvrir dans une nouvelle fenêtre.

Lorsque vous intégrez IPAM à des comptes AWS extérieurs à votre organisation, quatre comptes AWS sont impliqués dans le processus :

- Propriétaire de l'organisation principale : compte de gestion AWS Organizations de l'organisation 1.
- Compte IPAM de l'organisation principale : compte administrateur délégué IPAM de l'organisation 1.
- Propriétaire de l'organisation secondaire : compte de gestion AWS Organizations de l'organisation 2.
- Compte administrateur de l'organisation secondaire : compte administrateur délégué IPAM de l'organisation 2.

Étapes

1. Le propriétaire de l'organisation principale délègue un membre de son organisation en tant que compte IPAM de l'organisation principale (voir la section Intégrer l'IPAM aux comptes d'une organisation AWS) (français non garanti).
2. Le compte IPAM de l'organisation principale crée un IPAM (voir la section Création d'un IPAM) (français non garanti).
3. Le propriétaire de l'organisation secondaire délègue un membre de son organisation comme compte administrateur de l'organisation secondaire (voir la section Intégrer l'IPAM aux comptes d'une organisation AWS).
4. Le compte administrateur de l'organisation secondaire crée une découverte de ressources et la partage avec le compte IPAM de l'organisation principale à l'aide d'AWS RAM (voir les sections Créer une découverte de ressources et Partage d'une découverte de ressources) (français non garanti). La découverte de ressources doit être créée dans la même région d'origine que l'IPAM de l'organisation principale.

5. Le compte IPAM de l'organisation principale accepte l'invitation de partage de ressources à l'aide d'AWS RAM (voir la section Acceptation et rejet des invitations de partage de ressources du Guide de l'utilisateur AWS RAM) (français non garanti).
6. Le compte IPAM de l'organisation principale associe la découverte de ressources à son IPAM (voir la section Associer une découverte de ressources à un IPAM) (français non garanti).
7. Le compte IPAM de l'organisation principale peut désormais surveiller et/ou gérer les ressources IPAM créées par les comptes de l'organisation secondaire.
8. (Facultatif) Le compte IPAM de l'organisation principale partage des groupes IPAM avec les comptes membres de l'organisation secondaire (voir la section Partage d'un groupe IPAM à l'aide d'AWS RAM) (français non garanti).
9. (Facultatif) Si le compte IPAM de l'organisation principale souhaite arrêter la découverte de ressources dans l'organisation secondaire, il peut la dissocier de l'IPAM (voir la section Dissocier une découverte de ressources) (français non garanti).
10. (Facultatif) Si le compte administrateur de l'organisation secondaire souhaite ne plus participer à l'IPAM de l'organisation principale, il peut annuler le partage de découverte de ressources (voir la section Mettre à jour un partage de ressources dans AWS RAM du Guide de l'utilisateur AWS RAM) ou supprimer la découverte de ressources (voir la section Supprimer une découverte de ressources) (français non garanti).

Utilisation d'IPAM avec un seul compte

Si vous choisissez de ne pas Intégrer l'IPAM aux comptes d'une organisation AWS, vous pouvez utiliser IPAM avec un seul compte AWS.

Lorsque vous créez un IPAM dans la section suivante, un rôle lié à un service est automatiquement créé pour le service IPAM Amazon VPC dans AWS Identity and Access Management. IPAM utilise le rôle lié au service pour surveiller et stocker les métriques des CIDR associés aux ressources réseau EC2. Pour plus d'informations sur le rôle lié à un service et la façon dont IPAM l'utilise, consultez Rôles liés à un service pour IPAM.

> **Important**
>
> Si vous utilisez IPAM avec un seul compte AWS, vous devez vous assurer que le compte AWS que vous utilisez pour créer l'IPAM utilise un rôle IAM avec une politique qui lui est associée et qui autorise l'action `iam:CreateServiceLinkedRole`. Lorsque vous créez l'IPAM, vous créez automatiquement le rôle lié au service AWSServiceRoleForIPAM.

Pour plus d'informations sur la gestion des politiques IAM, consultez Modification des politiques IAM dans le Guide de l'utilisateur IAM.

Une fois que le compte unique AWS est autorisé à créer le rôle lié au service IPAM, accédez à Création d'un IPAM.

Création d'un IPAM

Suivez les étapes de cette section pour créer votre IPAM. Si vous avez délégué un administrateur IPAM, ces étapes doivent être réalisées par le compte IPAM.

Important

Lorsque vous créez un IPAM, il vous est demandé d'autoriser IPAM à répliquer les données des comptes source vers un compte IPAM délégué. Pour intégrer IPAM à AWS Organizations, IPAM a besoin de votre autorisation pour répliquer les détails d'utilisation des ressources et des adresses IP entre les comptes (des comptes membres au compte membre IPAM délégué) et entre les Régions AWS (des Régions d'exploitation à la Région d'origine de votre IPAM). Pour les utilisateurs IPAM à compte unique, IPAM a besoin de votre autorisation pour répliquer les détails d'utilisation des ressources et des adresses IP dans les Régions d'exploitation vers la Région d'origine de votre IPAM.

Lorsque vous créez l'IPAM, vous choisissez les Régions AWS où l'IPAM est autorisé à gérer les CIDR d'adresses IP. Ces Régions AWS sont appelées Régions d'exploitation. IPAM ne détecte et ne contrôle les ressources que dans les Régions AWS que vous sélectionnez comme Régions d'exploitation. IPAM ne stocke aucune donnée en dehors des Régions d'exploitation que vous sélectionnez.

L'exemple de hiérarchie suivant illustre comment les Régions AWS que vous attribuez lorsque vous créez l'IPAM auront un impact sur les Régions qui seront disponibles pour les groupes que vous créez ultérieurement.

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée privée
    - Groupe IPAM de niveau supérieur
      - Groupe régional IPAM dans la Région AWS 2

- Groupe de développement
  - Allocation pour un VPC dans la Région AWS 2

Vous ne pouvez créer qu'un seul IPAM. Pour plus d'informations sur l'augmentation des quotas liés à IPAM, consultez Quotas pour votre IPAM.

AWS Management Console

Création d'un IPAM

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans la Console de gestion AWS, sélectionnez la Région AWS dans laquelle vous souhaitez créer l'IPAM. Créez IPAM dans votre Région d'opérations principale.
3. Sur la page d'accueil, sélectionnez Create IPAM (Créer un IPAM).
4. Sélectionnez Allow Amazon VPC IP Address Manager to replicate data from source account(s) into an IPAM Delegate account (Autoriser Amazon VPC IP Address Manager à répliquer les données du ou des comptes source dans le compte IPAM délégué). Si vous ne sélectionnez pas cette option, vous ne pouvez pas créer d'IPAM.
5. Choisissez un niveau IPAM. Pour plus d'informations sur les fonctionnalités disponibles dans chaque niveau et les coûts associés aux niveaux, consultez l'onglet IPAM sur la page de tarification d'Amazon VPC.
6. Sous Operating regions (Régions d'exploitation), sélectionnez les Régions AWS dans lesquelles cet IPAM peut gérer et découvrir des ressources. La Région AWS dans laquelle vous créez votre IPAM est sélectionnée par défaut comme l'une des Régions d'exploitation. Par exemple, si vous créez cet IPAM dans la Région AWS `us-east-1`, mais vous souhaitez créer ultérieurement des groupes IPAM régionaux qui fournissent des CIDR aux VPC dans `us-west-2`, sélectionnez `us-west-2` ici. Si vous oubliez une Région d'exploitation, vous pouvez revenir ultérieurement et modifier vos paramètres IPAM.

> **Note**
>
> Si vous créez un IPAM dans le cadre de l'offre gratuite, vous pouvez sélectionner plusieurs régions d'exploitation pour votre IPAM, mais la seule fonctionnalité IPAM qui sera disponible dans toutes les régions d'exploitation est Public IP Insights. Vous ne pouvez pas utiliser d'autres fonctionnalités dans le cadre de l'offre gratuite, comme BYOIP, dans les régions d'exploitation de l'IPAM. Vous ne pouvez les utiliser que

dans la Région d'accueil de l'IPAM. Pour utiliser toutes les fonctionnalités IPAM dans toutes les régions d'exploitation, créez un IPAM dans le niveau avancé.

7. Sélectionnez Create IPAM (Créer un IPAM).

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour créer, modifier et afficher les détails liés à votre IPAM :

1. Créez l'IPAM : create-ipam
2. Affichez l'IPAM que vous avez créé : describe-ipams
3. Affichez les portées créées automatiquement : describe-ipam-scopes
4. Modifiez un IPAM existant : modify-ipam

Lorsque vous avez terminé ces étapes, IPAM a effectué les opérations suivantes :

- La création de votre IPAM. Vous pouvez voir l'IPAM et les Régions d'exploitation actuellement sélectionnées en sélectionnant IPAM dans le panneau de navigation gauche de la console.
- La création d'une portée privée et d'une portée publique. Vous pouvez consulter les portées en sélectionnant Scopes (Portées) dans le panneau de navigation. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.

Planification de l'approvisionnement des adresses IP

Suivez les étapes de cette section pour planifier l'approvisionnement des adresses IP à l'aide de groupes IPAM. Si vous avez configuré un compte IPAM, ces étapes doivent être effectuées par ce compte. Le processus de création de pool est différent pour les pools situés dans des zones publiques et privées. Cette section décrit les étapes de création d'un pool régional dans le cadre privé. Pour les didacticiels BYOIP et BYOASN, voir. Didacticiels

> **Important**
>
> Pour utiliser des pools IPAM sur plusieurs AWS comptes, vous devez intégrer IPAM à AWS Organizations, sinon certaines fonctionnalités risquent de ne pas fonctionner correctement. Pour plus d'informations, consultez Intégrer l'IPAM aux comptes d'une organisation AWS.

Dans IPAM, un groupe est un ensemble de plages d'adresses IP contiguës (ou CIDR). Les groupes vous permettent d'organiser vos adresses IP en fonction de vos besoins de routage et de sécurité. Vous pouvez créer des pools pour les AWS régions situées en dehors de votre région IPAM. Par exemple, si vous avez des besoins de routage et de sécurité distincts pour les applications de développement et de production, vous pouvez créer un groupe pour chacune d'elles.

Dans la première étape de cette section, vous allez créer un groupe de niveau supérieur. Vous créerez ensuite un groupe régional dans le groupe de niveau supérieur. Dans le groupe régional, vous pouvez créer des groupes supplémentaires au besoin, tels que les groupes d'environnement de production et de développement. Par défaut, vous pouvez créer des groupes jusqu'à une profondeur de 10. Pour plus d'informations sur les quotas IPAM, consultez Quotas pour votre IPAM.

> **Note**
>
> Les termes approvisionnement/provisionner et allocation/allouer sont utilisés dans ce guide de l'utilisateur et dans la console IPAM. Approvisionnement/provisionner sont des termes utilisés lorsque vous ajoutez un CIDR à un groupe IPAM. Allocation/allouer sont des termes utilisés lorsque vous associez un CIDR d'un groupe IPAM à une ressource.

L'exemple suivant illustre la hiérarchie de la structure de groupes que vous allez créer en complétant les étapes de cette section :

- IPAM opérant dans les AWS régions 1 et AWS 2
  - Portée privée
    - Groupe de niveau supérieur
      - Piscine régionale dans AWS la Région 1
        - Groupe de développement
          - Allocation pour un VPC

Cette structure sert d'exemple de la manière dont vous pouvez utiliser IPAM, mais vous pouvez utiliser IPAM afin de répondre aux besoins de votre organisation. Pour plus d'informations sur les bonnes pratiques, consultez Amazon VPC IP Address Manager Best Practices (Bonnes pratiques du gestionnaire d'adresses IP Amazon VPC).

Si vous créez un groupe IPAM unique, complétez les étapes décrites dans Création d'un groupe IPv4 de niveau supérieur, puis passez à Allocation de CIDR.

Table des matières

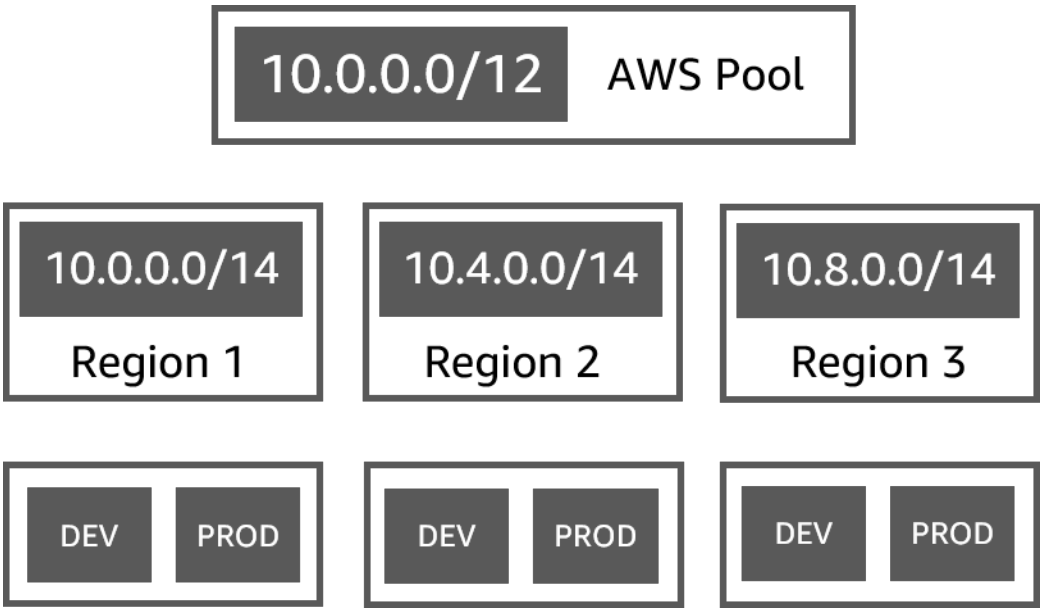
- Exemples de plans de groupes IPAM
- Création de groupes IPv4
- Création de groupes IPv6

Exemples de plans de groupes IPAM

Vous pouvez utiliser IPAM pour répondre aux besoins de votre organisation. Cette section fournit des exemples sur la façon d'organiser vos adresses IP.

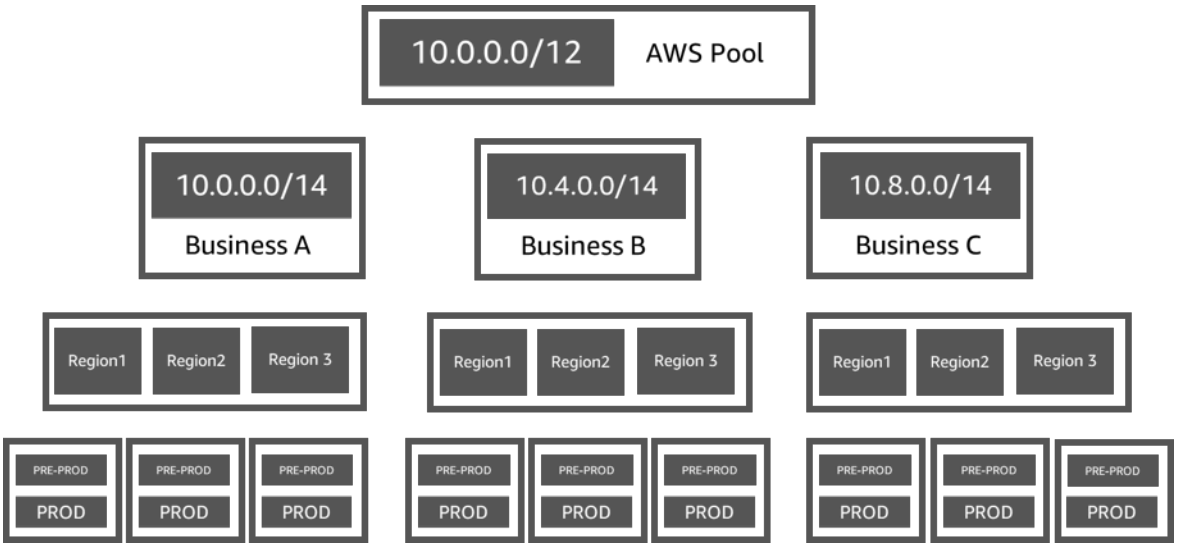
Groupes IPv4 dans plusieurs régions AWS

L'exemple suivant représente une hiérarchie de groupes IPAM pour plusieurs Régions AWS au sein d'un groupe de niveau supérieur. Chaque groupe régional AWS comprend deux groupes de développement IPAM, un groupe pour les ressources de développement et un groupe pour les ressources de production.



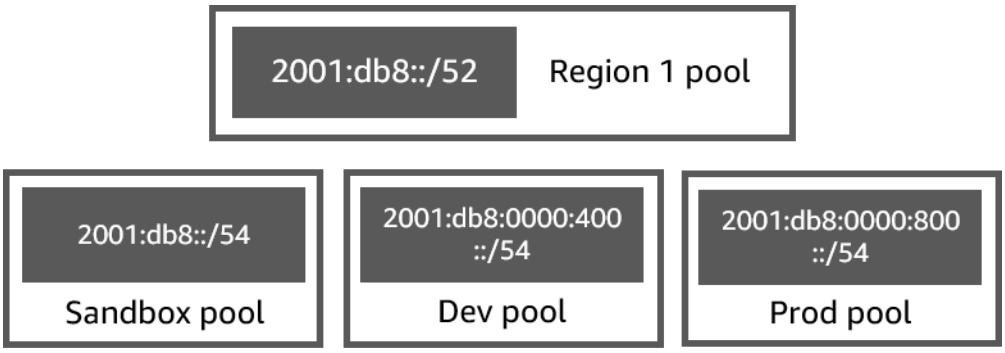
Groupes IPv4 pour plusieurs secteurs d'activité

L'exemple suivant représente une hiérarchie de groupes IPAM pour plusieurs secteurs d'activité au sein d'un groupe de niveau supérieur. Chaque groupe de chaque secteur d'activité contient trois groupes régionaux AWS. Chaque groupe régional comprend deux groupes de développement IPAM, un groupe pour les ressources de préproduction et un groupe pour les ressources de production.



Groupes IPv6 dans une région AWS

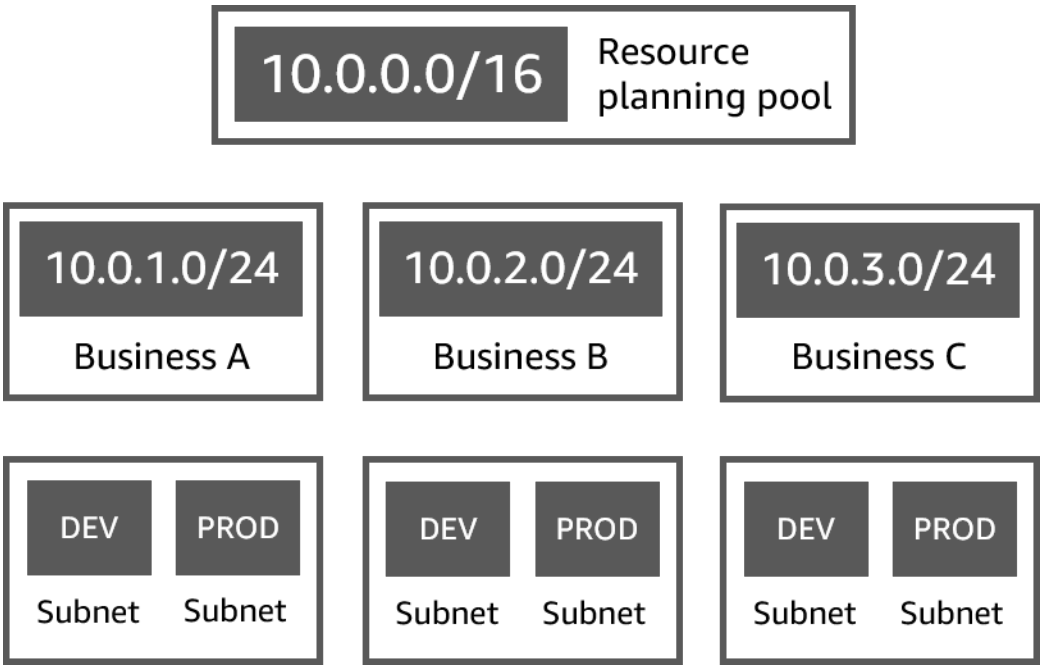
L'exemple suivant montre une hiérarchie de groupes IPAM IPv6 pour plusieurs secteurs d'activité au sein d'un groupe régional. Chaque groupe régional contient trois groupes IPAM : un pour les ressources d'environnement de test (sandbox), un pour les ressources de développement et un pour les ressources de production.



Groupes de sous-réseau pour plusieurs secteurs d'activité

L'exemple suivant représente une hiérarchie de groupes de planification des ressources pour plusieurs secteurs d'activité et des groupes de sous-réseaux de développement/production. Pour

plus d'informations sur la planification de l'espace des adresses IP des sous-réseaux à l'aide d'IPAM, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.



Création de groupes IPv4

Suivez les étapes de cette section pour créer une hiérarchie de groupes IPAM IPv4.

L'exemple suivant illustre la hiérarchie de la structure de groupe que vous pouvez créer à l'aide des instructions fournies dans ce guide. Dans cette section, vous créez une hiérarchie de groupes IPAM IPv4 :

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée privée
    - Groupe de niveau supérieur (10.0.0.0/8)
      - Groupe régional dans la Région AWS 2 (10.0.0.0/16)
        - Groupe de développement (10.0.0.0/24)
          - Allocation pour un VPC (10.0.0.0/25)

Dans l'exemple précédent, les CIDR utilisés ne sont que des exemples. Chaque groupe du groupe de niveau supérieur y est provisionné avec une partie du CIDR de niveau supérieur.

Table des matières

- Création d'un groupe IPv4 de niveau supérieur
- Création d'un groupe IPv4 régional
- Création d'un groupe IPv4 de développement

Création d'un groupe IPv4 de niveau supérieur

Suivez les étapes de cette section pour créer un groupe IPAM de niveau supérieur IPv4. Lorsque vous créez le groupe, vous provisionnez un CIDR pour que le groupe puisse l'utiliser. Vous attribuez ensuite cet espace à une allocation. Une allocation est une attribution CIDR d'un groupe IPAM à un autre groupe IPAM ou à une ressource.

L'exemple suivant illustre la hiérarchie de la structure de groupe que vous pouvez créer à l'aide des instructions fournies dans ce guide. À cette étape, vous créez le groupe IPAM de niveau supérieur :

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée privée
    - Groupe de niveau supérieur (10.0.0.0/8)
      - Groupe régional dans Région 1 AWS (10.0.0.0/16)
        - Groupe de développement pour VPC autres que de production (10.0.0.0/24)
          - Allocation pour un VPC (10.0.0.0/25)

Dans l'exemple précédent, les CIDR utilisés ne sont que des exemples. Chaque groupe du groupe de niveau supérieur y est provisionné avec une partie du CIDR de niveau supérieur.

Lorsque vous créez un groupe IPAM, vous pouvez configurer des règles pour les allocations effectuées dans le groupe IPAM.

Les règles d'allocation vous permettent d'effectuer les configurations suivantes :

- Indique si IPAM doit importer automatiquement des CIDR dans le groupe IPAM s'il les trouve dans la plage CIDR dudit groupe
- La longueur de masque réseau requise pour les allocations au sein du groupe
- Les étiquettes requises pour les ressources du groupe
- Les paramètres régionaux requis pour les ressources du groupe. Les paramètres régionaux sont la Région AWS où un groupe IPAM est disponible pour les allocations.

Les règles d'allocation déterminent si les ressources sont conformes ou non. Pour plus d'informations sur la conformité, consultez Contrôle de l'utilisation du CIDR par ressource.

> **Important**
>
> Il existe une règle implicite supplémentaire qui n'est pas affichée dans les règles d'allocation. Si la ressource se trouve dans un groupe IPAM qui est une ressource partagée dans AWS Resource Access Manager (RAM), le propriétaire de la ressource doit être configuré comme principal dans AWS RAM. Pour plus d'informations sur le partage de groupes avec RAM, consultezPartage d'un groupe IPAM à l'aide d'AWS RAM.

L'exemple suivant montre comment vous pouvez utiliser des règles d'allocation pour contrôler l'accès à un groupe IPAM :

Example

Lorsque vous créez vos groupes selon les besoins de routage et de sécurité, vous pouvez autoriser uniquement certaines ressources à utiliser un groupe. Dans ce cas, vous pouvez définir une règle d'allocation indiquant que toute ressource souhaitant un CIDR de ce groupe doit posséder une étiquette correspondant aux exigences liées aux étiquettes de règles d'allocation. Par exemple, vous pouvez définir une règle d'allocation indiquant que seuls les VPC possédant l'étiquette prod peuvent recevoir des CIDR d'un groupe IPAM. Vous pouvez également définir une règle indiquant que les CIDR alloués à partir de ce groupe ne peuvent pas excéder /24. Dans ce cas, une ressource peut toujours être créée à l'aide d'un CIDR supérieur à /24 à partir de ce groupe si l'espace est disponible, mais comme cela enfreint une règle d'allocation concernant le groupe, IPAM signale cette ressource comme non conforme.

> **Important**
>
> Cette section explique comment créer un groupe IPv4 de niveau supérieur avec une plage d'adresses IP fournie par AWS. Si vous souhaitez fournir votre propre plage d'adresses IPv4 à AWS (BYOIP), certaines conditions sont requises. Pour de plus amples informations, veuillez consulter Didacticiel : apporter vos adresses IP à IPAM.

AWS Management Console

Création d'un groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Sélectionnez Create pool (Créer un groupe).
4. Sous Portée IPAM, sélectionnez la portée privée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.

   Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Les groupes de la portée privée doivent être des groupes IPv4. Les groupes de la portée publique peuvent être des groupes IPv4 ou IPv6. La portée publique est destinée à tous les espaces publics.
5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une description du groupe.
6. Sous Source, choisissez Portée IPAM.
7. SousAddress family (Famille d'adresses), choisissezIPv4.
8. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
9. Pour Locale (Paramètres régionaux), sélectionnez None (Aucun). Vous définirez les paramètres régionaux sur le groupe régional.

   Les paramètres régionaux constituent la Région AWS dans laquelle vous souhaitez que ce groupe IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP.
10. (Facultatif) Vous pouvez créer un groupe sans CIDR, mais vous ne pourrez pas l'utiliser pour les allocations tant que vous n'aurez pas provisionné de CIDR pour celui-ci. Afin de provisionner un CIDR, sélectionnez Ajouter un nouveau CIDR. Saisissez un CIDR IPv4 à provisionner pour le groupe. Si vous souhaitez fournir votre propre plage d'adresses IP

IPv4 ou IPv6 à AWS, certaines conditions sont requises. Pour de plus amples informations, veuillez consulter Didacticiel : apporter vos adresses IP à IPAM.

11. Sélectionnez des règles d'allocation en option pour ce groupe :

- Importer automatiquement les ressources découvertes : cette option n'est pas disponible si la valeur Locale (Paramètre régional) est définie sur None (Aucun). Si cette option est sélectionnée, IPAM recherchera en permanence les ressources dans la plage CIDR de ce groupe et les importera automatiquement sous forme d'allocations dans votre IPAM. Notez ce qui suit :
  - Les CIDR qui seront alloués à ces ressources ne doivent pas déjà être alloués à d'autres ressources pour que l'importation réussisse.
  - IPAM importera un CIDR indépendamment de sa conformité avec les règles d'allocation du groupe, de sorte qu'une ressource puisse être importée puis marquée comme non conforme.
  - Si IPAM découvre plusieurs CIDR qui se chevauchent, IPAM n'importera que le plus grand CIDR.
  - Si IPAM découvre plusieurs CIDR avec des CIDR correspondants, IPAM n'importera qu'un seul d'entre eux de manière aléatoire.

  ⚠ Warning
  - Après avoir créé un IPAM, lorsque vous créez un VPC, choisissez l'option de bloc d'adresse CIDR alloué à l'IPAM. Dans le cas contraire, l'adresse CIDR que vous choisissez pour votre VPC risque de se chevaucher avec une allocation d'adresse CIDR IPAM.
  - Si un VPC est déjà alloué dans un groupe IPAM, un VPC dont le CIDR se chevauche ne peut pas être importé automatiquement. Par exemple, si vous avez un VPC avec une adresse CIDR 10.0.0.0/26 allouée dans un groupe IPAM, un VPC avec une adresse CIDR 10.0.0.0/23 (qui couvrirait l'adresse CIDR 10.0.0.0/26) ne peut pas être importé.
  - L'importation automatique dans IPAM des allocations d'adresse CIDR de VPC existantes prend un certain temps.
- Longueur minimale du masque réseau : la longueur minimale du masque réseau requise pour que les allocations CIDR dans ce groupe IPAM soient conformes et le bloc d'adresse CIDR de la plus grande taille pouvant être alloué à partir du groupe. La longueur minimale

du masque réseau doit être inférieure à la longueur maximale du masque réseau. Les longueurs possibles du masque réseau pour les adresses IPv4 sont comprises entre 0 et 32. Les longueurs possibles du masque réseau pour les adresses IPv6 sont comprises entre 0 et 128.

- Longueur du masque réseau par défaut : longueur de masque réseau par défaut pour les allocations ajoutées à ce groupe. Par exemple, si le CIDR provisionné à ce groupe est **10.0.0.0/8** et que vous saisissez **16** ici, toutes les nouvelles allocations de ce groupe auront par défaut une longueur de masque réseau de /16.
- Longueur maximale du masque réseau : longueur maximale du masque réseau requise pour les allocations CIDR dans ce groupe. Cette valeur dicte le bloc d'adresse CIDR de la plus petite taille pouvant être alloué à partir du groupe.
- Exigences d'étiquette : étiquettes requises pour que les ressources allouent de l'espace à partir du groupe. Si les étiquettes des ressources ont été modifiées après l'allocation de l'espace ou si les règles d'étiquette des allocations sont modifiées sur le groupe, la ressource peut être marquée comme non conforme.
- Paramètres régionaux : paramètres régionaux requis pour les ressources qui utilisent des CIDR de ce groupe. Les ressources importées automatiquement qui ne possèdent pas ces paramètres régionaux seront marquées non conformes. Les ressources qui ne sont pas automatiquement importées dans le groupe ne seront pas autorisées à allouer de l'espace à partir du groupe à moins qu'elles ne se trouvent dans ces paramètres régionaux.

12. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
13. Sélectionnez Create pool (Créer un groupe).
14. Consultez Création d'un groupe IPv4 régional.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour créer ou modifier un groupe de niveau supérieur dans votre IPAM :

1. Créez un groupe : create-ipam-pool.
2. Modifiez le groupe après l'avoir créé pour modifier les règles d'allocation : modify-ipam-pool.

Création d'un groupe IPv4 régional

Suivez les étapes de cette section pour créer un groupe régional dans votre groupe de niveau supérieur. Si vous n'avez besoin que d'un groupe de premier niveau et que vous n'avez pas besoin de groupes régionaux et de développement supplémentaires, passez à Allocation de CIDR.

> **Note**
>
> Le processus de création de pool est différent pour les pools situés dans des zones publiques et privées. Cette section décrit les étapes à suivre pour créer un pool régional dans le cadre privé. Pour les didacticiels BYOIP et BYOASN, consultez. Didacticiels

L'exemple suivant illustre la hiérarchie de la structure de groupe que vous créez en suivant les instructions de ce guide. À cette étape, vous créez le groupe IPAM régional :

- IPAM opérant dans les AWS régions 1 et AWS 2
  - Portée privée
    - Groupe de niveau supérieur (10.0.0.0/8)
      - Piscine régionale dans AWS la région 1 (10.0.0.0/16)
        - Groupe de développement pour VPC autres que de production (10.0.0.0/24)
          - Allocation pour un VPC (10.0.0.0/25)

Dans l'exemple précédent, les CIDR utilisés ne sont que des exemples. Chaque groupe du groupe de niveau supérieur y est provisionné avec une partie du CIDR de niveau supérieur.

AWS Management Console

Création d'un groupe dans un groupe de niveau supérieur

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Sélectionnez Create pool (Créer un groupe).
4. Sous Portée IPAM, sélectionnez la portée que vous avez utilisée lors de la création du groupe de niveau supérieur. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.

5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une description du groupe.
6. Sous Source, choisissez Groupe IPAM. Puis sélectionnez le groupe de niveau supérieur créé dans la section précédente.
7. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
8. Choisissez les paramètres régionaux du groupe. La sélection d'un paramètre régional garantit qu'il n'y a aucune dépendance régionale entre votre groupe et les ressources qui y sont allouées. Les options disponibles proviennent des Régions d'exploitation que vous avez sélectionnées lors de la création de votre IPAM.

   Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP.

   > **Note**
   >
   > Si vous créez un groupe dans l'offre gratuite, vous ne pouvez choisir que les paramètres régionaux correspondant à la région d'accueil de votre IPAM. Pour utiliser toutes les fonctionnalités IPAM dans tous les paramètres régionaux, passez au niveau avancé.

9. (En option) Sélectionnez un CIDR à provisionner pour le groupe. Vous pouvez créer un groupe sans CIDR, mais vous ne pourrez pas utiliser le groupe pour les allocations tant que vous n'aurez pas provisionné un CIDR pour celui-ci. Vous pouvez ajouter des CIDR à un groupe à tout moment en modifiant le groupe.
10. Vous disposez ici des mêmes options de règle d'allocation que lorsque vous avez créé le groupe de premier niveau. Consultez Création d'un groupe IPv4 de niveau supérieur pour obtenir une explication des options disponibles lorsque vous créez des groupes. Les règles

d'allocation du groupe régional ne sont pas héritées du groupe de niveau supérieur. Si vous n'appliquez aucune règle ici, aucune règle d'allocation ne sera définie pour le groupe.

11. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
12. Lorsque vous avez fini de configurer votre groupe, choisissez Create pool (Créer un groupe).
13. veuillez consulter Création d'un groupe IPv4 de développement.

Command line

Les commandes de cette section renvoient à la documentation de référence de la AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les AWS CLI commandes suivantes pour créer un pool régional dans votre IPAM :

1. Obtenez l'ID de l'étendue dans laquelle vous souhaitez créer le pool : describe-ipam-scopes
2. Obtenez l'ID du pool dans lequel vous souhaitez créer le pool : describe-ipam-pools
3. Créez le pool : create-ipam-pool
4. Découvrez le nouveau pool : describe-ipam-pools

Répétez ces étapes pour créer des groupes supplémentaires dans le groupe de niveau supérieur, le cas échéant.

Création d'un groupe IPv4 de développement

Suivez les étapes de cette section pour créer un groupe de développement au sein de votre groupe régional. Si vous n'avez besoin que d'un groupe régional et de niveau supérieur, et que vous n'avez pas besoin de groupes de développement, passez à Allocation de CIDR.

L'exemple suivant illustre la hiérarchie de la structure de groupe que vous pouvez créer à l'aide des instructions de ce guide. À cette étape, vous créez un groupe IPAM de développement :

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée privée
    - Groupe de niveau supérieur (10.0.0.0/8)
      - Groupe régional dans Région 1 AWS (10.0.0.0/16)
        - Groupe de développement pour VPC autres que de production (10.0.0.0/24)

- Allocation pour un VPC (10.0.1.0/25)

Dans l'exemple précédent, les CIDR utilisés ne sont que des exemples. Chaque groupe du groupe de niveau supérieur y est provisionné avec une partie du CIDR de niveau supérieur.

AWS Management Console

Pour créer un groupe de développement au sein d'un groupe régional

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Sélectionnez Create pool (Créer un groupe).
4. Sous Portée IPAM, sélectionnez la portée que vous avez utilisée lors de la création des groupes de niveau supérieur et régionaux. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une description du groupe.
6. Sous Source, choisissez Groupe IPAM. Sélectionnez groupe régional.
7. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
8. (Facultatif) Choisissez un CIDR à provisionner pour le groupe. Vous pouvez uniquement provisionner un CIDR qui a été provisionné au groupe de niveau supérieur. Vous pouvez créer un groupe sans CIDR, mais vous ne pourrez pas utiliser le groupe pour les allocations tant que vous n'aurez pas provisionné un CIDR pour celui-ci. Vous pouvez ajouter des CIDR à un groupe à tout moment en modifiant le groupe.
9. Vous disposez ici des mêmes options de règle d'allocation que lorsque vous avez créé le groupe régional et le groupe de niveau supérieur. Consultez Création d'un groupe IPv4 de niveau supérieur pour obtenir une explication des options disponibles lorsque vous créez des groupes. Les règles d'allocation du groupe ne sont pas héritées du groupe situé au-dessus de lui dans la hiérarchie. Si vous n'appliquez aucune règle ici, aucune règle d'allocation ne sera définie pour le groupe.
10. (Facultatif) Choisissez Tags (Étiquettes) pour le groupe.
11. Lorsque vous avez fini de configurer votre groupe, choisissez Create pool (Créer un groupe).

12. Consultez Allocation de CIDR.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour créer un groupe régional dans votre IPAM :

1. Obtenez l'ID de la portée dans laquelle vous voulez créer le groupe : describe-ipam-scopes
2. Obtenez l'ID du groupe dans lequel vous voulez créer le groupe : describe-ipam-pools
3. Créez le groupe : create-ipam-pool
4. Affichez le nouveau groupe : describe-ipam-pools

Répétez ces étapes pour créer des groupes de développement supplémentaires au sein du groupe régional, le cas échéant.

Création de groupes IPv6

Suivez les étapes de cette section pour créer une hiérarchie de groupes IPAM IPv6. Lorsque vous créez le groupe, vous pouvez provisionner un CIDR à utiliser par celui-ci. Le groupe attribue de l'espace dans ce CIDR aux allocations au sein du groupe. Une allocation est une affectation CIDR d'un groupe IPAM vers un autre groupe de ressources ou IPAM.

L'exemple suivant illustre la hiérarchie de la structure de groupe que vous pouvez créer à l'aide des instructions fournies dans ce guide. Dans cette section, vous créez une hiérarchie de groupes IPAM IPv6 :

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée publique
    - Groupe régional dans région AWS 1 (2001:db8::/52)
      - Groupe de développement (2001:db8::/54)
        - Allocation pour un VPC (2001:db8::/56)

Table des matières

- Création d'un groupe IPv6 régional

- Création d'un groupe IPv6 de développement

Création d'un groupe IPv6 régional

Suivez les étapes de cette section pour créer un groupe IPAM régional IPv6. Lorsque vous provisionnez un bloc CIDR IPv6 fourni par Amazon à un groupe, il doit être provisionné dans un groupe avec des paramètres régionaux (région AWS) sélectionnés. Lorsque vous créez le groupe, vous pouvez provisionner un CIDR pour que le groupe l'utilise ou l'ajoute ultérieurement. Vous attribuez ensuite cet espace à une allocation. Une allocation est une attribution CIDR d'un groupe IPAM à un autre groupe IPAM ou à une ressource.

L'exemple suivant illustre la hiérarchie de la structure de groupe que vous pouvez créer à l'aide des instructions fournies dans ce guide. À cette étape, vous créez le groupe IPAM régional IPv6 :

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée publique
    - Groupe régional dans région AWS 1 (2001:db8::/52)
      - Groupe de développement (2001:db8::/54)
        - Allocation pour un VPC (2001:db8::/56)

Dans l'exemple précédent, les CIDR utilisés ne sont que des exemples. Cela permet d'illustrer que chaque groupe au sein du groupe régional IPv6 est provisionné avec une partie du CIDR régional IPv6.

Lorsque vous créez un groupe IPAM, vous pouvez configurer des règles pour les allocations effectuées dans le groupe IPAM.

Les règles d'allocation vous permettent d'effectuer les configurations suivantes :

- La longueur de masque réseau requise pour les allocations au sein du groupe
- Les étiquettes requises pour les ressources du groupe
- Les paramètres régionaux requis pour les ressources du groupe. Les paramètres régionaux sont la Région AWS où un groupe IPAM est disponible pour les allocations.

Les règles d'allocation déterminent si les ressources sont conformes ou non. Pour plus d'informations sur la conformité, consultez Contrôle de l'utilisation du CIDR par ressource.

> **Important**
>
> Il existe une règle implicite supplémentaire qui n'est pas affichée dans les règles d'allocation. Si la ressource se trouve dans un groupe IPAM qui est une ressource partagée dans AWS Resource Access Manager (RAM), le propriétaire de la ressource doit être configuré comme principal dans AWS RAM. Pour plus d'informations sur le partage de groupes avec RAM, consultezPartage d'un groupe IPAM à l'aide d'AWS RAM.

L'exemple suivant montre comment vous pouvez utiliser des règles d'allocation pour contrôler l'accès à un groupe IPAM :

Example

Lorsque vous créez vos groupes selon les besoins de routage et de sécurité, vous pouvez autoriser uniquement certaines ressources à utiliser un groupe. Dans ce cas, vous pouvez définir une règle d'allocation indiquant que toute ressource souhaitant un CIDR de ce groupe doit posséder une étiquette correspondant aux exigences liées aux étiquettes de règles d'allocation. Par exemple, vous pouvez définir une règle d'allocation indiquant que seuls les VPC possédant l'étiquette prod peuvent recevoir des CIDR d'un groupe IPAM.

> **Important**
>
> Cette section explique comment créer un groupe régional IPv6 avec une plage d'adresses IP fournie par AWS. Si vous souhaitez intégrer vos propres plages d'adresses IP IPv4 ou IPv6 à AWS (BYOIP), certaines conditions sont requises. Pour de plus amples informations, veuillez consulter Didacticiel : apporter vos adresses IP à IPAM.

AWS Management Console

Création d'un groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Sélectionnez Create pool (Créer un groupe).
4. Sous Portée IPAM, sélectionnez la portée publique. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.

Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Les groupes de la portée privée doivent être des groupes IPv4. Les groupes de la portée publique peuvent être des groupes IPv4 ou IPv6. La portée publique est destinée à tous les espaces pouvant être ou étant actuellement publiés par AWS sur Internet.

5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une description du groupe.
6. Sous Source, choisissez Portée IPAM.
7. Pour Famille d'adresses, sélectionnez IPv6. L'option Autoriser les CIDR de ce groupe à être publiés publiquement s'affiche. Par défaut, tous les CIDR de ce groupe pourront être publiés publiquement. Vous ne pouvez pas activer ou désactiver cette option.
8. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
9. Sélectionnez les Paramètres régionaux du groupe. Lorsque vous provisionnez un bloc CIDR IPv6 fourni par Amazon à un groupe, il doit être provisionné dans un groupe avec des paramètres régionaux (région AWS) sélectionnés. Le choix d'un paramètre régional garantit qu'il n'y a aucune dépendance entre les Régions entre votre groupe et les ressources qui y sont allouées. Les options disponibles proviennent des régions d'exploitation que vous avez choisies pour l'IPAM lors de sa création. Vous pouvez ajouter des régions d'exploitation à tout moment.

   Le paramètre régional est la Région AWS dans laquelle vous souhaitez que ce groupe IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP.

   > **Note**
   >
   > Si vous créez un groupe dans l'offre gratuite, vous ne pouvez choisir que les paramètres régionaux correspondant à la région d'accueil de votre IPAM. Pour utiliser

toutes les fonctionnalités IPAM dans tous les paramètres régionaux, passez au niveau avancé.

10. Sous Service, choisissez EC2 (EIP/VPC). Le service que vous sélectionnez détermine le service AWS où le CIDR pourra être annoncé. Actuellement, la seule option est EC2 (EIP/VPC), ce qui signifie que les CIDR alloués à partir de ce groupe pourront être annoncés pour le service Amazon EC2 (pour les adresses IP Elastic) et le service Amazon VPC (pour les CIDR associés aux VPC).
11. Sous l'option Source IP publique, sélectionnez Propriété d'Amazon afin qu'AWS fournisse une plage d'adresses IPv6 pour ce groupe. Comme indiqué ci-dessus, cette section explique comment créer un groupe régional IPv6 avec une plage d'adresses IP fournie par AWS. Si vous souhaitez fournir votre propre plage d'adresses IPv4 ou IPv6 à AWS (BYOIP), certaines conditions sont requises. Pour de plus amples informations, veuillez consulter Didacticiel : apporter vos adresses IP à IPAM.
12. Pour les groupes du champ d'application public qui utilisent la source IP publique BYOIP, vous pouvez décider si AWS peut publier publiquement les CIDR de ce groupe avec Autoriser les CIDR de ce groupe à être publiés publiquement. Cette option est activée par défaut. Désactivez cette option si vous ne souhaitez pas autoriser AWS à publier publiquement les CIDR de ce groupe.
13. (Facultatif) Vous pouvez créer un groupe sans CIDR, mais vous ne pourrez pas l'utiliser pour les allocations tant que vous n'aurez pas provisionné de CIDR pour celui-ci. Afin de provisionner un CIDR, choisissez Ajouter un CIDR appartenant à Amazon, puis la taille du masque réseau du CIDR (entre /40 et /52).

> **Note**
>
> Notez ce qui suit :
>
> - Par défaut, vous pouvez ajouter un bloc CIDR IPv6 fourni par Amazon au groupe régional. Pour plus d'informations sur l'augmentation de la limite par défaut, veuillez consulter la section Quotas pour votre IPAM (français non garanti).
> - Lorsque vous choisissez une longueur de masque réseau dans le menu déroulant, vous pouvez voir la longueur du masque réseau ainsi que le nombre de CIDR /56 qu'il représente.

14. Sélectionnez des règles d'allocation en option pour ce groupe :

- Longueur minimale du masque réseau : la longueur minimale du masque réseau requise pour que les allocations CIDR dans ce groupe IPAM soient conformes et le bloc d'adresse CIDR de la plus grande taille pouvant être alloué à partir du groupe. La longueur minimale du masque réseau doit être inférieure à la longueur maximale du masque réseau. Les longueurs possibles du masque réseau pour les adresses IPv6 sont comprises entre 0 et 128.
- Longueur du masque réseau par défaut : longueur de masque réseau par défaut pour les allocations ajoutées à ce groupe. Par exemple, si le CIDR provisionné à ce groupe est `2001:db8::/52` et que vous saisissez 56 ici, toutes les nouvelles allocations de ce groupe auront par défaut une longueur de masque réseau de /56.
- Longueur maximale du masque réseau : longueur maximale du masque réseau requise pour les allocations CIDR dans ce groupe. Cette valeur dicte le bloc d'adresse CIDR de la plus petite taille pouvant être alloué à partir du groupe. Par exemple, si vous saisissez /56 ici, ce sera également la plus petite longueur de masque réseau pouvant être allouée aux CIDR à partir de ce groupe.
- Exigences d'étiquette : étiquettes requises pour que les ressources allouent de l'espace à partir du groupe. Si les étiquettes des ressources ont été modifiées après l'allocation de l'espace ou si les règles d'étiquette des allocations sont modifiées sur le groupe, la ressource peut être marquée comme non conforme.
- Paramètres régionaux : paramètres régionaux requis pour les ressources qui utilisent des CIDR de ce groupe. Les ressources importées automatiquement qui ne possèdent pas ces paramètres régionaux seront marquées non conformes. Les ressources qui ne sont pas automatiquement importées dans le groupe ne seront pas autorisées à allouer de l'espace à partir du groupe à moins qu'elles ne se trouvent dans ces paramètres régionaux.

15. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
16. Sélectionnez Create pool (Créer un groupe).
17. Consultez Création d'un groupe IPv6 de développement.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour créer ou modifier un groupe régional IPv6 dans votre IPAM :

1. Créez un groupe : create-ipam-pool.
2. Modifiez le groupe après l'avoir créé pour modifier les règles d'allocation : modify-ipam-pool.

Création d'un groupe IPv6 de développement

Suivez les étapes de cette section pour créer un groupe de développement au sein de votre groupe régional IPv6. Si vous n'avez besoin que d'un groupe régional sans groupes de développement, passez à Allocation de CIDR.

L'exemple suivant illustre la hiérarchie de la structure de groupe que vous pouvez créer à l'aide des instructions de ce guide. À cette étape, vous créez un groupe IPAM de développement :

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée publique
    - Groupe régional dans région AWS 1 (2001:db8::/52)
      - Groupe de développement (2001:db8::/54)
        - Allocation pour un VPC (2001:db8::/56)

Dans l'exemple précédent, les CIDR utilisés ne sont que des exemples. Chaque groupe du groupe de niveau supérieur y est provisionné avec une partie du CIDR de niveau supérieur.

AWS Management Console

Pour créer un groupe de développement au sein d'un groupe régional IPv6

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Sélectionnez Create pool (Créer un groupe).
4. Sous Portée IPAM, sélectionnez la portée publique. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.

   Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Les groupes de la portée privée doivent être des groupes IPv4. Les groupes de la portée publique

peuvent être des groupes IPv4 ou IPv6. La portée publique est destinée à tous les espaces pouvant être ou étant actuellement publiés par AWS sur Internet.

5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une description du groupe.
6. Sous Source, choisissez Groupe IPAM. Puis, sous Groupe source, sélectionnez le groupe régional IPv6.
7. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
8. (Facultatif) Choisissez un CIDR à provisionner pour le groupe. Vous pouvez uniquement provisionner un CIDR qui a été provisionné au groupe de niveau supérieur. Vous pouvez créer un groupe sans CIDR, mais vous ne pourrez pas utiliser le groupe pour les allocations tant que vous n'aurez pas provisionné un CIDR pour celui-ci. Vous pouvez ajouter des CIDR à un groupe à tout moment en modifiant le groupe.
9. Vous disposez ici des mêmes options de règle d'allocation que lorsque vous avez créé le groupe régional IPv6. Consultez Création d'un groupe IPv6 régional pour obtenir une explication des options disponibles lorsque vous créez des groupes. Les règles d'allocation du groupe ne sont pas héritées du groupe situé au-dessus de lui dans la hiérarchie. Si vous n'appliquez aucune règle ici, aucune règle d'allocation ne sera définie pour le groupe.
10. (Facultatif) Choisissez Tags (Étiquettes) pour le groupe.
11. Lorsque vous avez fini de configurer votre groupe, choisissez Create pool (Créer un groupe).
12. Consultez Allocation de CIDR.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour créer un groupe régional IPv6 dans votre IPAM :

1. Obtenez l'ID de la portée dans laquelle vous voulez créer le groupe : describe-ipam-scopes
2. Obtenez l'ID du groupe dans lequel vous voulez créer le groupe : describe-ipam-pools
3. Créez le groupe : create-ipam-pool

4. Affichez le nouveau groupe : describe-ipam-pools

Répétez ces étapes pour créer des groupes de développement supplémentaires au sein du groupe régional IPv6, le cas échéant.

Allocation de CIDR

Suivez les étapes de cette section pour allouer un CIDR d'un groupe IPAM à une ressource.

> **Note**
>
> Les termes approvisionnement/provisionner et allocation/allouer sont utilisés dans ce guide de l'utilisateur et dans la console IPAM. Approvisionnement/provisionner sont des termes utilisés lorsque vous ajoutez un CIDR à un groupe IPAM. Allocation/allouer sont des termes utilisés lorsque vous associez un CIDR d'un groupe IPAM à une ressource.

Vous pouvez allouer des CIDR à partir d'un groupe IPAM de l'une des manières suivantes :

- Utilisez un service AWS intégré à IPAM, tel qu'Amazon VPC, et sélectionnez l'option permettant d'utiliser un groupe IPAM pour le CIDR. IPAM crée automatiquement l'allocation dans le groupe pour vous.
- Allouez manuellement un CIDR dans un groupe IPAM pour le réserver pour une utilisation ultérieure avec un service AWS intégré à IPAM, tel qu'Amazon VPC.

Cette section explique les deux options : comment utiliser les services AWS intégrés à IPAM pour provisionner un CIDR de groupe IPAM et comment réserver manuellement l'espace d'adresse IP.

Table des matières

- Création d'un VPC qui utilise un CIDR de groupe IPAM
- Allocation manuelle d'un CIDR à un groupe pour réserver de l'espace d'adresse IP

Création d'un VPC qui utilise un CIDR de groupe IPAM

Suivez les étapes décrites dans la section Création d'un VPC du Guide de l'utilisateur Amazon VPC. Lorsque vous arrivez à l'étape du choix de CIDR pour le VPC, vous aurez la possibilité d'utiliser un CIDR à partir d'un groupe IPAM.

Si vous choisissez l'option d'utiliser un groupe IPAM lorsque vous créez le VPC, AWS alloue un CIDR dans le groupe IPAM. Vous pouvez afficher l'allocation dans IPAM en choisissant un groupe dans le panneau de contenu de la console IPAM et en affichant l'onglet Resources (Ressources) du groupe.

> **Note**
>
> Pour obtenir des instructions complètes à l'aide de l'AWS CLI, notamment la création d'un VPC, consultez la section Didacticiels pour Amazon VPC IP Address Manager (IPAM).

Allocation manuelle d'un CIDR à un groupe pour réserver de l'espace d'adresse IP

Suivez les étapes de cette section pour allouer un CIDR à un groupe. Vous pouvez le faire afin de réserver un CIDR dans un groupe IPAM pour une utilisation ultérieure. Vous pouvez également réserver de l'espace dans votre groupe IPAM pour représenter un réseau sur site. IPAM gérera cette réservation pour vous et indiquera si des CIDR chevauchent votre espace IP sur site.

AWS Management Console

Pour allouer manuellement un CIDR

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, la portée privée par défaut est sélectionnée. Si vous ne souhaitez pas utiliser la portée privée par défaut, dans le menu déroulant en haut du panneau de contenu, choisissez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Dans le panneau de contenu, choisissez un groupe.
5. Choisissez Actions > Create custom allocation (Créer une allocation personnalisée).

6. Choisissez d'ajouter un CIDR spécifique à allouer (par exemple, `10.0.0.0/24` pour IPv4 ou `2001:db8::/52` pour IPv6) ou un CIDR par taille en spécifiant uniquement la longueur du masque réseau (par exemple, `/24` pour IPv4 ou `/52` pour IPv6).
7. Choisissez Allocate (Allouer).
8. Vous pouvez afficher l'allocation dans IPAM en choisissant Pools (Groupes) dans le panneau de navigation, en choisissant un groupe et en affichant l'onglet Allocations du groupe.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour allouer manuellement un CIDR à un groupe :

1. Générez l'ID du groupe IPAM dans lequel vous voulez créer l'allocation : describe-ipam-pools.
2. Créez l'allocation : allocate-ipam-pool-cidr.
3. Affichez l'allocation : get-ipam-pool-allocations.

Pour libérer un CIDR alloué manuellement, consultez Libération d'une allocation.

Gestion de l'espace d'adressage IP dans IPAM

Les tâches de cette section sont en option. Si vous souhaitez effectuer les tâches de cette section et que vous avez délégué un compte IPAM, les tâches doivent être exécutées par l'administrateur IPAM.

Suivez les étapes de cette section pour gérer votre espace d'adressage IP dans IPAM.

Table des matières

- Application de l'utilisation d'IPAM pour la création de VPC
- Partage d'un groupe IPAM à l'aide d'AWS RAM
- Approvisionnement de CIDR à un groupe
- Pour désapprovisionner un CIDR de groupe
- Modification d'un groupe
- Suppression d'un groupe
- Utilisation des découvertes de ressources
- Création de portées supplémentaires
- Déplacez des CIDR VPC entre les portées
- Modifiez l'état de contrôle des CIDR VPC
- Suppression d'une portée
- Libération d'une allocation
- Modifier un IPAM
- Suppression d'un IPAM

Application de l'utilisation d'IPAM pour la création de VPC

> **Note**
>
> Cette section s'applique à vous uniquement si vous avez activé l'intégration d'IPAM à AWS Organizations. Pour de plus amples informations, veuillez consulter Intégrer l'IPAM aux comptes d'une organisation AWS.

Cette section décrit comment créer une politique de contrôle de service dans AWS Organizations qui oblige les membres de votre organisation à utiliser IPAM lorsqu'ils créent un VPC. Les politiques de contrôle des services (SCP) constituent un type de stratégie d'organisation que vous pouvez utiliser pour gérer les autorisations dans votre organisation. Pour plus d'informations, consultez la section Politiques de contrôle de service du Guide de l'utilisateur AWS Organizations.

Appliquer IPAM lors de la création de VPC

Suivez les étapes de cette section pour obliger les membres de votre organisation à utiliser IPAM lors de la création de VPC.

Créer une politique de contrôle de service (SCP) et restreindre la création de VPC à IPAM

1. Suivez les étapes de la section Création d'une SCP du Guide de l'utilisateur d'AWS Organizations et saisissez le texte suivant dans l'éditeur JSON :

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

2. Associez la stratégie à une ou plusieurs unités organisationnelles de votre organisation. Pour obtenir de plus amples informations, consultez Attachement et détachement de politiques de contrôle des services dans le Guide de l'utilisateur AWS Organizations.

Appliquer un groupe IPAM lors de la création de VPC

Suivez les étapes de cette section pour obliger les membres de votre organisation à utiliser un groupe IPAM spécifique lors de la création de VPC.

Créer une politique de contrôle de service (SCP) et restreindre la création de VPC à un groupe IPAM

1. Suivez les étapes de la section Création d'une SCP du Guide de l'utilisateur d'AWS Organizations et saisissez le texte suivant dans l'éditeur 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. Modifiez l'exemple de valeur `ipam-pool-0123456789abcdefg` de l'ID de groupe IPv4 auquel vous souhaitez restreindre les utilisateurs.
3. Associez la stratégie à une ou plusieurs unités organisationnelles de votre organisation. Pour obtenir de plus amples informations, consultez Attachement et détachement de politiques de contrôle des services dans le Guide de l'utilisateur AWS Organizations.

Appliquer IPAM à toutes les unités d'organisation à l'exception d'une liste donnée

Suivez les étapes décrites dans cette section pour appliquer IPAM à toutes les unités d'organisation (UO), à l'exception d'une liste donnée. La politique décrite dans cette section exige que les UO de l'organisation, à l'exception des UO que vous spécifiez dans `aws:PrincipalOrgPaths`, utilisent IPAM pour créer et développer des VPC. Les UO répertoriées peuvent utiliser IPAM lors de la création de VPC ou spécifier une plage d'adresses IP manuellement.

Pour créer un SCP et appliquer IPAM à toutes les UO à l'exception d'une liste donnée

1. Suivez les étapes de la section Création d'une SCP du Guide de l'utilisateur d'AWS Organizations et saisissez le texte suivant dans l'éditeur JSON :

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

2. Supprimez les valeurs de l'exemple (comme `o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/`) et ajoutez les chemins de l'entité des AWS Organizations des UO pour lesquelles vous voulez avoir la possibilité (mais pas l'obligation) d'utiliser IPAM. Pour plus d'informations sur le chemin de l'entité, consultez Comprendre le chemin d'entité des AWS Organizations et aws:PrincipalOrgPaths dans le Guide de l'utilisateur AWS Identity and Access Management.
3. Attachez la politique à la racine de votre organisation. Pour obtenir de plus amples informations, consultez Attachement et détachement de politiques de contrôle des services dans le Guide de l'utilisateur AWS Organizations.

Partage d'un groupe IPAM à l'aide d'AWS RAM

Suivez les étapes de cette section pour partager un groupe IPAM à l'aide d'AWS Resource Access Manager (RAM). Lorsque vous partagez un groupe IPAM avec RAM, les « principaux » peuvent allouer des CIDR du groupe à des ressources AWS, telles que des VPC, à partir de leurs comptes respectifs. Un principal est un concept RAM qui sous-entend tout compte AWS, rôle IAM ou unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez la section Partage de vos ressources AWS du Guide de l'utilisateur AWS RAM.

Note

- Vous pouvez uniquement partager un groupe IPAM avec AWS RAM si vous avez intégré IPAM à AWS Organizations. Pour de plus amples informations, veuillez consulter Intégrer l'IPAM aux comptes d'une organisation AWS. Vous ne pouvez pas partager un groupe IPAM avec AWS RAM si vous êtes un utilisateur IPAM à compte unique.
- Vous devez activer le partage de ressources avecAWSOrganizations AWSutilisant RAM Pour de plus amples informations, veuillez consulter Activer le partage des ressources dans AWS Organizations dans le Guide de l'utilisateur RAMAWS.
- Le partage RAM n'est disponible que dans la région AWS d'origine de votre IPAM. Vous devez créer le partage dans la Région AWS dans laquelle se trouve l'IPAM, et non dans la Région du groupe IPAM.
- Le compte qui crée et supprime les partages de ressources de groupe IPAM doit disposer des autorisations suivantes dans la politique IAM associée au rôle IAM :
  - `ec2:PutResourcePolicy`
  - `ec2:DeleteResourcePolicy`
- Vous pouvez ajouter plusieurs groupes IPAM à un partage RAM.

AWS Management Console

Pour partager un groupe IPAM à l'aide de RAM

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, la portée privée par défaut est sélectionnée. Si vous ne souhaitez pas utiliser la portée privée par défaut, dans le menu déroulant en haut du panneau de contenu, choisissez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Dans le panneau de contenu, sélectionnez le groupe que vous souhaitez partager et sélectionnez Actions > View details (Afficher les détails).
5. Sous Resource sharing (Partage de ressources), sélectionnez Create resource share (Créer un partage de ressources). La console AWS RAM s'ouvre en conséquence. Vous créerez le groupe partagé dans AWS RAM.
6. Sélectionnez Create a resource share (Créer un partage de ressources).

7. Ajoutez une valeur Name (Nom) pour la ressource partagée.
8. Sous Select resource type (Sélectionner le type de ressource), sélectionnez les groupes IPAM et choisissez un ou plusieurs groupes IPAM.
9. Choisissez Next (Suivant).
10. Choisissez l'une des autorisations pour le partage de ressources :

    - AWSRAMDefaultPermissionsIpamPool : choisissez cette autorisation pour permettre aux principaux d'afficher les CIDR et les allocations dans le groupe IPAM partagé et d'allouer/de libérer des CIDR dans le groupe.
    - AWSRAMPermissionIpamPoolByoipCidrImport : choisissez cette autorisation pour autoriser les principaux à importer des CIDR BYOIP dans le groupe IPAM partagé. Vous n'aurez besoin de cette autorisation que si vous possédez des CIDR BYOIP existants et que vous souhaitez les importer dans IPAM et les partager avec les principaux. Pour plus d'informations sur les CIDR BYOIP vers IPAM, consultez Didacticiel : transfert d'un CIDR IPv4 BYOIP vers IPAM.
11. Choisissez les principaux autorisés à accéder à cette ressource. Si les principaux doivent importer des CIDR BYOIP existants dans ce groupe IPAM partagé, ajoutez le compte propriétaire du CIDR BYOIP en tant que mandataire.
12. Examinez les options de partage de ressources et les principaux avec lesquels vous procéderez au partage, et sélectionnez Create (Créer).

Command line

La ou les commandes de cette section renvoient vers la documentation de référence d'AWS CLI. Vous y trouverez des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez la ou les commandes.

Utilisez les commandes AWS CLI suivantes pour partager un groupe IPAM à l'aide de RAM :

1. Générez l'ARN de l'IPAM : describe-ipam-pools
2. Créez le partage de ressources : create-resource-share
3. Affichez le partage de ressources : get-resource-share

À la suite de la création du partage de ressources dans RAM, d'autres principaux peuvent désormais allouer des CIDR aux ressources à l'aide du groupe IPAM. Pour plus d'informations sur le contrôle des ressources créées par les principaux, consultez Contrôle de l'utilisation du CIDR par ressource.

Pour plus d'informations sur la création d'un VPC et l'allocation d'un CIDR à partir d'un groupe IPAM partagé, consultez Création d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Approvisionnement de CIDR à un groupe

Suivez les étapes de cette section pour provisionner des CIDR à un groupe. Si vous avez déjà provisionné un CIDR lorsque vous avez créé le groupe, vous devrez peut-être provisionner des CIDR supplémentaires si un groupe est presque entièrement alloué. Pour contrôler l'utilisation du groupe, consultez Contrôle de l'utilisation des CIDR à l'aide du tableau de bord IPAM.

> **Note**
>
> Les termes approvisionnement/provisionner et allocation/allouer sont utilisés dans ce guide de l'utilisateur et dans la console IPAM. Approvisionnement/provisionner sont des termes utilisés lorsque vous ajoutez un CIDR à un groupe IPAM. Allocation/allouer sont des termes utilisés lorsque vous associez un CIDR de groupe IPAM à un VPC ou une adresse IP Elastic.

AWS Management Console

Pour provisionner des CIDR à un groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, la portée privée par défaut est sélectionnée. Si vous ne souhaitez pas utiliser la portée privée par défaut, dans le menu déroulant en haut du panneau de contenu, choisissez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Dans le panneau de contenu, sélectionnez le groupe auquel vous souhaitez ajouter un CIDR.
5. Sélectionnez Actions > Provision CIDRs (Provisionner des CIDR).
6. Saisissez le CIDR que vous souhaitez ajouter, puis sélectionnez Add new CIDR (Ajouter un nouveau CIDR) en cas de CIDR supplémentaires.

> **Note**
>
> - Par défaut, vous pouvez ajouter un bloc CIDR IPv6 fourni par Amazon à un groupe régional. Pour plus d'informations sur l'augmentation de la limite par défaut, veuillez consulter la section Quotas pour votre IPAM (français non garanti).
> - Le CIDR que vous souhaitez provisionner doit être disponible dans la portée.
> - Si vous provisionnez des CIDR à un groupe au sein d'un groupe, l'espace CIDR que vous souhaitez provisionner doit être disponible dans le groupe.

7. Sélectionnez Request provisioning (Demander l'approvisionnement).
8. Vous pouvez afficher le CIDR dans IPAM en sélectionnant Pools (Groupes) dans le panneau de navigation, en sélectionnant un groupe et en affichant l'onglet CIDR du groupe.

Command line

Les commandes de cette section renvoient vers la documentation de référence de la CLI AWS. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour provisionner des CIDR à un groupe :

1. Générez l'ID d'un groupe IPAM : describe-ipam-pools
2. Générez les CIDR provisionnés dans le groupe : get-ipam-pool-cidrs
3. Provisionnez un nouveau CIDR au groupe : provision-ipam-pool-cidr
4. Générez les CIDR provisionnés dans le groupe et affichez le nouveau CIDR : get-ipam-pool-cidrs

Pour désapprovisionner un CIDR de groupe

Suivez les étapes décrites dans cette section pour désactiver les CIDR d'un groupe IPAM. Lorsque vous désactivez tous les CIDR de groupe, le groupe ne peut plus être utilisé pour les allocations. Vous devez d'abord provisionner un nouveau CIDR au groupe avant de pouvoir utiliser le groupe pour les allocations.

> **Important**
>
> Vous ne pouvez pas désactiver le CIDR s'il y a des allocations dans le groupe. Pour supprimer des allocations, consultez Libération d'une allocation.

AWS Management Console

Pour désactiver un CIDR de groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez Pools (Groupes).
3. Dans le menu déroulant se trouvant dans la partie supérieure du panneau de contenu, sélectionnez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Dans le panneau de contenu, sélectionnez le groupe dont vous voulez désactiver les CIDR.
5. Cliquez sur l'onglet CIDR.
6. Sélectionnez un ou plusieurs CIDR et sélectionnez Deprovision CIDRs (Désactiver les CIDR).
7. Sélectionnez Deprovision CIDR (Désactiver le CIDR).

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour désactiver un CIDR de groupe :

1. Obtenez un ID de groupe IPAM : describe-ipam-pools
2. Affichez vos CIDR actuels pour le groupe : get-ipam-pool-cidrs
3. Désactivez les CIDR : deprovision-ipam-pool-cidr
4. Affichez vos CIDR mis à jour : get-ipam-pool-cidrs

Pour provisionner un nouveau CIDR au groupe, consultez Pour désapprovisionner un CIDR de groupe. Si vous souhaitez supprimer le groupe, consultez Suppression d'un groupe.

Modification d'un groupe

Suivez les étapes de cette section pour modifier un groupe IPAM. Vous pouvez modifier un groupe pour modifier les règles d'allocation dans le groupe. Pour plus d'informations sur les règles d'allocations, consultez Création d'un groupe IPv4 de niveau supérieur.

AWS Management Console

Pour modifier un groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, la portée privée par défaut est sélectionnée. Si vous ne souhaitez pas utiliser la portée privée par défaut, dans le menu déroulant en haut du panneau de contenu, sélectionnez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Dans le panneau de contenu, sélectionnez le groupe dont vous souhaitez modifier le CIDR.
5. Sélectionnez Actions > Edit (Modifier).
6. Apportez toutes les modifications dont vous avez besoin aux groupes. Pour plus d'informations sur les options de configuration des groupes, consultez Création d'un groupe IPv4 de niveau supérieur.
7. Sélectionnez Update (Mise à jour).

Command line

Utilisez les commandes AWS CLI suivantes pour modifier un groupe :

1. Obtenez un ID de groupe IPAM : describe-ipam-pools
2. Modifiez le groupe : modify-ipam-pool

Suppression d'un groupe

Suivez les étapes de cette section pour supprimer un groupe IPAM.

> **Important**
>
> Vous ne pouvez pas supprimer un groupe d'adresses IP s'il contient des allocations. Vous devez d'abord libérer les allocations et Pour désapprovisionner un CIDR de groupe avant de pouvoir supprimer le groupe.

AWS Management Console

Pour supprimer un groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez Pools (Groupes).
3. Dans le menu déroulant se trouvant dans la partie supérieure du panneau de contenu, sélectionnez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Dans le panneau de contenu, sélectionnez le groupe dont vous voulez supprimer le CIDR.
5. Sélectionnez Actions > Delete Pool (Supprimer un groupe).
6. Saisissez **`delete`** (supprimer), puis sélectionnez Delete (Supprimer).

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour supprimer un groupe :

1. Affichez les groupes et générez un ID de groupe IPAM : describe-ipam-pools
2. Supprimez un groupe : delete-ipam-pool
3. Affichez vos groupes : describe-ipam-pools

Pour créer un nouveau groupe, consultez Création d'un groupe IPv4 de niveau supérieur.

Utilisation des découvertes de ressources

Une découverte de ressources est un composant IPAM qui permet à IPAM de gérer et surveiller les ressources appartenant au compte propriétaire. Une découverte de ressources est créée par défaut lorsque vous créez un IPAM. Vous pouvez également créer une découverte de ressources indépendamment d'un IPAM et l'intégrer à un IPAM appartenant à un autre compte ou une autre organisation. Si le propriétaire de la découverte de ressources est l'administrateur délégué d'une organisation, IPAM surveille les ressources de tous les membres de l'organisation.

> **Note**
>
> La création, le partage et l'association de découvertes de ressources font partie du processus d'intégration d'IPAM à des comptes extérieurs à votre organisation. Pour plus d'informations, veuillez consulter la section Intégration d'IPAM à des comptes extérieurs à votre organisation (français non garanti). Si vous ne créez pas et n'intégrez pas d'IPAM à des comptes extérieurs à votre organisation, vous n'avez pas besoin de créer, partager ou associer des découvertes de ressources.

Table des matières

- Créer une découverte de ressources
- Afficher les détails d'une découverte de ressources
- Partage d'une découverte de ressources
- Associer une découverte de ressources à un IPAM
- Dissocier une découverte de ressources
- Supprimer une découverte de ressources

Créer une découverte de ressources

Cette section explique comment créer une découverte de ressources. Une découverte de ressources est créée par défaut lorsque vous créez un IPAM. Le quota par défaut est une découverte de ressources par région. Pour de plus amples informations sur les quotas d'IPAM, veuillez consulter la section Quotas pour votre IPAM (français non garanti).

> **Note**
>
> La création, le partage et l'association de découvertes de ressources font partie du processus d'intégration d'IPAM à des comptes extérieurs à votre organisation. Pour plus d'informations, veuillez consulter la section Intégration d'IPAM à des comptes extérieurs à votre organisation (français non garanti). Si vous ne créez pas et n'intégrez pas d'IPAM à des comptes extérieurs à votre organisation, vous n'avez pas besoin de créer, partager ou associer des découvertes de ressources.

Si vous intégrez un IPAM à des comptes extérieurs à vos organisations, cette étape est obligatoire et doit être effectuée par le compte administrateur de l'organisation secondaire. Pour plus d'informations sur les rôles impliqués dans ce processus, veuillez consulter la section Présentation du processus (français non garanti).

AWS Management Console

Pour créer une découverte de ressources

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le volet de navigation, sélectionnez Découvertes de ressources.
3. Sélectionnez Créer une découverte de ressources.
4. Sélectionnez Allow Amazon VPC IP Address Manager to replicate data from source account(s) into an IPAM Delegate account (Autoriser Amazon VPC IP Address Manager à répliquer les données du ou des comptes source dans le compte IPAM délégué). Si vous ne sélectionnez pas cette option, vous ne pouvez pas créer de découverte de ressources.
5. (Facultatif) Ajoutez une balise Nom à la découverte de ressources. Une balise est une étiquette que vous affectez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative. Vous pouvez utiliser des balises pour rechercher et filtrer vos ressources ou suivre vos AWS coûts.
6. (Facultatif) Ajoutez une description.
7. Sous Régions d'exploitation, sélectionnez les régions AWS dans lesquelles les ressources seront découvertes. La région actuelle sera automatiquement définie comme l'une des régions d'exploitation. Si vous créez la découverte de ressources afin de pouvoir la partager avec un IPAM de la région d'exploitation `us-east-1`, assurez-vous de sélectionner `us-`

`east-1` ici. Si vous oubliez une région d'exploitation, vous pouvez revenir ultérieurement et modifier vos paramètres de découverte de ressources.

> **Note**
>
> Dans la plupart des cas, la découverte de ressources doit avoir les mêmes régions d'exploitation que l'IPAM, sinon vous n'obtenez la découverte de ressources que dans cette région.

8. (Facultatif) Choisissez des balises supplémentaires pour le groupe.
9. Choisissez Créer.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Créer une découverte de ressources : create-ipam-resource-discovery

Afficher les détails d'une découverte de ressources

Cette section explique comment afficher les détails d'une découverte de ressources. Ceux-ci incluent les CIDR de ressource et les statuts de découverte des comptes surveillés dans le cadre de votre découverte de ressources.

AWS Management Console

Pour afficher les détails d'une découverte de ressources

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le volet de navigation, sélectionnez Découvertes de ressources.
3. Sélectionnez une découverte de ressources.
4. Sous Détails relatifs à la découverte, affichez les détails relatifs à la découverte de ressources. Par exemple, la section Par défaut indique s'il s'agit de la découverte de ressources par défaut. La découverte de ressources par défaut est celle créée automatiquement lorsque vous créez un IPAM.

5. Dans les onglets, affichez les détails d'une découverte de ressources :

   - Ressources découvertes : ressources surveillées dans le cadre d'une découverte de ressources. L'IPAM surveille les CIDR à partir des types de ressources suivants : VPC, groupes IPv4 publics, sous-réseaux VPC et adresses IP Elastic.
     - Nom (ID de ressource) : ID de découverte de ressources.
     - Utilisation de l'adresse IP : pourcentage d'espace d'adressage IP utilisé. Afin de convertir la décimale en pourcentage, multipliez-la par 100. Notez ce qui suit :
       - Pour les ressources qui sont des VPC, il s'agit du pourcentage d'espace d'adressage IP dans le VPC occupé par les CIDR de sous-réseau.
       - Pour les ressources qui constituent des sous-réseaux, si un CIDR IPv4 est provisionné pour le sous-réseau, il s'agit du pourcentage d'espace d'adressage IPv4 dans le sous-réseau utilisé. Si un CIDR IPv6 est provisionné pour le sous-réseau, le pourcentage d'espace d'adressage IPv6 utilisé n'est pas représenté. Le pourcentage d'espace d'adressage IPv6 utilisé ne peut pas être calculé pour le moment.
       - Pour les ressources qui sont des groupes IPv4 publics, il s'agit du pourcentage d'espace d'adressage IP dans le groupe qui a été alloué aux adresses IP Elastic (EIP).
     - CIDR : CIDR de ressource.
     - Région : région de ressource.
     - ID de propriétaire : ID de propriétaire de ressource.
     - Temps d'échantillonnage : heure de la dernière découverte de ressources réussie.
   - Comptes découverts : comptes AWS surveillés dans le cadre d'une découverte de ressources. Si vous avez intégré IPAM à AWS Organizations, tous les comptes de l'organisation sont des comptes découverts.
     - ID de compte : ID du compte.
     - Région : région AWS à partir de laquelle les informations de compte sont renvoyées.
     - Heure de la dernière tentative de découverte : heure de la dernière tentative de découverte de ressource.
     - Heure de la dernière découverte réussie : heure de la dernière découverte de ressources réussie.
     - Statut : motif de l'échec de la découverte de ressources.
   - Régions d'exploitation : régions d'exploitation pour la découverte de ressources.

- Partage des ressources : si la découverte de ressources a été partagée, l'ARN du partage des ressources est répertorié.
  - ARN du partage de ressources : ARN du partage de ressources.
  - Statut : statut actuel du partage de ressources. Les valeurs possibles sont :
    - Actif : le partage de ressources est actif et peut être utilisé.
    - Supprimé : le partage de ressources est supprimé et ne peut plus être utilisé.
    - En attente : une invitation à accepter le partage de ressources est en attente de réponse.
  - Créé le : date de création du partage de ressources.
- Balises : une balise est une étiquette que vous attribuez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative. Vous pouvez utiliser des balises pour rechercher et filtrer vos ressources ou suivre vos AWS coûts.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Afficher les détails d'une découverte de ressources : describe-ipam-resource-discovery

Partage d'une découverte de ressources

Suivez les étapes de cette section pour partager une découverte de ressources à l'aide d'AWS Resource Access Manager. Pour plus d'informations sur AWS RAM, veuillez consulter la section Partage de vos ressources AWS du Guide de l'utilisateur AWS RAM (français non garanti).

> **Note**
>
> La création, le partage et l'association de découvertes de ressources font partie du processus d'intégration d'IPAM à des comptes extérieurs à votre organisation. Pour plus d'informations, veuillez consulter la section Intégration d'IPAM à des comptes extérieurs à votre organisation (français non garanti). Si vous ne créez pas et n'intégrez pas d'IPAM à des comptes extérieurs à votre organisation, vous n'avez pas besoin de créer, partager ou associer des découvertes de ressources.

Lorsque vous créez un IPAM qui surveille des comptes extérieurs à votre organisation, le compte administrateur de l'organisation secondaire partage sa découverte de ressources avec le compte IPAM de l'organisation principale à l'aide d'AWS RAM. Vous devez d'abord partager une découverte de ressources avec le compte IPAM de l'organisation principale avant que celui-ci puisse l'associer à son IPAM. Pour plus d'informations sur les rôles impliqués dans ce processus, veuillez consulter la section Présentation du processus (français non garanti).

> **Note**
>
> - Lorsque vous créez un partage de ressources à l'aide d'AWS RAM pour partager une découverte de ressources, vous devez le créer dans la région d'origine de l'IPAM de l'organisation principale.
> - Le compte qui crée et supprime un partage de ressources pour une découverte de ressources doit disposer des autorisations suivantes dans sa politique IAM :
>   - ec2:PutResourcePolicy
>   - ec2:DeleteResourcePolicy

Si vous intégrez un IPAM à des comptes extérieurs à vos organisations, cette étape est obligatoire et doit être effectuée par le compte administrateur de l'organisation secondaire.

AWS Management Console

Pour partager une découverte de ressources

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le volet de navigation, sélectionnez Découvertes de ressources.
3. Sélectionnez l'onglet Partage des ressources.
4. Choisissez Créer une ressource. La console AWS RAM s'ouvre afin de vous permettre de créer le partage de ressources.
5. Dans la console AWS RAM, choisissez Paramètres.
6. Sélectionnez Activer le partage avec AWS Organizations, puis Enregistrer les paramètres.
7. Sélectionnez Create a resource share (Créer un partage de ressources).
8. Ajoutez une valeur Name (Nom) pour la ressource partagée.

9. Sous Sélectionner le type de ressource, sélectionnez Découverte de ressources IPAM, puis la découverte de ressources.
10. Choisissez Next (Suivant).
11. Sous Autorisations d'association, vous pouvez afficher l'autorisation par défaut qui sera activée pour les principaux ayant accès à ce partage de ressources :
    - AWSRAMPermissionIpamResourceDiscovery
    - Actions autorisées par cette autorisation :
      - ec2:AssociateIpamResourceDiscovery
      - ec2:GetIpamDiscoveredAccounts
      - ec2:GetIpamDiscoveredPublicAddresses
      - ec2:GetIpamDiscoveredResourceCidrs
12. Spécifiez les principaux autorisés à accéder à la ressource partagée. Pour Principaux, sélectionnez le compte IPAM de l'organisation principale, puis cliquez sur Ajouter.
13. Choisissez Next (Suivant).
14. Passez en revue les options de partage de ressources et les principaux avec lesquels vous procéderez au partage. Ensuite, sélectionnez Créer un partage de ressources.
15. Une fois qu'une découverte de ressources est partagée, elle doit être acceptée puis associée à un IPAM par le compte IPAM de l'organisation principale. Pour de plus amples informations, veuillez consulter Associer une découverte de ressources à un IPAM.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

1. Créez le partage de ressources : create-resource-share
2. Affichez le partage de ressources : get-resource-share

Associer une découverte de ressources à un IPAM

Cette section explique comment associer une découverte de ressources à un IPAM. Lorsque vous associez une découverte de ressources à un IPAM, celui-ci surveille tous les CIDR de ressources

et comptes découverts dans le cadre de la découverte de ressources. Lorsque vous créez un IPAM, une découverte de ressources par défaut est créée et associée automatiquement à votre IPAM.

Le quota par défaut pour les associations de découvertes de ressources est égal à cinq. Pour plus d'informations (notamment sur la manière d'ajuster ce quota), veuillez consulter la section Quotas pour votre IPAM (français non garanti).

> **Note**
>
> La création, le partage et l'association de découvertes de ressources font partie du processus d'intégration d'IPAM à des comptes extérieurs à votre organisation. Pour plus d'informations, veuillez consulter la section Intégration d'IPAM à des comptes extérieurs à votre organisation (français non garanti). Si vous ne créez pas et n'intégrez pas d'IPAM à des comptes extérieurs à votre organisation, vous n'avez pas besoin de créer, partager ou associer des découvertes de ressources.

Si vous intégrez un IPAM à des comptes extérieurs à vos organisations, il s'agit d'une étape obligatoire qui doit être effectuée par le compte IPAM de l'organisation principale. Pour plus d'informations sur les rôles impliqués dans ce processus, veuillez consulter la section Présentation du processus (français non garanti).

AWS Management Console

Pour associer une découverte de ressources

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez IPAMs (IPAM).
3. Sélectionnez Découvertes associées, puis Découvertes de ressources associées.
4. Sous Découvertes de ressources IPAM, sélectionnez une découverte de ressources qui a été partagée avec vous par le compte administrateur de l'organisation secondaire.
5. Choisissez Associate.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Associer une découverte de ressources : associate-ipam-resource-discovery

Dissocier une découverte de ressources

Cette section explique comment dissocier une découverte de ressources d'un IPAM. Lorsque vous dissociez une découverte de ressources d'un IPAM, celui-ci ne surveille plus tous les CIDR de ressources et comptes découverts dans le cadre de la découverte de ressources.

> **Note**
>
> Vous ne pouvez pas dissocier une association de découverte de ressources par défaut. Lorsque vous créez un IPAM, une association de découverte de ressources par défaut est créée automatiquement. Cependant, l'association de découverte de ressources par défaut est supprimée si vous supprimez l'IPAM.

Cette étape doit être effectuée par le compte IPAM de l'organisation principale. Pour plus d'informations sur les rôles impliqués dans ce processus, veuillez consulter la section Présentation du processus (français non garanti).

AWS Management Console

Pour dissocier une découverte de ressources

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez IPAMs (IPAM).
3. Sélectionnez Découvertes associées, puis Dissocier les découvertes de ressources.
4. Sous Découvertes de ressources IPAM, sélectionnez une découverte de ressources qui a été partagée avec vous par le compte administrateur de l'organisation secondaire.
5. Choisissez Dissocier.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Pour dissocier une découverte de ressources : disassociate-ipam-resource-discovery

Supprimer une découverte de ressources

Cette section explique comment supprimer une découverte de ressources.

> **Note**
>
> Vous ne pouvez pas supprimer une découverte de ressources par défaut. Lorsque vous créez un IPAM, une découverte de ressources par défaut est créée automatiquement. Cependant, la découverte de ressources par défaut est supprimée si vous supprimez l'IPAM.

Cette étape doit être effectuée par le compte administrateur de l'organisation secondaire. Pour plus d'informations sur les rôles impliqués dans ce processus, veuillez consulter la section Présentation du processus (français non garanti).

AWS Management Console

Pour supprimer une découverte de ressources

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le volet de navigation, sélectionnez Découvertes de ressources.
3. Sélectionnez une découverte de ressources, puis Actions et Supprimer la découverte de ressources.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Pour supprimer une découverte de ressources : delete-ipam-resource-discovery

Création de portées supplémentaires

Suivez les étapes de cette section pour créer une portée supplémentaire.

Une portée est le conteneur de niveau le plus élevé d'IPAM. Lorsque vous créez un IPAM, IPAM crée deux portées par défaut pour vous. Chaque portée représente l'espace IP d'un réseau unique.

La portée privée est destinée à tous les espaces privés. La portée publique est destinée à tous les espaces publics. Les portées vous permettent de réutiliser les adresses IP sur plusieurs réseaux non connectés sans provoquer de chevauchement ou de conflit d'adresses IP.

Lorsque vous créez un IPAM, des portées par défaut (une portée privée et une publique) sont créées pour vous. Vous pouvez créer d'autres portées privées. Vous ne pouvez pas créer d'autres portées publiques.

Vous pouvez créer des portées privées supplémentaires si vous avez besoin d'une prise en charge de plusieurs réseaux privés déconnectés. Les portées privées supplémentaires vous permettent de créer des groupes et de gérer des ressources utilisant le même espace IP.

> **Important**
>
> Si IPAM détecte des ressources avec des CIDR IPv4 privés, les CIDR de ressource sont importés dans la portée privée par défaut et n'apparaissent dans aucune portée privée supplémentaire que vous créez. Vous pouvez déplacer les CIDR de la portée privée par défaut vers une autre portée privée. Pour plus d'informations, consultez Déplacez des CIDR VPC entre les portées.

AWS Management Console

Pour créer une portée privée supplémentaire

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Scopes (Portées).
3. Choisissez Create scope (Créer une portée).
4. Choisissez l'IPAM auquel vous souhaitez ajouter la portée.
5. Ajoutez une description de la portée.
6. Choisissez Create scope (Créer une portée).
7. Vous pouvez afficher la portée dans IPAM en choisissant Scopes (Portées) dans le panneau de navigation.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour créer une portée privée supplémentaire :

1. Affichez vos portées actuelles : describe-ipam-scopes
2. Créez une nouvelle portée privée : create-ipam-scope
3. Affichez vos portées actuelles pour afficher la nouvelle portée : describe-ipam-scopes

Déplacez des CIDR VPC entre les portées

Suivez les étapes de cette section pour déplacer un CIDR VPC d'une portée à une autre.

⚠ Important

- Vous pouvez uniquement déplacer des CIDR VPC. Lorsque vous déplacez un CIDR VPC, les CIDR de sous-réseau du VPC sont également déplacés automatiquement.
- Vous ne pouvez déplacer que les CIDR VPC d'une portée privée à une autre. Vous ne pouvez pas déplacer les CIDR VPC hors d'une portée publique vers une portée privée ou d'une portée privée vers une portée publique.
- Le même compte AWS doit posséder les deux portées.
- Si un CIDR VPC est actuellement alloué à partir d'un groupe dans une portée privée, la demande de déplacement réussit, mais le CIDR VPC ne sera pas déplacé jusqu'à ce que vous libériez l'allocation du CIDR VPC du groupe actuel. Pour plus d'informations sur la libération d'une allocation, consultez Libération d'une allocation.

AWS Management Console

Pour déplacer un CIDR alloué à un VPC

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Resources (Ressources).

3. Dans le menu déroulant situé dans la partie supérieure du panneau de contenu, sélectionnez la portée que vous voulez utiliser.
4. Dans le panneau de contenu, sélectionnez un VPC et affichez les détails du VPC.
5. Sous VPC CIDRs (CIDR VPC), sélectionnez l'un des CIDR alloués à la ressource et sélectionnez Actions > Move CIDR to different scope (Déplacer le CIDR vers une autre portée).
6. Sélectionnez la portée vers laquelle vous souhaitez déplacer le CIDR VPC.
7. Choisissez Move CIDR to different scope (Déplacer le CIDR vers une autre portée).

Command line

Utilisez les commandes AWS CLI suivantes pour déplacer un CIDR VPC :

1. Obtenez un CIDR VPC dans la portée actuelle : get-ipam-resource-cidrs
2. Déplacez un CIDR VPC : modify-ipam-resource-cidr
3. Obtenez un CIDR VPC dans l'autre portée : get-ipam-resource-cidrs

Modifiez l'état de contrôle des CIDR VPC

Suivez les étapes de cette section pour modifier l'état de contrôle d'un CIDR VPC. Vous voudrez peut-être changer un CIDR VPC de l'état monitored (Contrôlé) à l'état ignored (Ignoré) si vous ne souhaitez pas qu'IPAM gère ou contrôle le VPC et autorise le CIDR alloué au VPC à être disponible pour utilisation. Vous voudrez peut-être changer un CIDR VPC de l'état ignored (Ignoré) à l'état monitored (Contrôlé) si vous souhaitez qu'IPAM gère et contrôle le CIDR VPC.

> **Note**
>
> - Vous ne pouvez pas ignorer les CIDR VPC dans la portée publique.
> - Si un CIDR est ignoré, les adresses IP actives dans le CIDR vous sont toujours facturées. Pour de plus amples informations, veuillez consulter Tarification d'IPAM.
> - Si un CIDR est ignoré, vous pouvez toujours consulter l'historique des adresses IP dans le CIDR. Pour de plus amples informations, veuillez consulter Afficher l'historique des adresses IP.

Vous pouvez modifier l'état de contrôle d'un CIDR VPC sur monitored (Contrôlé) ou ignored (Ignoré) :

- Monitored (Contrôlé) : le CIDR VPC a été détecté par IPAM et est contrôlé pour détecter les chevauchements avec d'autres CIDR et la conformité aux règles d'allocation.
- Ignored (Ignoré) : la ressource a été choisie de manière à être exemptée de contrôle. Les CIDR VPC ignorés ne sont pas évalués pour les chevauchements avec d'autres CDIR ou la conformité aux règles d'allocation. Une fois qu'un CIDR VPC est choisi pour être ignoré, tout espace qui lui est alloué à partir d'un groupe IPAM est renvoyé au groupe et le CIDR VPC ne sera plus importé via l'importation automatique (si la règle d'allocation d'importation automatique est définie sur le groupe).

AWS Management Console

Pour modifier l'état de surveillance d'un CIDR alloué à un VPC

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Resources (Ressources).
3. Dans le menu déroulant situé dans la partie supérieure du panneau de contenu, sélectionnez la portée privée que vous voulez utiliser.
4. Dans le panneau de contenu, sélectionnez le VPC et affichez les détails du VPC.
5. Sous CIDR de VPC, sélectionnez l'un des CIDR alloués au VPC et choisissez Actions > Marquer comme ignoré ou Ne pas marquer comme ignoré.
6. Choisissez Mark as ignored (Marquer comme ignoré) ou Unmark as ignored (Ne pas marquer comme ignoré).

Command line

Utilisez les commandes AWS CLI suivantes pour modifier l'état de contrôle d'un CIDR VPC :

1. Obtenez un ID de portée : describe-ipam-scopes
2. Affichez l'état actuel de contrôle du CIDR VPC : get-ipam-ressource-cidrs
3. Modifiez l'état du CIDR VPC : modify-ipam-resource-cidr
4. Affichez le nouvel état de contrôle du CIDR VPC : get-ipam-ressource-cidrs

Suppression d'une portée

Suivez les étapes de cette section pour supprimer une portée IPAM.

> **Important**
>
> Vous ne pouvez pas supprimer une portée si l'une des conditions suivantes est vraie :
>
> - La portée est une portée par défaut. Lorsque vous créez un IPAM, deux portées par défaut (une publique, une privée) sont créées automatiquement et ne peuvent pas être supprimées. Pour voir si une portée est une portée par défaut, consultez Scope type (Type de portée) dans les détails de la portée.
> - Il y a un ou plusieurs groupes dans la portée. Il faut d'abord Suppression d'un groupe avant de pouvoir supprimer la portée.

AWS Management Console

Pour supprimer une portée

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez Scopes (Portées).
3. Dans le panneau de contenu, sélectionnez la portée que vous souhaitez supprimer.
4. Sélectionnez Actions > Delete scope (Supprimer une portée).
5. Saisissez **`delete`** (supprimer), puis sélectionnez Delete (Supprimer).

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour supprimer une portée :

1. Affichez les portées : describe-ipam-scopes
2. Supprimez une portée : delete-ipam-scope
3. Affichez les portées mises à jour : describe-ipam-scopes

Pour créer une nouvelle portée, consultez Création de portées supplémentaires. Pour supprimer l'IPAM consultez Suppression d'un IPAM.

Libération d'une allocation

Suivez les étapes de cette section pour libérer une allocation CIDR à partir d'un groupe IPAM. Une allocation est une affectation CIDR d'un groupe IPAM à une autre ressource ou un autre groupe IPAM.

Si vous envisagez de supprimer un groupe, vous devrez peut-être libérer une allocation de groupe. Vous ne pouvez pas supprimer des groupes si ceux-ci ont des CIDR alloués, et vous ne pouvez pas mettre hors service des CIDR si ceux-ci sont alloués à des ressources.

Note

- Pour libérer une allocation manuelle, suivez les étapes de cette section ou appelez l'API ReleaseIpamPoolAllocation.
- Pour libérer une allocation dans une étendue privée, vous devez ignorer ou supprimer le CIDR de la ressource. Pour de plus amples informations, veuillez consulter Modifiez l'état de contrôle des CIDR VPC. Après un certain temps, Amazon VPC IPAM libérera automatiquement l'allocation en votre nom.

  Example

  Example (Exemple)

  Si vous avez un CIDR de VPC dans une portée privée, vous devez ignorer ou supprimer celui-ci pour libérer l'allocation. Après un certain temps, Amazon VPC IPAM libère automatiquement l'allocation de CIDR de VPC du groupe d'IPAM.
- Pour libérer une allocation dans une étendue publique, vous devez supprimer le CIDR de la ressource. Vous ne pouvez pas ignorer les CIDR de ressources publiques. Pour plus d'informations, consultez Cleanup (Nettoyage) dans Apportez votre propre CIDR IPv4 public à IPAM en utilisant uniquement la CLI AWS ou Cleanup (Nettoyage) dans Apportez votre propre CIDR IPv6 à l'IPAM en utilisant uniquement la CLI AWS. Après un certain temps, Amazon VPC IPAM libérera automatiquement l'allocation en votre nom.

Pour qu'Amazon VPC IPAM libère des allocations en votre nom, toutes les autorisations de compte doivent être correctement configurées pour une utilisation à compte unique ou à plusieurs comptes.

Lorsque vous libérez un CIDR géré par votre IPAM, l'IPAM d'Amazon VPC recycle le CIDR dans un groupe IPAM. Il faut quelques minutes pour que le CIDR devienne disponible pour les allocations futures. Pour plus d'informations sur les groupes et allocations, consultez Fonctionnement d'IPAM.

AWS Management Console

Pour libérer une allocation de groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Dans le menu déroulant situé dans la partie supérieure du panneau de contenu, sélectionnez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Dans le panneau de contenu, sélectionnez le groupe dans lequel se trouve l'allocation.
5. Cliquez sur l'onglet Allocations.
6. Sélectionnez une ou plusieurs allocations. Vous pouvez identifier les allocations en fonction de leur type de ressource :
   - custom : allocation personnalisée.
   - vpc : allocation de VPC.
   - ipam-pool : allocation de groupe IPAM.
   - ec2-public-ipv4-pool : allocation de groupe IPv4 public.
7. Choisissez Actions > Release custom allocation (Lancer l'allocation personnalisée).
8. Sélectionner Deallocate CIDR (Désallouer le CIDR).

Command line

Les commandes de cette section renvoient vers la documentation de référence de la CLI AWS. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour libérer une allocation de groupe :

1. Générez l'ID d'un groupe IPAM : describe-ipam-pools
2. Consultez vos allocations actuelles dans le groupe : get-ipam-pool-allocations
3. Libérez une allocation : release-ipam-pool-allocation
4. Affichez vos allocations mises à jour : get-ipam-pool-allocations

Pour ajouter une nouvelle allocation, consultez Allocation de CIDR. Pour supprimer le groupe après avoir libéré des allocations, vous devez d'abord Pour désapprovisionner un CIDR de groupe.

Modifier un IPAM

Suivez les étapes de cette section pour modifier un IPAM.

Table des matières

- Modifier un niveau IPAM
- Modifiez les régions d'exploitation IPAM

Modifier un niveau IPAM

Suivez les étapes de cette section pour modifier le niveau IPAM. L'IPAM propose deux niveaux : le niveau gratuit et le niveau avancé. Pour plus d'informations sur les fonctionnalités disponibles dans chaque niveau gratuit et les coûts associés aux niveau avancé, consultez l'onglet IPAM sur la page de tarification d'Amazon VPC.

⚠ Important

Avant de pouvoir passer du niveau avancé au niveau gratuit, vous devez :

- Supprimer les groupes de portée privée.
- Supprimer les portées privées autres que celles par défaut.
- Supprimer les groupes dont les paramètres régionaux sont différents de ceux de la région d'accueil de l'IPAM.
- Supprimer les associations de découvertes de ressources autres que celles par défaut.
- Supprimer les allocations de groupe aux comptes qui ne sont pas le propriétaire de l'IPAM.

AWS Management Console

Pour modifier le niveau IPAM

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez IPAMs (IPAM).
3. Dans le panneau de contenu, sélectionnez votre IPAM.
4. Sélectionnez Actions > Edit (Modifier).
5. Choisissez le niveau IPAM que vous souhaitez utiliser pour l'IPAM.
6. Choisissez Enregistrer les modifications.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour afficher et modifier un niveau IPAM :

1. Affichez les IPAM actuels : describe-ipams
2. Modifiez le niveau IPAM : modify-ipam
3. Affichez vos IPAM mises à jour : describe-ipam

Modifiez les régions d'exploitation IPAM

Suivez les étapes de cette section pour modifier les régions d'exploitation IPAM. Les régions d'exploitation sont les régions AWS où l'IPAM est autorisé à gérer les CIDR d'adresses IP. IPAM ne détecte et ne contrôle les ressources que dans les régions AWS que vous sélectionnez comme régions d'exploitation.

AWS Management Console

Pour modifier les régions d'exploitation IPAM

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez IPAMs (IPAM).

3. Dans le panneau de contenu, sélectionnez votre IPAM.
4. Sélectionnez Actions > Edit (Modifier).
5. Sous Paramètres IPAM, choisissez les Régions d'exploitation que vous souhaitez utiliser pour l'IPAM.
6. Choisissez Enregistrer les modifications.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour afficher et modifier les régions d'exploitation IPAM :

1. Affichez les IPAM actuels : describe-ipams
2. Ajoutez ou supprimez des régions d'exploitation IPAM : modify-ipam
3. Affichez vos IPAM mises à jour : describe-ipam

Suppression d'un IPAM

Suivez les étapes de cette section pour supprimer un IPAM. Pour plus d'informations sur l'augmentation du nombre d'IPAM par défaut que vous pouvez posséder plutôt que de supprimer un IPAM existant, consultez Quotas pour votre IPAM.

> **Important**
>
> La suppression d'un IPAM supprime toutes les données contrôlées associées à l'IPAM, y compris les données historiques des CIDR.

AWS Management Console

Pour supprimer un IPAM

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.

2. Dans le panneau de navigation, sélectionnez IPAMs (IPAM).
3. Dans le panneau de contenu, sélectionnez votre IPAM.
4. Pour Actions, sélectionnez Delete (Supprimer).
5. Effectuez l'une des actions suivantes :

   - Choisissez Cascade delete (Suppression en cascade) pour supprimer l'IPAM, les portées privées, les groupes dans des portées privées, et les allocations dans des groupes dans des portées privées. Vous ne pouvez pas supprimer l'IPAM avec cette option s'il existe un groupe dans votre portée publique. Si vous utilisez cette option, IPAM effectue les opérations suivantes :
     - Désalloue tous les CIDR alloués aux ressources VPC (tels que les VPC) dans des groupes dans des portées privées.

       > **Note**
       >
       > Aucune ressource VPC n'est supprimée suite à l'activation de cette option. Le CIDR associé à la ressource ne sera plus alloué à partir d'un groupe IPAM, mais le CIDR lui-même restera inchangé.

     - Déprovisionne tous les CIDR IPv4 approvisionnés dans des groupes IPAM dans des portées privées.
     - Supprime tous les groupes IPAM dans des portées privées.
     - Supprime toutes les portées privées par défaut dans l'IPAM.
     - Supprime les portées publiques et privées par défaut et l'IPAM.
   - Si vous ne cochez pas la case Cascade delete (Suppression en cascade), avant de pouvoir utiliser une IPAM, vous devez effectuer les opérations suivantes :
     - Libérer les allocations au sein des groupes IPAM. Pour plus d'informations, consultez Libération d'une allocation.
     - Désactiver des CIDR provisionnés dans des groupes au sein de l'IPAM. Pour plus d'informations, consultez Pour désapprovisionner un CIDR de groupe.
     - Supprimer toutes les portées autres que celles par défaut. Pour plus d'informations, consultez Suppression d'une portée.
     - Supprimer vos groupes IPAM. Pour de plus amples informations, veuillez consulter Suppression d'un groupe.
6. Saisissez **`delete`** (supprimer), puis sélectionnez Delete (Supprimer).

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour supprimer un IPAM :

1. Affichez les IPAM actuels : describe-ipams
2. Supprimez un IPAM : delete-ipam
3. Affichez vos IPAM mises à jour : describe-ipam

Pour créer un nouvel IPAM, consultez Création d'un IPAM.

Suivi de l'utilisation des adresses IP dans IPAM

Les tâches décrites dans cette section sont facultatives. Si vous souhaitez effectuer les tâches de cette section et que vous avez délégué un compte IPAM, les tâches doivent être exécutées par le compte IPAM.

Suivez les étapes décrites dans cette section pour procéder au suivi de l'utilisation des adresses IP avec IPAM.

Table des matières

- Contrôle de l'utilisation des CIDR à l'aide du tableau de bord IPAM
- Contrôle de l'utilisation du CIDR par ressource
- Surveiller l'IPAM avec Amazon CloudWatch
- Afficher l'historique des adresses IP
- Affichage de Public IP Insights

Contrôle de l'utilisation des CIDR à l'aide du tableau de bord IPAM

Suivez les étapes de cette section pour accéder au tableau de bord IPAM et afficher l'état de tous les CIDR dans une portée IPAM particulière.

AWS Management Console

Pour contrôler l'utilisation des CIDR à l'aide du tableau de bord IPAM

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez Dashboard (Tableau de bord).
3. Par défaut, lorsque vous affichez le tableau de bord, la portée privée par défaut est sélectionnée. Si vous ne souhaitez pas utiliser la portée privée par défaut, dans le menu déroulant en haut du panneau de contenu, sélectionnez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Le tableau de bord présente une vue d'ensemble de vos groupes IPAM et de vos CIDR au sein d'une portée. Vous pouvez ajouter, supprimer, redimensionner et déplacer des widgets pour personnaliser le tableau de bord.

- Scope (Portée) : les détails de cette portée. Une portée est le conteneur de niveau le plus élevé d'IPAM. Un IPAM contient deux portées par défaut, une privée et une publique. Chaque portée représente l'espace IP d'un réseau unique. Vous pouvez avoir plusieurs portées privées, mais vous ne pouvez avoir qu'une seule portée publique.
  - Scope ID (ID de la portée) : ID de cette portée.
  - Scope Type (Type de portée) : le type de portée.
  - IPAM ID (ID IPAM) : ID de l'IPAM dans lequel la portée se trouve.
  - Groupes IPAM dans cette portée : l'ID de l'IPAM dans lequel la portée se trouve.
  - Afficher les ressources réseau dans cette portée : permet d'accéder à la section Ressources de la console IPAM.
  - Rechercher dans l'historique d'une adresse IP dans cette portée : permet d'accéder à la section Rechercher dans l'historique des adresses IP de la console IPAM.
- Types de CIDR des ressources : types de CIDR de ressources dans la portée.
  - Sous-réseau : nombre de CIDR pour les sous-réseaux.
  - VPC : nombre de CIDR pour les VPC.
  - EIP : nombre de CIDR pour les adresses IP Elastic.
  - Groupes IPv4 publics : nombre de CIDR pour les groupes IPv4 publics.
- État de gestion : état de gestion des CIDR.
  - Unmanaged CIDRs (CIDR non gérés) : le nombre de CIDR de ressource pour les ressources non gérées dans cette portée.
  - Ignored CIDRs (CIDR ignorés) : le nombre de CIDR de ressource que vous avez choisis de manière à être exemptés de contrôle avec IPAM dans la portée. IPAM n'évalue pas le chevauchement ou la conformité des ressources ignorées dans une portée. Lorsqu'une ressource est choisie pour être ignorée, tout espace qui lui est alloué à partir d'un groupe IPAM est renvoyé au groupe, et la ressource n'est plus importée par importation automatique (si la règle d'allocation d'importation automatique est définie sur le groupe).
  - Managed CIDRs (CIDR gérés) : le nombre de CIDR de ressource pour les ressources gérables (VPC ou groupes IPv4 publics) qui sont alloués à partir d'un groupe IPAM dans la portée.
- CIDR de ressources qui se chevauchent : nombre de CIDR qui se chevauchent et qui ne se chevauchent pas. Le chevauchement des CIDR peut entraîner un routage incorrect dans vos VPC.

    - Overlapping CIDRs (Chevauchement de CIDR) : le nombre de CIDR qui se chevauchent actuellement au sein des groupes IPAM dans cette portée. Le chevauchement des CIDR peut entraîner un routage incorrect dans vos VPC.
    - CIDR qui ne se chevauchent pas : nombre de CIDR de ressources qui ne se chevauchent pas au sein des groupes IPAM de la portée.
- CIDR de ressources conformes : nombre de CIDR de ressources conformes.
    - Compliant CIDRs (CIDR conformes) : le nombre de CIDR de ressource conformes aux règles d'allocation des groupes IPAM dans la portée.
    - Noncompliant CIDRs (CIDR non conformes) : le nombre de CIDR de ressource qui ne sont pas conformes aux règles d'allocation des groupes IPAM dans la portée.
- Statut de chevauchement : nombre de CIDR qui se chevauchent au fil du temps.
    - OverlappingResourceCidrs : nombre de CIDR qui se chevauchent au sein des groupes IPAM dans cette portée. Le chevauchement des CIDR peut entraîner un routage incorrect dans vos VPC.
- Statut de conformité : nombre de CIDR conformes et non conformes aux règles d'allocation des groupes IPAM dans la portée au fil du temps.
    - CompliantResourceCidrs : nombre de CIDR de ressources conformes aux règles d'allocation.
    - NoncompliantResourceCidrs : nombre de CIDR de ressources non conformes aux règles d'allocation.
- Utilisation du VPC : VPC (IPv4 et IPv6) avec l'utilisation IP la plus élevée ou la plus faible. Vous pouvez utiliser ces informations pour configurer des alarmes Amazon CloudWatch afin d'être alerté en cas de dépassement d'un seuil d'utilisation IP. Pour de plus amples informations, veuillez consulter Métriques d'utilisation des ressources.
- Utilisation du sous-réseau : sous-réseaux (IPv4 uniquement) avec l'utilisation IP la plus élevée ou la plus faible. Vous pouvez utiliser ces informations pour décider si vous souhaitez conserver ou supprimer les ressources sous-utilisées. Pour de plus amples informations, veuillez consulter Métriques d'utilisation des ressources.
- VPC ayant le plus grand nombre d'adresses IP allouées : VPC dont le pourcentage d'espace d'adressage IP alloué aux sous-réseaux est le plus élevé. Cela est utile pour vous indiquer si vous devez allouer un espace d'adressage IP supplémentaire aux VPC.
- Sous-réseaux ayant le plus grand nombre d'adresses IP allouées : sous-réseaux dont le pourcentage d'espace d'adressage IP alloué aux ressources est le plus élevé. Cela est utile

pour vous indiquer si vous devez allouer un espace d'adressage IP supplémentaire aux sous-réseaux.

- Affectation de groupe : pourcentage d'espace IP affecté aux ressources et aux allocations manuelles dans la portée au fil du temps.
- Allocation de groupe : pourcentage de l'espace IP d'un groupe qui a été alloué à d'autres groupes de la portée au fil du temps.

Command line

Les informations affichées dans le tableau de bord proviennent de métriques stockées dans Amazon CloudWatch. Pour plus d'informations sur les métriques stockées dans Amazon CloudWatch, consultez Surveiller l'IPAM avec Amazon CloudWatch. Utilisez les options Amazon CloudWatch dans la Référence de l'AWS CLI pour afficher les métriques des allocations dans vos groupes et portées IPAM.

Si vous constatez que le CIDR provisionné pour un groupe est presque entièrement alloué, vous devrez peut-être provisionner des CIDR supplémentaires. Pour plus d'informations, consultez Approvisionnement de CIDR à un groupe.

Contrôle de l'utilisation du CIDR par ressource

Dans IPAM, une ressource désigne entité de service AWS qui se voit attribuer une adresse IP ou un bloc d'adresse CIDR. IPAM gère certaines ressources, mais contrôle uniquement d'autres ressources.

- Ressource gérée : un CIDR est alloué à une ressource gérée à partir d'un groupe IPAM. IPAM contrôle le CIDR pour détecter le chevauchement potentiel d'adresses IP avec d'autres CIDR du groupe, et contrôle la conformité du CIDR aux règles d'allocation d'un groupe. IPAM prend en charge les types de ressources suivants :
  - VPC
  - Groupes IPv4 publics

> **Important**
>
> Les groupes IPv4 publics et IPAM sont gérés par des ressources distinctes dans AWS. Les groupes IPv4 publics sont des ressources de compte unique qui vous permettent de

convertir vos CIDR publics en adresses IP Elastic. Les groupes IPAM vous permettent d'allouer votre espace public à des groupes IPv4 publics.

- Ressource contrôlée : si une ressource est contrôlée par IPAM, la ressource a été détectée par IPAM et vous pouvez afficher des détails sur le CIDR de la ressource lorsque vous utilisez `get-ipam-resource-cidrs` avec l'AWS CLI, ou lorsque vous consultez Resources (Ressources) dans le panneau de navigation. IPAM prend en charge le contrôle des ressources suivantes :
  - VPC
  - Groupes IPv4 publics
  - Sous-réseaux VPC
  - Adresses IP élastiques

Les étapes suivantes vous montrent comment contrôler l'utilisation du CIDR et la conformité aux règles d'allocation par ressource.

AWS Management Console

Pour contrôler l'utilisation du CIDR par ressource

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez Resources (Ressources).
3. Dans le menu déroulant se trouvant dans la partie supérieure du panneau de contenu, sélectionnez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Utilisez la carte CIDR des ressources pour afficher l'espace d'adresses IP disponible, alloué et superposé dans une portée :
   - Disponible : une plage d'adresses IP est disponible pour l'allocation.
   - Conforme et sans chevauchement : une plage d'adresses IP est allouée à une ressource gérée par IPAM.
   - Occupé : une plage d'adresses IP est allouée à une ressource.
   - Chevauchement : une plage d'adresses IP a été allouée à plusieurs ressources et est en chevauchement.
   - Non conforme : une plage d'adresses IP n'est pas conforme. Une ressource utilisant la plage d'adresses IP n'est pas conforme aux règles d'allocation définies pour le groupe.

Dans la carte CIDR, choisissez un bloc d'adresses IP en bas pour afficher les ressources dans des blocs CIDR plus petits. Choisissez un bloc d'adresses IP en haut de la carte pour afficher les ressources dans des blocs CIDR plus grands.

5. Dans le tableau, vous pouvez afficher les détails suivants concernant les ressources de la portée :

   - Name (Resource ID) (Nom (ID de ressource)) : nom et identifiant de la ressource.
   - CIDR : le CIDR associé à la ressource.
   - Management state (État de gestion) : état de la ressource.
     - Managed (Géré) : la ressource dispose d'un CIDR alloué à partir d'un groupe IPAM et est contrôlée par IPAM afin de vérifier le chevauchement CIDR potentiel et la conformité aux règles d'allocation de groupe.
     - Unmanaged (Non géré) : la ressource ne dispose pas d'un CIDR alloué à partir d'un groupe IPAM et IPAM ne contrôle pas la conformité potentielle du CIDR aux règles d'allocation de groupe. Le CIDR est contrôlé pour détecter les chevauchements.
     - Ignored (Ignoré) : la ressource a été choisie de manière à être exemptée de contrôle. Les ressources ignorées ne sont pas évaluées pour détecter les chevauchements ou vérifier la conformité aux règles d'allocation. Si une ressource est choisie pour être ignorée, tout espace qui lui est alloué à partir d'un groupe IPAM est renvoyé au groupe et la ressource ne sera plus importée via l'importation automatique (si la règle d'allocation d'importation automatique est définie sur le groupe).
     - - : cette ressource ne fait pas partie des types de ressources qu'IPAM peut gérer.
   - Compliance status (Statut de conformité) : statut de conformité du CIDR.
     - Compliant (Conforme) : une ressource gérée est conforme aux règles d'allocation du groupe IPAM.
     - Noncompliant (Non conforme) : le CIDR de ressource n'est pas conforme à au moins une des règles d'allocation du groupe IPAM.

       Example

       Si un VPC possède un CIDR qui ne répond pas aux paramètres de longueur du masque réseau du groupe IPAM, ou si la ressource ne se trouve pas dans la même Région AWS que le groupe IPAM, le CIDR sera signalé comme non conforme.

  - Unmanaged (Non géré) : aucun CIDR n'est alloué à la ressource à partir d'un groupe IPAM et l'IPAM ne contrôle pas la conformité CIDR potentielle de la ressource aux règles d'allocation de groupe. Le CIDR est contrôlé pour détecter les chevauchements.
  - Ignored (Ignoré) : la ressource a été choisie de manière à être exemptée de contrôle. Les ressources ignorées ne sont pas évaluées pour détecter les chevauchements ou vérifier la conformité aux règles d'allocation. Si une ressource est choisie pour être ignorée, tout espace qui lui est alloué à partir d'un groupe IPAM est renvoyé au groupe et la ressource ne sera plus importée via l'importation automatique (si la règle d'allocation d'importation automatique est définie sur le groupe).
  - - : cette ressource ne fait pas partie des types de ressources qu'IPAM peut gérer.
- Overlap status (Statut de chevauchement) : statut de chevauchement du CIDR.
  - Nonoverlapping (Aucun chevauchement) : il n'existe aucun chevauchement entre le CIDR de ressource et un autre CIDR de la même portée.
  - Overlapping (Chevauchement) : il existe un chevauchement entre le CIDR de ressource et un autre CIDR de la même portée. Notez que si un CIDR de ressource présente un chevauchement, celui-ci peut concerner une allocation manuelle.
  - Ignored (Ignoré) : la ressource a été choisie de manière à être exemptée de contrôle. L'IPAM n'évalue pas le chevauchement ni la conformité aux règles d'allocation des ressources ignorées. Si une ressource est choisie pour être ignorée, tout espace qui lui est alloué à partir d'un groupe IPAM est renvoyé au groupe et la ressource ne sera plus importée via l'importation automatique (si la règle d'allocation d'importation automatique est définie sur le groupe).
  - - : cette ressource ne fait pas partie des types de ressources qu'IPAM peut gérer.
- Utilisation de l'IP : pour les ressources qui constituent des VPC, il s'agit du pourcentage d'espace d'adresse IP dans le VPC qui est occupé par les CIDR de sous-réseau. Pour les ressources qui constituent des sous-réseaux, si un CIDR IPv4 est provisionné pour le sous-réseau, il s'agit du pourcentage d'espace d'adressage IPv4 dans le sous-réseau utilisé. Si un CIDR IPv6 est provisionné pour le sous-réseau, le pourcentage d'espace d'adressage IPv6 utilisé n'est pas représenté. Le pourcentage d'espace d'adressage IPv6 utilisé ne peut pas être calculé pour le moment. Pour les ressources qui sont des groupes IPv4 publics, il s'agit du pourcentage d'espace d'adressage IP dans le groupe qui a été alloué aux adresses IP Elastic (EIP).
- Region (Région) : la Région AWS de la ressource.

- ID propriétaire : l'ID de compte AWS de la personne qui a créé cette ressource.
- Type de ressource : si la ressource est un VPC, un sous-réseau, une adresse IP Elastic ou un groupe IPv4 public.
- ID du groupe : ID du groupe IPAM dans lequel la ressource se trouve.

6. Utilisez Filtrer les ressources pour filtrer le tableau des ressources par propriété de colonne, telle que l'ID VPC ou le statut de conformité.

Command line

Les commandes de cette section renvoient vers la documentation de référence de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

Utilisez les commandes AWS CLI suivantes pour contrôler l'utilisation du CIDR par ressource :

1. Obtenez l'ID de portée : describe-ipam-scopes
2. Demandez des informations sur les ressources : get-ipam-resource-cidrs

Surveiller l'IPAM avec Amazon CloudWatch

IPAM stocke automatiquement les métriques associées à l'utilisation des adresses IP (telles que l'espace d'adressage IP disponible dans vos groupes IPAM et le nombre de CIDR de ressource conformes aux règles d'allocation) et à l'utilisation des ressources dans l'espace de noms Amazon CloudWatch `AWS/IPAM` dans la région d'origine de votre IPAM.

Table des matières

- Métriques relatives aux groupes et champs d'application IPAM
- Métriques d'utilisation des ressources

Métriques relatives aux groupes et champs d'application IPAM

IPAM publie des données concernant vos groupes et champs d'application IPAM sur Amazon CloudWatch. Vous pouvez utiliser ces métriques pour créer des alarmes pour les groupes IPAM afin de vous avertir si les groupes d'adresses sont presque épuisés ou si les ressources ne sont pas conformes aux règles d'allocation définies sur un groupe. La création d'alarmes et la définition des

notifications avec Amazon CloudWatch ne fait pas partie de cette section. Pour plus d'informations, consultez Utilisation des alarmes Amazon CloudWatch dans le Guide de l'utilisateur Amazon CloudWatch.

Les métriques et dimensions qu'IPAM envoie à Amazon CloudWatch sont répertoriées ci-dessous.

Métriques de groupes IPAM

Nom des métriques	Description
CompliantResourceCidrs	Le nombre de CIDR de ressource gérés conformes aux règles d'allocation du groupe IPAM. Pour plus d'informations sur les règles d'allocations, consultez Création d'un groupe IPv4 de niveau supérieur.
NoncompliantResourceCidrs	Le nombre de CIDR de ressource gérés non conformes aux règles d'allocation du groupe IPAM. Pour plus d'informations sur les règles d'allocations, consultez Création d'un groupe IPv4 de niveau supérieur.
PercentAllocated	Le pourcentage de l'espace IP d'un groupe qui a été alloué à d'autres groupes.
PercentAssigned	Le pourcentage d'un espace IP de groupe qui a été alloué aux ressources, y compris les allocations manuelles.
PercentAvailable	Le pourcentage de l'espace IP d'un groupe qui n'a pas été alloué à d'autres groupes ou ressources.

Métriques de champs d'application IPAM

Nom des métriques	Description
CompliantResourceCidrs	Le nombre de CIDR de ressource conformes aux règles d'allocation des groupes IPAM dans la portée.
ManagedResourceCidrs	Le nombre de CIDR de ressource pour les ressources gérables (VPC ou groupes IPv4 publics) qui sont alloués à partir d'un groupe IPAM dans la portée.

Nom des métriques	Description
NoncompliantResourceCidrs	Le nombre de CIDR de ressource qui ne sont pas conformes aux règles d'allocation des groupes IPAM dans la portée.
OverlappingResourceCidrs	Le nombre de CIDR de ressource qui se chevauchent au sein de la portée.
UnmanagedResourceCidrs	Le nombre de CIDR de ressources dans le champ d'application qui sont actuellement associés à des ressources gérables mais qui ne sont pas gérés par IPAM.

Les dimensions que vous pouvez utiliser pour filtrer les métriques IPAM figurent ci-dessous.

Dimension	Description
AddressFamily	La famille d'adresses IP pour les CIDR ressource (IPv4 ou IPv6).
Paramètre régional	La Région AWS où un groupe IPAM est disponible pour les allocations.
PoolID	L'identifiant d'un groupe.
ScopeID	L'identifiant d'une portée.

Pour plus d'informations sur la surveillance des VPC avec Amazon CloudWatch, consultez Métriques CloudWatch pour vos VPC dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Métriques d'utilisation des ressources

IPAM publie des métriques d'utilisation IP pour les ressources qu'il surveille sur Amazon CloudWatch. Ces ressources comprennent :

- Les VPC (IPv4 et IPv6)
- Les sous-réseaux (IPv4)
- Groupes IPv4 publics

L'IPAM calcule et publie les métriques d'utilisation IP séparément par famille d'adresses IP (IPv4 ou IPv6). L'utilisation IP d'une ressource est calculée sur tous ses CIDR de la même famille d'adresses.

Pour chaque combinaison de type de ressource et de famille d'adresses, IPAM utilise trois règles pour déterminer les métriques à publier :

- Jusqu'à 50 ressources avec le taux d'utilisation IP le plus élevé. Vous pouvez utiliser ces informations pour configurer des alarmes afin d'être alerté en cas de dépassement d'un seuil d'utilisation IP.
- Jusqu'à 50 ressources avec le taux d'utilisation IP le plus faible. Vous pouvez utiliser ces informations pour décider si vous souhaitez conserver ou supprimer les ressources sous-utilisées.
- Jusqu'à 50 autres ressources. Vous pouvez utiliser ces informations pour suivre de manière cohérente l'utilisation IP des ressources qui peuvent ne pas être capturées au sein du groupe d'utilisation élevée ou faible.
  - Jusqu'à 50 VPC contenant un CIDR alloué à partir d'un groupe IPAM (hiérarchisé en fonction de la taille totale des blocs d'adresse CIDR).
  - Jusqu'à 50 sous-réseaux dont le VPC contient un CIDR alloué à partir d'un groupe IPAM (hiérarchisé en fonction de la taille totale des blocs d'adresse CIDR).
  - Jusqu'à 50 groupes IPv4 publics contenant un CIDR alloué à partir d'un groupe IPAM (hiérarchisé en fonction de la taille totale des blocs d'adresse CIDR).

Après l'application de chaque règle, les métriques sont agrégées et publiées sous le même nom de métrique pour chaque type de ressource. Vous trouverez ci-dessous des informations détaillées sur les noms des métriques et leurs dimensions.

> **Important**
>
> Il existe une limite unique pour chaque type de ressource, famille d'adresses et combinaison de règles. La valeur par défaut de chaque limite est 50. Vous pouvez ajuster ces limites en contactant le Centre de support AWS tel que décrit dans la section Quotas de service AWS dans la Références générales AWS.

Example Exemple

Supposons que votre IPAM surveille 2 500 VPC et 10 000 sous-réseaux, tous avec des CIDR IPv4 et IPv6. L'IPAM publie les métriques d'utilisation IP suivantes :

- Jusqu'à 150 métriques pour l'utilisation de l'adresse IP IPv4 des VPC, notamment :
  - Les 50 VPC avec le taux d'utilisation IP IPv4 le plus élevé
  - Les 50 VPC avec le taux d'utilisation IPv4 le plus faible
  - Jusqu'à 50 VPC contenant un CIDR IPv4 alloué à partir d'un groupe IPAM
- Jusqu'à 150 métriques pour l'utilisation IPv6 des VPC, notamment :
  - Les 50 VPC avec le taux d'utilisation IP IPv6 le plus élevé
  - Les 50 VPC avec le taux d'utilisation IPv6 le plus faible
  - Jusqu'à 50 VPC contenant un CIDR IPv6 alloué à partir d'un groupe IPAM
- Jusqu'à 150 métriques pour l'utilisation IPv4 des sous-réseaux, notamment :
  - Les 50 sous-réseaux avec le taux d'utilisation IP IPv4 le plus élevé
  - Les 50 sous-réseaux avec le taux d'utilisation IP IPv4 le plus faible
  - Jusqu'à 50 sous-réseaux dont le VPC contient un CIDR IPv4 alloué à partir d'un groupe IPAM

Métriques VPC

Le nom et la description de la métrique VPC sont répertoriés ci-dessous.

Nom des métriques	Description
VpcIPUsage	Le nombre total d'adresses IP couvertes par les CIDR dans les sous-réseaux du VPC divisé par le nombre total d'adresses IP couvertes par les CIDR dans le VPC. Ce nombre est calculé pour tous les CIDR de VPC du même champ d'application IPAM et séparément pour les CIDR IPv4 et IPv6.

Les dimensions que vous pouvez utiliser pour filtrer les métriques VPC figurent ci-dessous.

Dimension	Description
AddressFamily	La famille d'adresses IP pour les CIDR ressource (IPv4 ou IPv6).
OwnerID	L'ID du propriétaire du VPC.
Région	La Région AWS où se trouve le VPC.

Dimension	Description
ScopeID	L'ID du champ d'application IPAM auquel appartient le VPC.
VpcID	ID du VPC.

Métriques du sous-réseau

Le nom et la description de la métrique du sous-réseau sont répertoriés ci-dessous.

Nom des métriques	Description
SubnetIPUsage	Le nombre d'adresses IP actives divisé par le nombre total d'adresses IP dans le CIDR IPv4 du sous-réseau.

Les dimensions que vous pouvez utiliser pour filtrer les métriques de sous-réseau figurent ci-dessous.

Dimension	Description
AddressFamily	La famille d'adresses IP pour les CIDR de ressource (IPv4 uniquement).
OwnerID	L'ID du propriétaire du sous-réseau.
Région	La Région AWS où se trouve le sous-réseau.
ScopeID	L'ID du champ d'application IPAM auquel appartient le sous-réseau.
SubnetID	ID du sous-réseau.
VpcID	L'ID du VPC auquel appartient le sous-réseau.

Métriques du groupe IPv4 public

Le nom et la description de la métrique du groupe IPv4 public sont répertoriés ci-dessous.

Nom des métriques	Description
PublicIPv4PoolIPUsage	Le nombre d'EIP du groupe IPv4 public divisé par le nombre total d'adresses IP du groupe.

Les dimensions que vous pouvez utiliser pour filtrer les métriques du groupe IPv4 public figurent ci-dessous.

Dimension	Description
OwnerID	L'ID du propriétaire du groupe IPv4 public.
PublicIPv4PoolID	L'ID du groupe IPv4 public.
Région	La Région AWS dans laquelle se trouve le groupe IPv4 public.
ScopeID	L'ID du champ d'application IPAM auquel appartient le groupe IPv4 public.

Métriques Public IP insight

Les noms et les descriptions des métriques Public IP Insights sont répertoriés ci-dessous.

Nom des métriques	Description
AmazonOwnedElasticIPs	Le nombre d'adresses IP Elastic détenues par Amazon que vous avez provisionnées ou attribuées à des ressources dans votre compte AWS.
AssociatedAmazonOwnedElasticIPs	Le nombre d'adresses IP Elastic détenues par Amazon que vous avez associées aux ressources dans votre compte AWS.
AssociatedBringYourOwnIPs	Le nombre d'adresses IPv4 publiques que vous avez transférées vers AWS en utilisant Fourniture de vos propres adresses IP (BYOIP) et que vous avez associées à des ressources dans votre compte AWS.

Nom des métriques	Description
BringYourOwnIPs	Le nombre d'adresses IPv4 publiques que vous avez transféré es vers AWS en utilisant Fourniture de vos propres adresses IP (BYOIP).
EC2PublicIPs	Le nombre d'adresses IPv4 publiques attribuées à des instances EC2 lorsque les instances ont été lancées dans un sous-rése au par défaut ou dans un sous-réseau configuré pour attribuer automatiquement une adresse IPv4 publique.
ServiceManagedBrin gYourOwnIPs	Le nombre d'adresses IPv4 publiques que vous avez transféré es vers AWS en utilisant Fourniture de vos propres adresses IP (BYOIP) qui sont provisionnées et gérées par un service AWS.
ServiceManagedIPs	Le nombre d'adresses IPv4 publiques provisionnées et gérées par un service AWS.
UnassociatedAmazon OwnedElasticIPs	Le nombre d'adresses IP Elastic détenues par Amazon que vous n'avez pas associées aux ressources dans votre compte AWS.
UnassociatedBringY ourOwnIPs	Le nombre d'adresses IPv4 publiques que vous avez transféré es vers AWS en utilisant Fourniture de vos propres adresses IP (BYOIP) et que vous n'avez pas associées à des ressources dans votre compte AWS.

Les dimensions que vous pouvez utiliser pour filtrer les métriques public IP Insight figurent ci-dessous.

Dimension	Description
IpamId	L’ID de l’IPAM auquel appartient l’adresse IP.
Région	La région AWS dans laquelle se trouve l’adresse IP publique.

Astuce rapide pour créer des alarmes

Pour créer rapidement une alarme Amazon CloudWatch pour les ressources présentant un taux d'utilisation élevé des adresses IP, ouvrez la console CloudWatch, choisissez Métriques, Toutes les métriques, choisissez l'onglet Requête, choisissez le `AWS/IPAM > VPC IP Usage Metrics`, `AWS/IPAM > Subnet IP Usage Metrics` ou `AWS/IPAM > Public IPv4 Pool IP Usage Metrics` de l'Espace de noms, choisissez le `MAX(VpcIPUsage)`, `MAX(SubnetIPUsage)` ou `MAX(PublicIPv4PoolIPUsage)` du Nom de la métrique, et sélectionnez Créer une alarme. Pour plus d'informations, veuillez consulter la rubrique Création d'alarmes sur les requêtes Metrics Insights dans le Guide de l'utilisateur Amazon CloudWatch.

Afficher l'historique des adresses IP

Suivez les étapes de cette section pour afficher l'historique d'une adresse IP ou d'un CIDR dans une portée IPAM. Vous pouvez utiliser les données historiques pour analyser et auditer vos politiques de routage et de sécurité réseau. IPAM retient automatiquement les données de surveillance des adresses IP pendant trois ans maximum.

Vous pouvez utiliser les données historiques d'IP pour rechercher le changement d'état des adresses IP ou des CIDR pour les types de ressources suivants :

- VPC
- Sous-réseaux VPC
- Adresses IP élastiques
- Instances EC2
- Interfaces réseau EC2 connectées à des instances

> **Important**
>
> Bien qu'IPAM ne contrôle pas les instances Amazon EC2 ou les interfaces réseau EC2 qui sont reliées aux instances, vous pouvez utiliser la fonction d'historique de recherche d'IP pour rechercher des données historiques sur des CIDR d'interface réseau et d'instance EC2.

Note

- Si vous déplacez une ressource d'une portée IPAM à une autre, l'enregistrement d'historique précédent se termine et un nouvel enregistrement d'historique est créé sous la nouvelle portée. Pour plus d'informations, consultez Déplacez des CIDR VPC entre les portées.
- Si vous supprimez ou transférez une ressource vers un AWS compte qui n'est pas surveillé par votre IPAM, tout nouvel historique lié à la ressource ne sera pas visible et votre IPAM ne surveillera pas la ressource. L'adresse IP de la ressource sera toutefois toujours consultable.
- Si vousIntégration d'IPAM à des comptes extérieurs à votre organisation, le propriétaire de l'IPAM, pouvez consulter l'historique des adresses IP de tous les CIDR de ressources appartenant à ces comptes.

AWS Management Console

Pour afficher l'historique d'un CIDR

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, sélectionnez Historique de recherche d'IP.
3. Saisissez une adresse IP IPv4 ou IPv6 ou un CIDR. Il doit s'agir d'un CIDR spécifique à la ressource.
4. Choisissez un ID de portée IPAM.
5. Choisissez une plage de dates et d'heures.
6. Si vous souhaitez filtrer les résultats par VPC, saisissez un ID de VPC. Utilisez cette option si le CIDR apparaît dans plusieurs VPC.
7. Choisissez Rechercher.

Command line

Les commandes de cette section contiennent un lien vers la documentation de référence d'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Consultez l'historique d'un CIDR : get-ipam-address-history

Pour voir des exemples de la façon dont vous pouvez utiliser l'AWS CLIpour analyser et auditer l'utilisation des adresses IP, voir Didacticiel : afficher l'historique des adresses IP à l'aide du AWS CLI.

Les résultats de la recherche sont organisés dans les colonnes suivantes :

- Sampled end time (Heure de fin échantillonnée) : heure de fin échantillonnée de l'association entre la ressource et le CIDR dans la portée IPAM. Les modifications sont relevées dans des instantanés périodiques. Par conséquent, l'heure de fin peut s'être produite avant cette heure spécifique.
- Sampled start time (Heure de début échantillonnée) : heure de début échantillonnée de l'association entre la ressource et le CIDR dans la portée IPAM. Les modifications sont relevées dans des instantanés périodiques. Par conséquent, l'heure de début peut s'être produite avant cette heure spécifique.

  Example

  Pour expliquer les heures indiquées sous Sampled start time (Heure de début échantillonnée) et Sampled end time (Heure de fin échantillonnée), examinons un exemple de cas d'utilisation :

  À 14 h, un VPC a été créé avec le CIDR 10.0.0.0/16. À 15 h, vous créez un IPAM et un groupe IPAM avec le CIDR 10.0.0.0/8, puis vous sélectionnez l'option d'importation automatique pour autoriser l'IPAM à découvrir et à importer tous les CIDR compris dans la plage d'adresses IP 10.0.0.0/8. Étant donné que l'IPAM détecte les modifications apportées aux CIDR dans des instantanés périodiques, il ne détecte pas le CIDR de VPC existant avant 15 h 05. Lorsque vous recherchez l'ID de ce VPC à l'aide de la fonction d'historique de recherche d'IP, l'heure de début échantillonnée pour votre VPC indique 15 h 05, ce qui correspond au moment où l'IPAM a découvert le VPC, et non 14 h, à savoir l'heure de création du VPC. Imaginons maintenant que vous décidiez de supprimer le VPC à 17 h. Lorsque le VPC est supprimé, le CIDR 10.0.0.0/16 qui a été alloué au VPC est recyclé dans le groupe IPAM. L'IPAM prend un instantané périodique à 17 h 05 et découvre le changement. Lorsque vous recherchez l'ID de ce VPC dans l'historique de recherche d'IP, l'heure de fin échantillonnée pour le CIDR du VPC indique 17 h 05, et non 17 h, heure à laquelle le VPC a été supprimé.
- Resource ID (ID de ressource) : ID généré lorsque la ressource a été associée au CIDR.
- Name (Nom) : nom de la ressource (le cas échéant).
- Compliance status (Statut de conformité) : statut de conformité du CIDR.

- Compliant (Conforme) : une ressource gérée est conforme aux règles d'allocation du groupe IPAM.
- Noncompliant (Non conforme) : le CIDR de ressource n'est pas conforme à au moins une des règles d'allocation du groupe IPAM.

  Example

  Si un VPC possède un CIDR qui ne répond pas aux paramètres de longueur du masque réseau du groupe IPAM, ou si la ressource ne se trouve pas dans la même Région AWS que le groupe IPAM, le CIDR sera signalé comme non conforme.
- Unmanaged (Non géré) : aucun CIDR n'est alloué à la ressource à partir d'un groupe IPAM et l'IPAM ne contrôle pas la conformité CIDR potentielle de la ressource aux règles d'allocation de groupe. Le CIDR est contrôlé pour détecter les chevauchements.
- Ignored (Ignoré) : la ressource gérée a été choisie pour être exemptée de surveillance. Les ressources ignorées ne sont pas évaluées pour détecter les chevauchements ou vérifier la conformité aux règles d'allocation. Si une ressource est choisie pour être ignorée, tout espace qui lui est alloué à partir d'un groupe IPAM est renvoyé au groupe et la ressource ne sera plus importée via l'importation automatique (si la règle d'allocation d'importation automatique est définie sur le groupe).
- - : cette ressource ne fait pas partie des types de ressources qu'IPAM peut contrôler ou gérer.

- Overlap status (Statut de chevauchement) : statut de chevauchement du CIDR.
  - Nonoverlapping (Aucun chevauchement) : il n'existe aucun chevauchement entre le CIDR de ressource et un autre CIDR de la même portée.
  - Overlapping (Chevauchement) : il existe un chevauchement entre le CIDR de ressource et un autre CIDR de la même portée. Notez que si un CIDR de ressource présente un chevauchement, celui-ci peut concerner une allocation manuelle.
  - Ignored (Ignoré) : la ressource gérée a été choisie pour être exemptée de surveillance. L'IPAM n'évalue pas le chevauchement ni la conformité aux règles d'allocation des ressources ignorées. Si une ressource est choisie pour être ignorée, tout espace qui lui est alloué à partir d'un groupe IPAM est renvoyé au groupe et la ressource ne sera plus importée via l'importation automatique (si la règle d'allocation d'importation automatique est définie sur le groupe).
  - - : cette ressource ne fait pas partie des types de ressources qu'IPAM peut contrôler ou gérer.
- Type de ressource
  - vpc : le CIDR est associé à un VPC.
  - subnet (sous-réseau) : le CIDR est associé au sous-réseau d'un VPC.

  - eip : le CIDR est associé à une adresse IP élastique.
  - instance : le CIDR est associé à une instance EC2.
  - network-interface (interface réseau) : le CIDR est associé à une interface réseau.
- VPC ID (ID du VPC) : ID du VPC auquel cette ressource appartient (le cas échéant).
- Region (Région) : la Région AWS de cette ressource.
- Owner ID (ID du propriétaire) : l'ID du compte AWS de l'utilisateur qui a créé cette ressource (le cas échéant).

Affichage de Public IP Insights

Une adresse IPv4 publique est une adresse IPv4 qui est routable depuis Internet. Une adresse IPv4 publique est nécessaire pour qu'une ressource soit directement accessible depuis Internet via IPv4.

> **Note**
>
> AWS frais pour toutes les adresses IPv4 publiques, y compris les adresses IPv4 publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique de la page de tarification d'Amazon VPC.

Vous pouvez consulter des informations sur les types d'adresses IPv4 publiques suivants :

- Adresses IP élastiques (EIP) : adresses IPv4 publiques statiques fournies par Amazon que vous pouvez associer à une instance EC2, à une interface réseau élastique ou à une ressource. AWS
- Adresses IPv4 publiques EC2 : adresses IPv4 publiques attribuées à une instance EC2 par Amazon (si l'instance EC2 est lancée dans un sous-réseau par défaut ou si l'instance est lancée dans un sous-réseau configuré pour attribuer automatiquement une adresse IPv4 publique).
- Adresses BYOIPv4 : adresses IPv4 publiques de la plage d'adresses IPv4 que vous avez introduites à l' AWS aide de Bring your own IP addresses (BYOIP).
- Adresses IPv4 gérées par le service : adresses IPv4 publiques automatiquement provisionnées sur les AWS ressources et gérées par un service. AWS Par exemple, les adresses IPv4 publiques sur Amazon ECS, Amazon RDS ou Amazon. WorkSpaces

Vous pouvez utiliser Public IP Insights pour obtenir les informations suivantes :

- Si votre IPAM est intégré aux comptes d'une AWS organisation, vous pouvez consulter toutes les adresses IPv4 publiques utilisées par les services dans toutes les AWS régions pour l'ensemble AWS de votre organisation.
- Si votre IPAM est intégré à un seul compte, vous pouvez consulter toutes les adresses IPv4 publiques utilisées par les services dans toutes les AWS régions dans votre compte.

Public IP Insights affichent toutes les adresses IPv4 publiques utilisées par les services dans les régions. Vous pouvez utiliser ces informations pour identifier l'utilisation des adresses IPv4 publiques et consulter des recommandations pour publier les adresses IP Elastic non utilisées.

- Types d'adresses IP publiques : le nombre d'adresses IPv4 publiques organisées par type.
  - EIP appartenant à Amazon : adresses IP élastiques que vous avez provisionnées ou attribuées aux ressources de votre compte. AWS
  - Adresses IP publiques EC2 : adresses IPv4 publiques attribuées à des instances EC2 lorsque les instances ont été lancées dans un sous-réseau par défaut ou dans un sous-réseau configuré pour attribuer automatiquement une adresse IPv4 publique.
  - BYOIP : adresses IPv4 publiques que vous avez introduites à AWS l'aide de Bring your own IP addresses (BYOIP).
  - IP gérées par le service : adresses IPv4 publiques fournies et gérées par un AWS service.
- Utilisation d'EIP : le nombre d'adresses IP Elastic organisées selon leur utilisation.
  - EIP associées appartenant à Amazon : adresses IP élastiques que vous avez configurées dans votre AWS compte et que vous avez associées à une instance, une interface réseau ou une ressource EC2. AWS
  - BYOIP associé : adresses IPv4 publiques que vous avez introduites à AWS l'aide du BYOIP et que vous avez associées à une interface réseau.
  - EIP appartenant à Amazon non associés : adresses IP élastiques que vous avez configurées dans votre AWS compte mais que vous n'avez associées à aucune interface réseau.
  - BYOIP non associé : adresses IPv4 publiques que vous avez utilisées pour AWS utiliser BYOIP mais que vous n'avez associées à aucune interface réseau.
- Adresses IP publiques : un tableau des adresses IPv4 publiques et de leurs attributs.
  - Adresse IP : l'adresse IPv4 publique.
  - Associé : indique si l'adresse est associée ou non à une instance EC2, à une interface réseau ou à une AWS ressource.

  - Associé : l'adresse IPv4 publique est associée à une instance EC2, à une interface réseau ou AWS à une ressource.
  - Non associée : l'adresse IPv4 publique n'est associée à aucune ressource et est inactive dans votre AWS compte.
- Type d'adresse : le type d'adresse IP.
  - EIP détenue par Amazon : l'adresse IPv4 publique est une adresse IP Elastic.
  - BYOIP : L'adresse IPv4 publique a été amenée à AWS utiliser BYOIP.
  - IP publique EC2 : l'adresse IPv4 publique a été attribuée automatiquement à une instance EC2.
  - Service géré par BYOIP : l'adresse IPv4 publique a été introduite à AWS l'aide de Bring your own IP (BYOIP).
  - IP gérée par le service : l'adresse IPv4 publique a été fournie et est gérée par un AWS service.
- Service : le service auquel l'adresse IP est associée.
  - AGA : Un AWS Global Accelerator. Si un accélérateur de routage personnalisé est utilisé, ses adresses IP publiques ne sont pas répertoriées. Pour consulter ces adresses IP publiques, consultez la section Affichage de vos accélérateurs de routage personnalisés.
  - Service de migration de base de données : instance de réplication AWS Database Migration Service (DMS).
  - Redshift : un cluster Amazon Redshift.
  - RDS : une instance Amazon Relational Database Service (RDS).
  - Équilibreur de charge (EC2) : un Application Load Balancer ou un Network Load Balancer.
  - Passerelle NAT (VPC) : une passerelle NAT publique Amazon VPC.
  - VPN de site à site : passerelle privée virtuelle. AWS Site-to-Site VPN
  - Autre : autre service qui n'est pas identifiable actuellement.
- Nom (ID EIP) : si cette adresse IPv4 publique est une allocation d'adresse IP Elastic, il s'agit du nom et de l'ID de l'allocation EIP.
- ID d'interface réseau : si cette adresse IPv4 publique est associée à une interface réseau, il s'agit de l'ID de l'interface réseau.
- ID d'instance : si cette adresse IPv4 publique est associée à une instance EC2, il s'agit de l'ID de l'instance.
- Groupes de sécurité : si cette adresse IPv4 publique est associée à une instance EC2, il s'agit du nom et de l'ID du groupe de sécurité attribué à l'instance.

- Groupe IPv4 public : s'il s'agit d'une adresse IP Elastic issue d'un groupe d'adresses IP détenu et géré par Amazon, la valeur est « - ». S'il s'agit d'une adresse IP Elastic issue d'une plage d'adresses IP que vous possédez et que vous avez apportée à Amazon (à l'aide de BYOIP), la valeur est l'ID du groupe IPv4 public.
- Groupe frontalier du réseau : si l'adresse IP est annoncée, il s'agit de la AWS région à partir de laquelle l'adresse IP est annoncée.
- ID du propriétaire : AWS numéro de compte du propriétaire de la ressource.
- Temps d'échantillonnage : heure de la dernière découverte de ressources réussie.
- ID de découverte de ressource : ID de la découverte de ressource qui a découvert cette adresse IPv4 publique.
- Ressource de service : ARN ou ID de ressource.

Si une adresse IP Elastic est attribuée à votre compte, mais qu'elle n'est pas associée à une interface réseau, une bannière s'affiche pour vous informer que votre compte possède des EIP non associées et que vous devez les publier.

> **Important**
>
> Public IP Insights a récemment été mis à jour. Si vous voyez une erreur liée au fait que vous ne disposez pas des autorisations nécessaires pour appeler GetIpamDiscoveredPublicAddresses, l'autorisation gérée associée à une découverte de ressource qui a été partagée avec vous doit être mise à jour. Contactez la personne qui a créé la découverte de ressource et demandez-lui de mettre à jour l'autorisation gérée `AWSRAMPermissionIpamResourceDiscovery` vers la version par défaut. Pour de plus amples informations, consultez Mettre à jour un partage de ressources dans le Guide de l'utilisateur AWS RAM .

AWS Management Console

Pour consulter des informations sur les adresses IP publiques

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Public IP Insights.
3. Pour afficher les détails d'une adresse IP publique, sélectionnez une adresse IP en cliquant dessus.

4. Consultez les informations suivantes concernant l'adresse IP :

   - Détails : les mêmes informations que celles visibles dans les colonnes du panneau principal d'informations sur Public IP Insights, telles que Type d'adresse et Service.
   - Règles entrantes des groupes de sécurité : si cette adresse IP est associée à une instance EC2, ce sont les règles du groupe de sécurité qui contrôlent le trafic entrant vers l'instance.
   - Règles sortantes des groupes de sécurité : si cette adresse IP est associée à une instance EC2, ce sont les règles du groupe de sécurité qui contrôlent le trafic sortant depuis l'instance.
   - Tags : paires de clés et de valeurs qui agissent comme des métadonnées pour organiser vos AWS ressources.

Command line

Utilisez la commande suivante pour obtenir les adresses IP publiques découvertes par IPAM : - addresses get-ipam-discovered-public

Didacticiels pour Amazon VPC IP Address Manager (IPAM)

Les tutoriels suivants montrent comment exécuter les tâches IPAM courantes à l'aide d'AWS CLI. Pour obtenir la AWS CLI, consultez Accès à IPAM. Pour plus d'informations sur les concepts IPAM mentionnés dans ces didacticiels, consultez Fonctionnement d'IPAM.

Table des matières

- Didacticiel : créer un IPAM et des groupes à l'aide de la console
- Didacticiel : créer un IPAM et des groupes en utilisant la AWS CLI
- Didacticiel : affichez l'historique des adresses IP à l'aide de AWS CLI
- Didacticiel : apporter votre ASN à l'IPAM
- Didacticiel : apporter vos adresses IP à IPAM
- Didacticiel : transfert d'un CIDR IPv4 BYOIP vers IPAM
- Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau

Didacticiel : créer un IPAM et des groupes à l'aide de la console

Dans ce didacticiel, vous créez un IPAM, l'intégrez à AWS Organizations, créez des groupes d'adresses IP et créez un VPC avec un CIDR à partir d'un groupe IPAM.

Ce didacticiel explique comment utiliser IPAM pour organiser l'espace d'adressage IP en fonction de différents besoins de développement. Une fois ce didacticiel terminé, vous disposerez d'un groupe d'adresses IP pour les ressources de pré-production. Vous pouvez ensuite créer d'autres groupes en fonction de vos besoins en matière de routage et de sécurité, par exemple un groupe pour les ressources de production.

Bien que vous puissiez utiliser IPAM en tant qu'utilisateur unique, l'intégration avec AWS Organizations vous permet de gérer les adresses IP des différents comptes de votre organisation. Ce didacticiel traite de l'intégration d'IPAM avec les comptes d'une organisation. Il n'explique pas comment faire l'opération suivante : Intégration d'IPAM à des comptes extérieurs à votre organisation.

> **Note**
>
> Dans le cadre de ce didacticiel, les instructions vous indiqueront de nommer les ressources IPAM d'une manière particulière, de créer des ressources IPAM dans des Régions spécifiques et d'utiliser des plages d'adresses IP CIDR spécifiques pour vos groupes.

L'objectif est de rationaliser les choix disponibles dans IPAM et de vous permettre de démarrer rapidement avec IPAM. Une fois ce didacticiel terminé, vous pouvez décider de créer un nouvel IPAM et de le configurer différemment.

Table des matières

- Prérequis
- Comment AWS Organizations s'intègre à IPAM
- Étape 1 : délégation d'un administrateur IPAM
- Étape 2 : création d'un IPAM
- Étape 3 : Création d'un groupe IPAM de niveau supérieur
- Étape 4 : création de groupes IPAM régionaux
- Étape 5 : création d'un groupe de développement de pré-production
- Étape 6 : partage du groupe IPAM
- Étape 7 : création d'un VPC avec un CIDR alloué à partir d'un groupe IPAM
- Étape 8 : nettoyage

Prérequis

Avant de commencer, vous devez avoir configuré un compte AWS Organizations avec au moins un compte membre. Pour obtenir des instructions pratiques, veuillez consulter Création et gestion d'une organisation dans le Guide de l'utilisateur AWS Organizations.

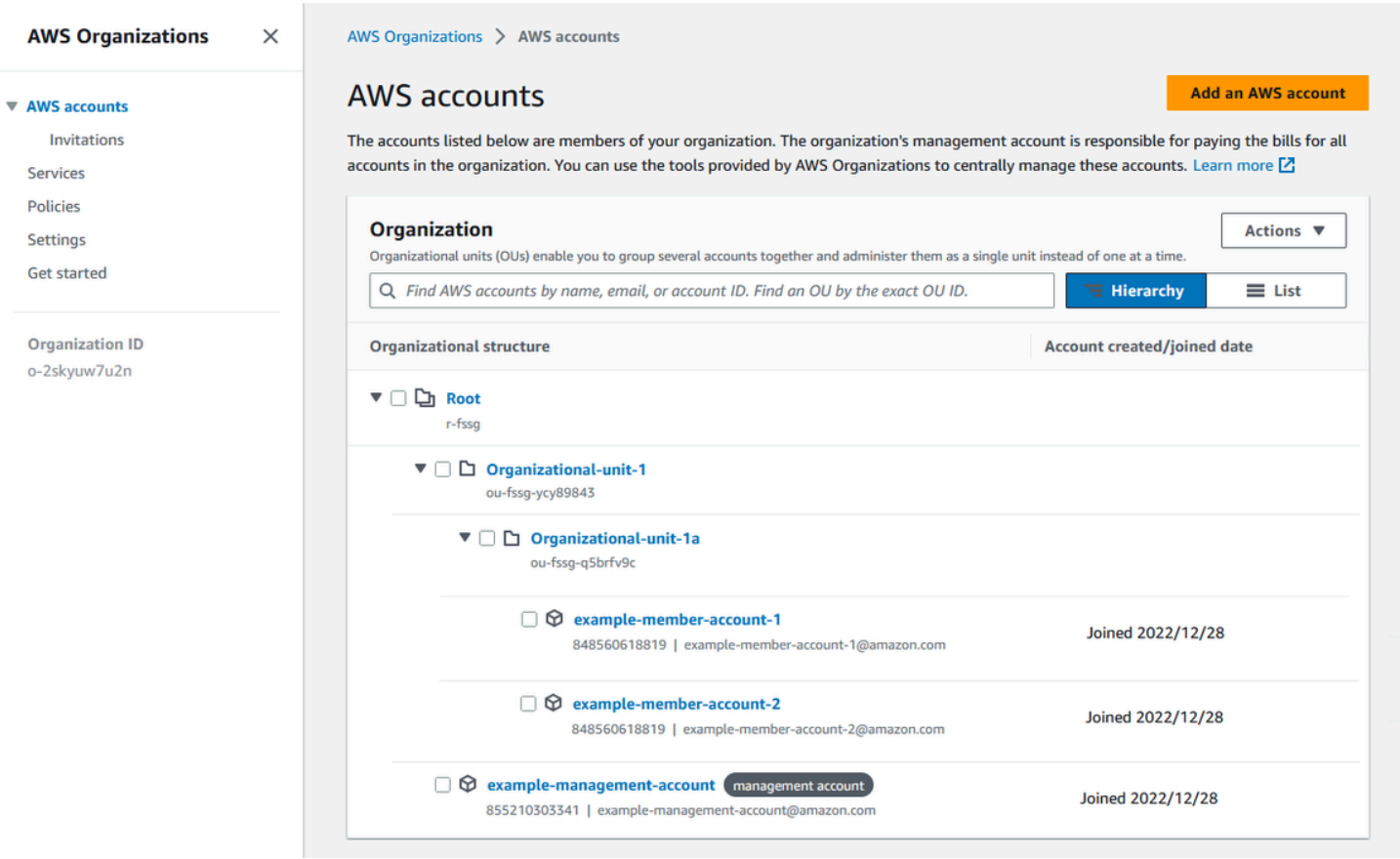
Comment AWS Organizations s'intègre à IPAM

Cette section présente un exemple des comptes AWS Organizations que vous utilisez dans ce didacticiel. Dans ce didacticiel, trois comptes de votre organisation sont utilisés pour l'intégration IPAM :

- Le compte de gestion (appelé example-management-account dans l'image suivante) pour se connecter à la console IPAM et déléguer un administrateur IPAM. Vous ne pouvez pas utiliser le compte de gestion de l'organisation en tant qu'administrateur IPAM.
- Un compte membre (appelé example-member-account-1 dans l'image suivante) en tant que compte administrateur IPAM. Le compte administrateur IPAM est responsable de la création d'un IPAM et de son utilisation pour gérer et contrôler l'utilisation des adresses IP au

sein de l'organisation. Tout compte membre de votre organisation peut être délégué en tant qu'administrateur IPAM.

- Un compte membre (appelé example-member-account-2 ci-dessus) en tant que compte de développeur. Ce compte crée un VPC avec un CIDR alloué à partir d'un groupe IPAM.



En plus des comptes, vous aurez besoin de l'identifiant de l'unité d'organisation (ou-fssg-q5brfv9c dans l'image précédente) qui contient le compte membre que vous utiliserez en tant que compte de développeur. Vous avez besoin de cet identifiant pour pouvoir, dans une étape ultérieure, partager votre groupe IPAM avec cette UO.

> **Note**
>
> Pour plus d'informations sur les types de comptes AWS Organizations tels que les comptes de gestion et les comptes de membres, consultez les concepts et la terminologie AWS Organizations.

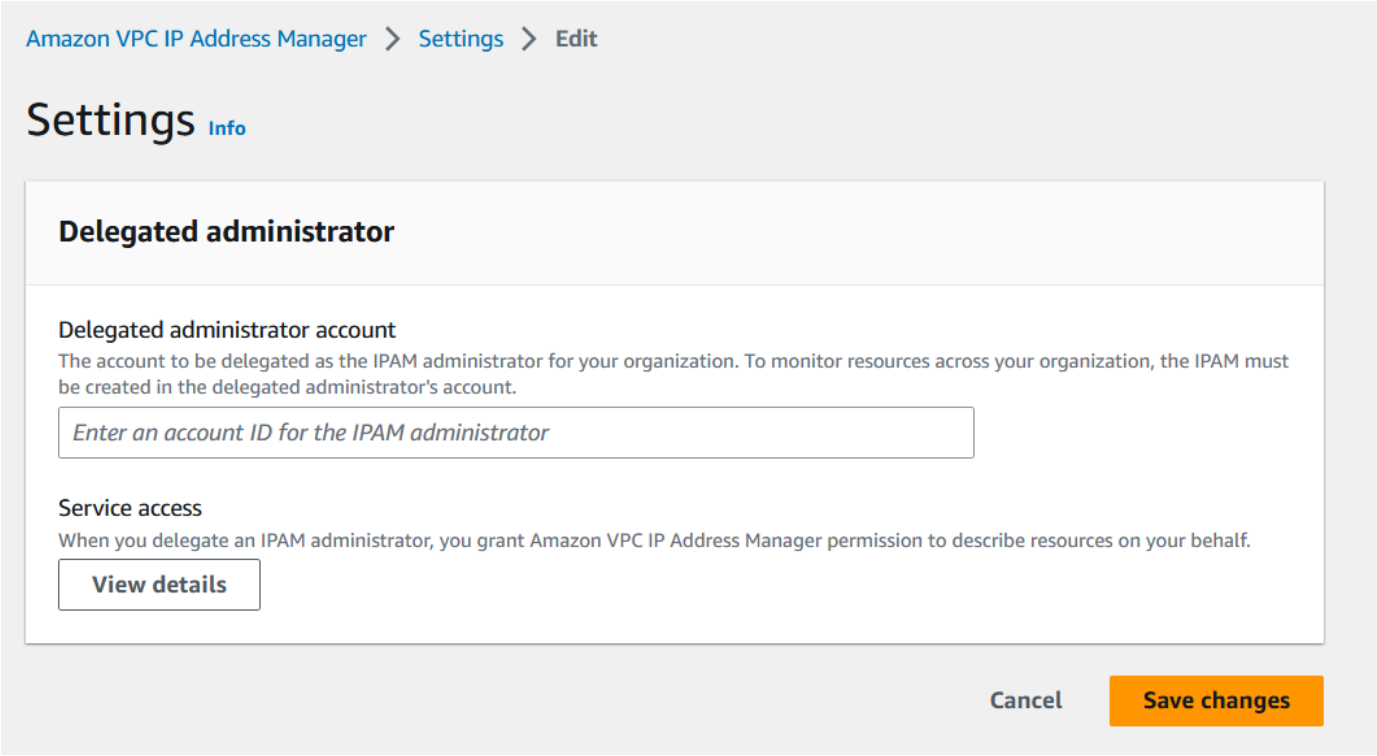
Étape 1 : délégation d'un administrateur IPAM

Au cours de cette étape, vous allez déléguer un compte membre AWS Organizations en tant qu'administrateur IPAM. Lorsque vous déléguez un administrateur IPAM, un rôle lié au service est automatiquement créé dans chacun de vos comptes membres AWS Organizations. IPAM contrôle l'utilisation des adresses IP dans ces comptes en assumant le rôle lié au service dans chaque compte membre. Il peut alors découvrir les ressources et leurs CIDR, quelle que soit leur unité d'organisation.

Vous ne pouvez effectuer cette étape que si vous disposez des autorisations AWS Identity and Access Management (IAM) requises. Pour de plus amples informations, veuillez consulter Intégrer l'IPAM aux comptes d'une organisation AWS.

Pour déléguer un compte administrateur IPAM

1. À l'aide du compte de gestion AWS Organizations, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans la console de gestion AWS, sélectionnez la Région AWS dans laquelle vous souhaitez travailler avec IPAM.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation).
4. Sélectionnez Delegate (Déléguer). L'option Déléguer n'est disponible que si vous vous êtes connecté à la console en tant que compte de gestion AWS Organizations.
5. Saisissez l'identifiant du compte AWS d'un compte membre de l'organisation. L'administrateur IPAM doit être un compte membre AWS Organizations et non le compte de gestion.



6. Choisissez Enregistrer les modifications. Les informations relatives à l'administrateur délégué sont renseignées avec les détails liés au compte membre.

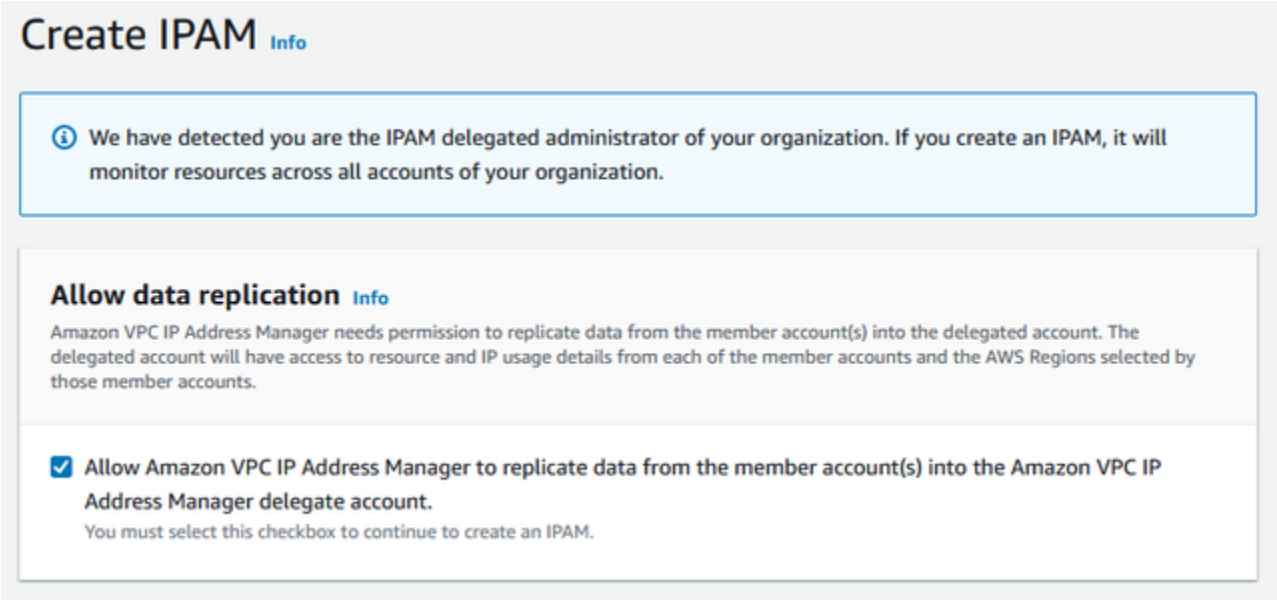
Étape 2 : création d'un IPAM

Au cours de cette étape, vous allez créer un IPAM. Lorsque vous créez un IPAM, celui-ci crée automatiquement deux portées pour l'IPAM : la portée privée qui est destinée à tout l'espace privé, et la portée publique qui est destinée à tout l'espace public. Les portées, ainsi que les groupes et les allocations, sont des composants clés de votre IPAM. Pour de plus amples informations, veuillez consulter Fonctionnement d'IPAM.

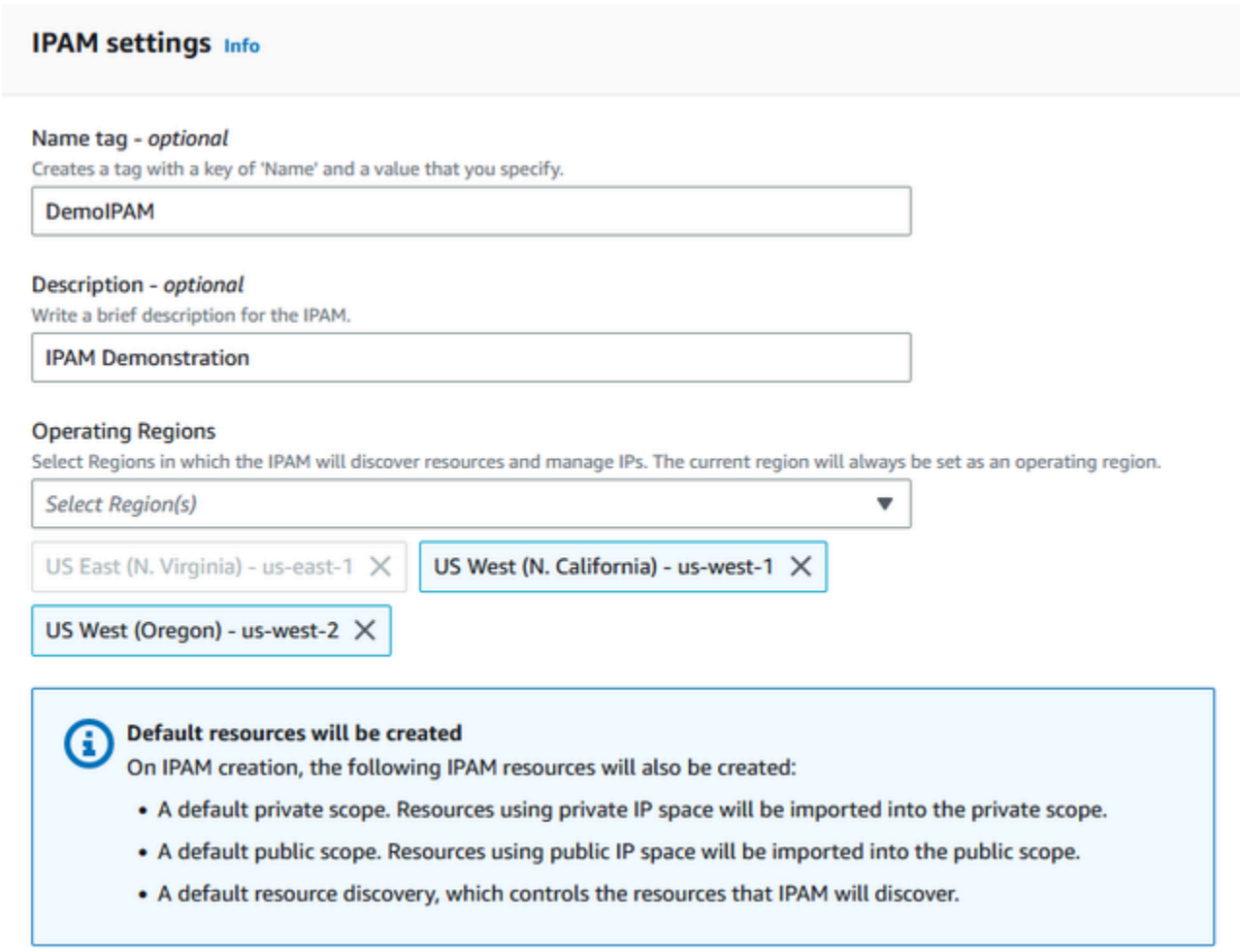
Création d'un IPAM

1. À l'aide du compte membre AWS Organizations délégué en tant qu'administrateur IPAM à l'étape précédente, ouvrez la console IPAM à l'adresse suivante :https://console.aws.amazon.com/ipam/.
2. Dans la Console de gestion AWS, sélectionnez la Région AWS dans laquelle vous souhaitez créer l'IPAM. Créez IPAM dans votre Région d'opérations principale.
3. Sur la page d'accueil, sélectionnez Create IPAM (Créer un IPAM).

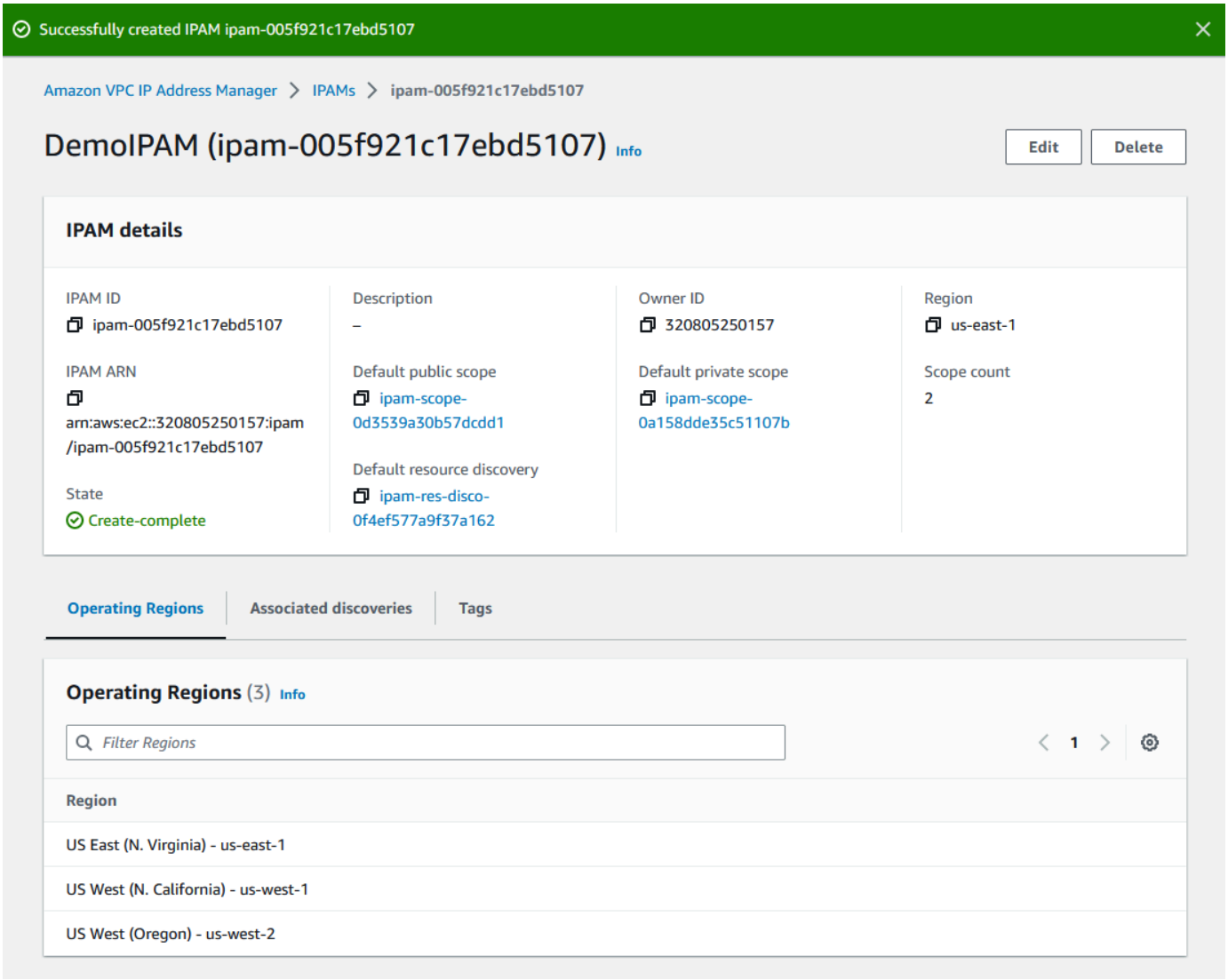
4. Sélectionnez Allow Amazon VPC IP Address Manager to replicate data from source account(s) into an IPAM Delegate account (Autoriser Amazon VPC IP Address Manager à répliquer les données du ou des comptes source dans le compte IPAM délégué). Si vous ne sélectionnez pas cette option, vous ne pouvez pas créer d'IPAM.



5. Sous Régions d'exploitation, sélectionnez les Régions AWS dans lesquelles cet IPAM peut gérer et découvrir des ressources. La Région AWS dans laquelle vous créez votre IPAM est automatiquement sélectionnée comme l'une des Régions d'exploitation. Dans ce didacticiel, la Région d'origine de notre IPAM est us-east-1, nous choisirons donc us-west-1 et us-west-2 comme Régions d'exploitation supplémentaires. Si vous oubliez une Région d'exploitation, vous pouvez modifier vos paramètres IPAM ultérieurement et ajouter ou supprimer des Régions.



6. Sélectionnez Create IPAM (Créer un IPAM).



Étape 3 : Création d'un groupe IPAM de niveau supérieur

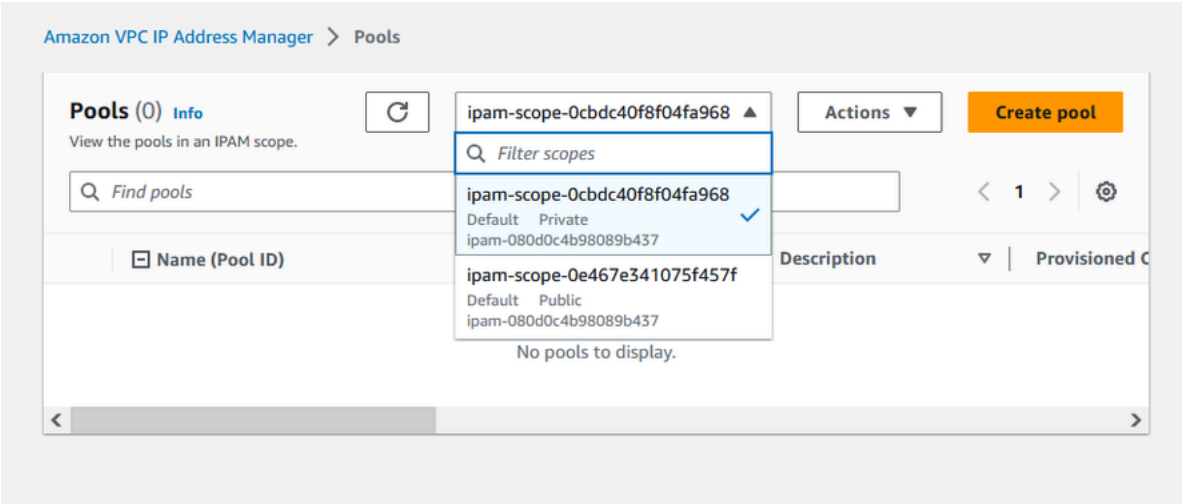
Dans ce didacticiel, vous créez une hiérarchie de groupes en commençant par le groupe IPAM de niveau supérieur. Dans les étapes suivantes, vous créerez une paire de groupes régionaux et un groupe de développement de pré-production dans l'un des groupes régionaux.

Pour plus d'informations sur les hiérarchies de groupes que vous pouvez créer avec IPAM, consultez Exemples de plans de groupes IPAM.

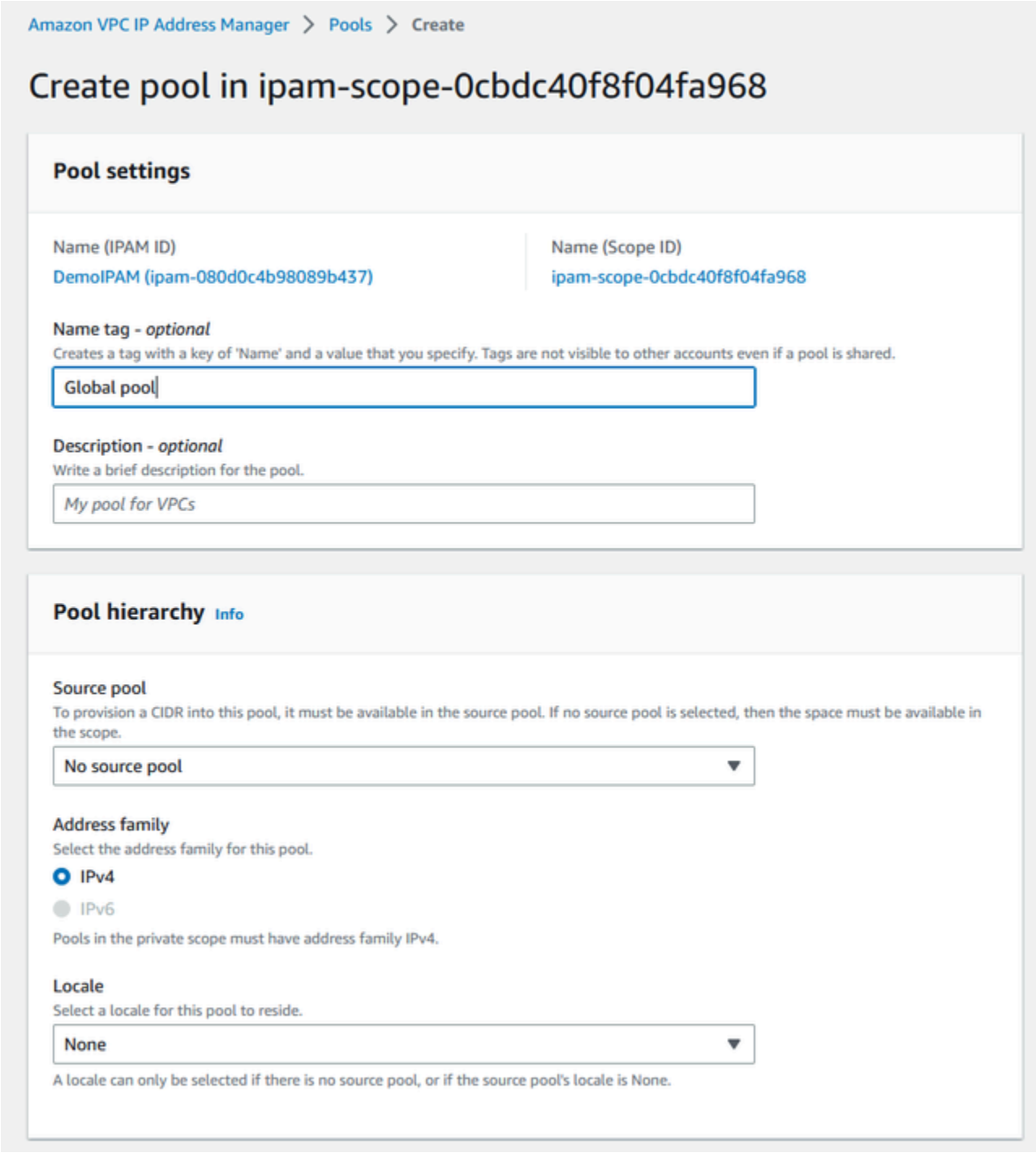
Pour créer un groupe de niveau supérieur

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.

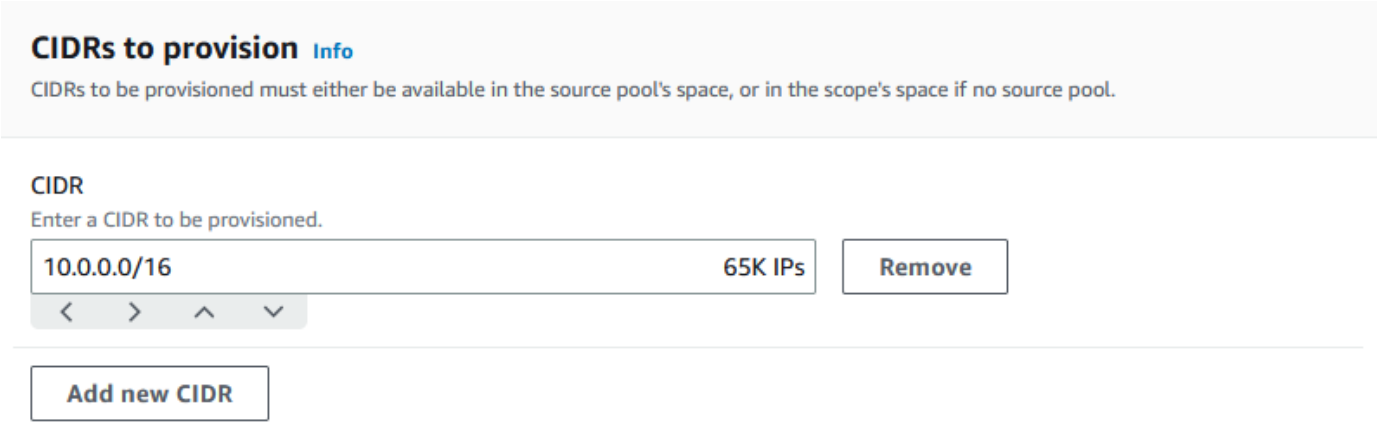
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez la portée privée.



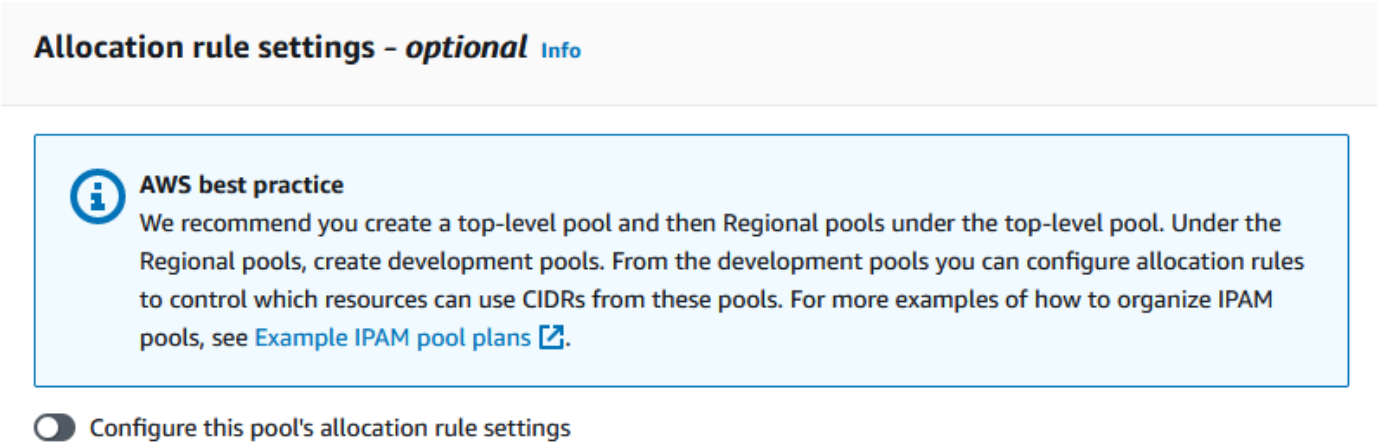
4. Sélectionnez Create pool (Créer un groupe).
5. Sous Portée IPAM, laissez la portée privée sélectionnée.
6. (Facultatif) Ajoutez une valeur Balise de nom pour le groupe et une description du groupe, par exemple « Groupe global ».
7. Sous Source, choisissez Portée IPAM. Comme il s'agit de notre groupe de niveau supérieur, il n'aura pas de groupe source.
8. SousAddress family (Famille d'adresses), choisissezIPv4.
9. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
10. Pour Locale (Paramètres régionaux), sélectionnez None (Aucun). Les paramètres locaux dans les Régions AWS dans laquelle vous souhaitez que ce groupe IPAM soit disponible pour les allocations. Vous définirez les paramètres régionaux pour les groupes régionaux que vous créez dans la section suivante de ce didacticiel.



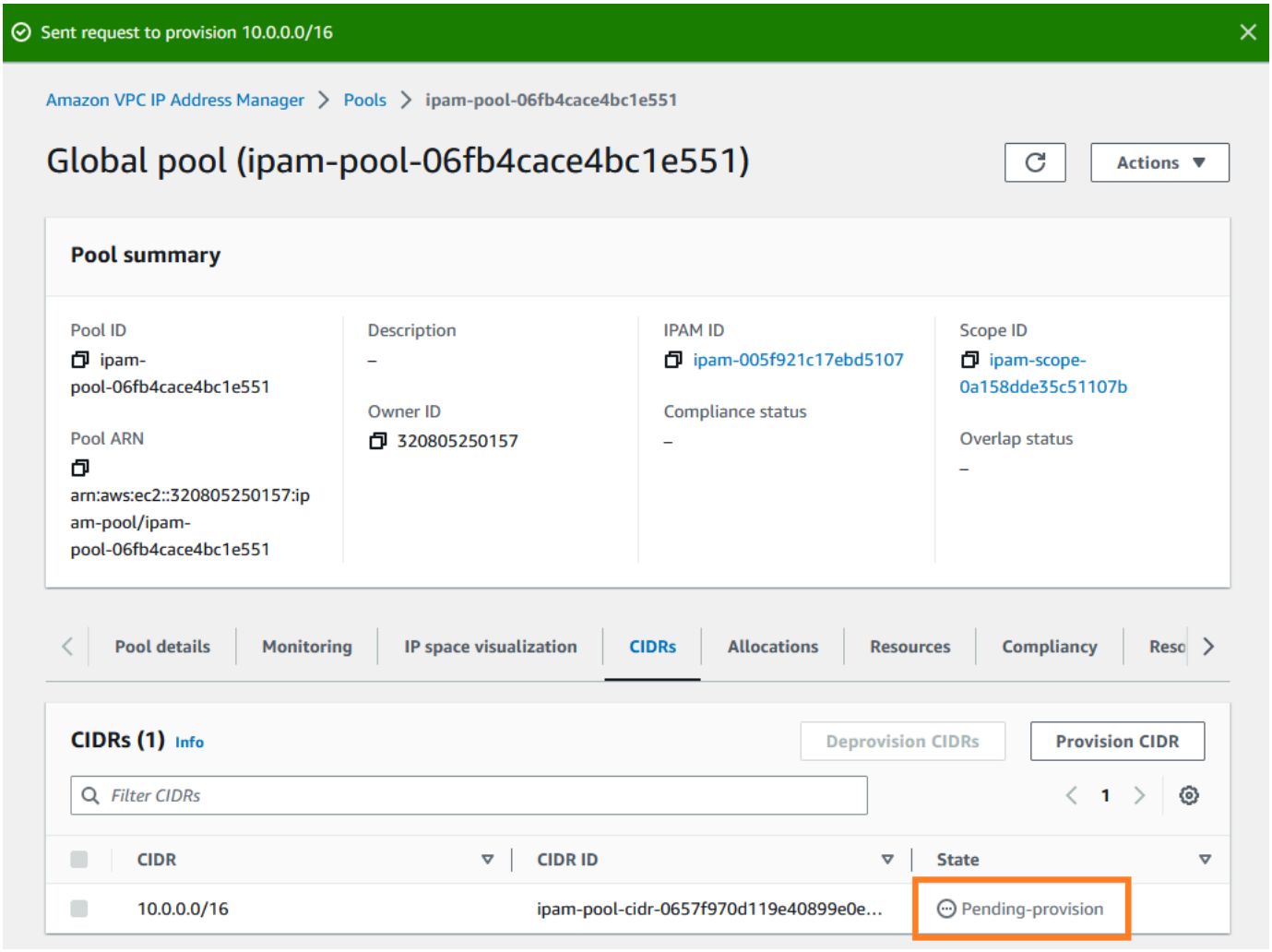
11. Choisissez un CIDR à provisionner pour le groupe. Dans cet exemple, nous provisionnons 10.0.0.0/16.



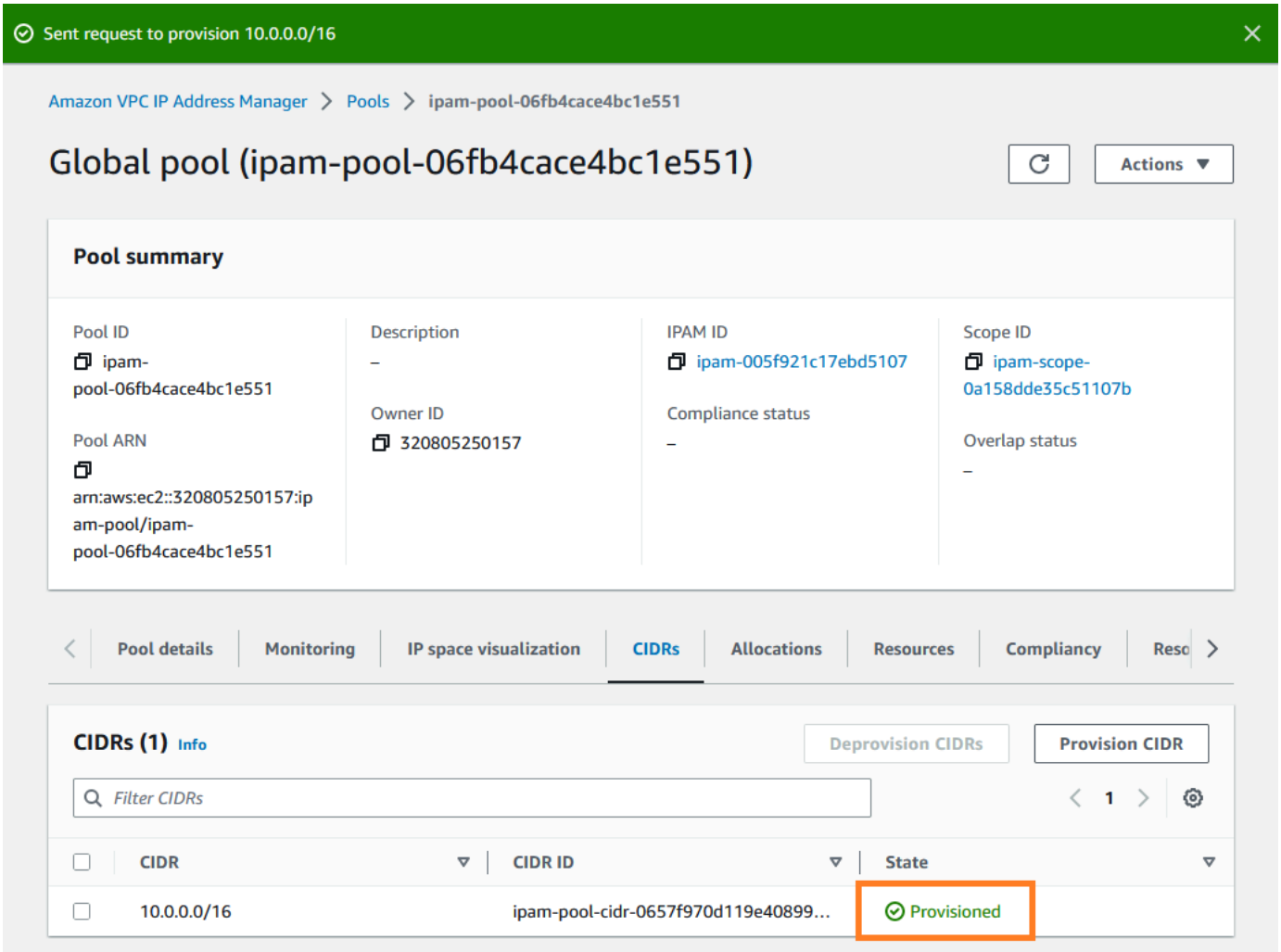
12. Laissez l'option Configurer les paramètres des règles d'allocation de ce groupe désactivées. Il s'agit de notre groupe de niveau supérieur, et vous n'allouerez pas de CIDR aux VPC directement à partir de ce groupe. Au lieu de cela, vous les allouerez à partir d'un sous-groupe que vous créerez à partir de ce groupe.



13. Sélectionnez Create pool (Créer un groupe). Le groupe est créé et le CIDR est dans un état de provision en attente :



14. Attendez que l'état soit Provisionné avant de passer à l'étape suivante.



Maintenant que vous avez créé votre groupe de niveau supérieur, vous allez créer des groupes régionaux dans us-west-1 et us-west-2.

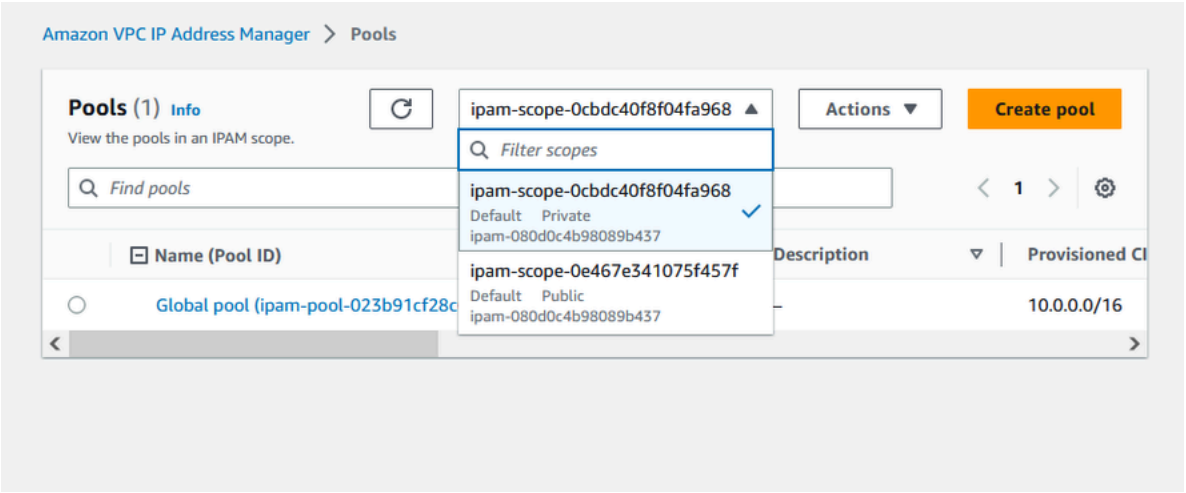
Étape 4 : création de groupes IPAM régionaux

Cette section vous montre comment organiser vos adresses IP à l'aide de deux groupes régionaux. Dans ce didacticiel, nous suivons l'un des exemples de plans de groupe IPAM et créons deux groupes régionaux qui peuvent être utilisés par les comptes membres de votre organisation pour allouer des CIDR à leurs VPC.

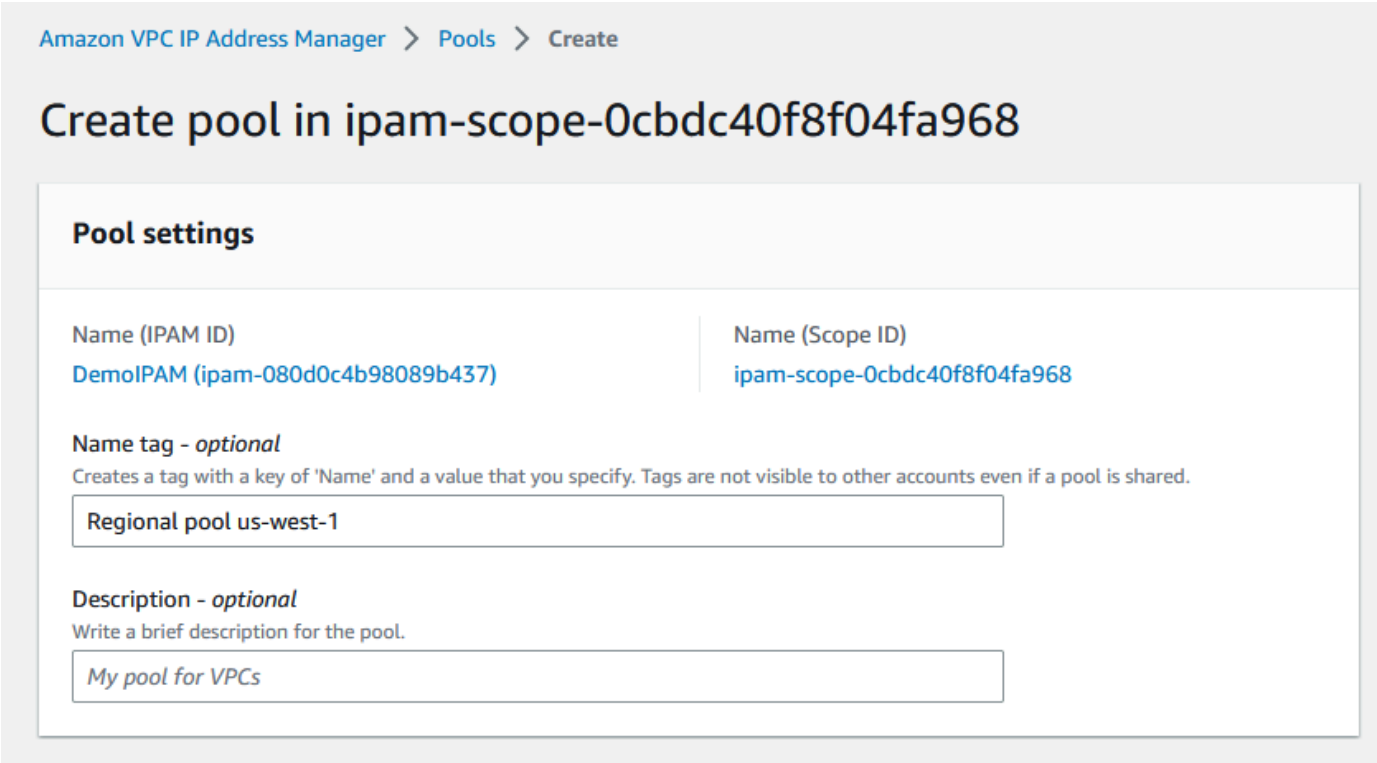
Pour créer un groupe régional

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.

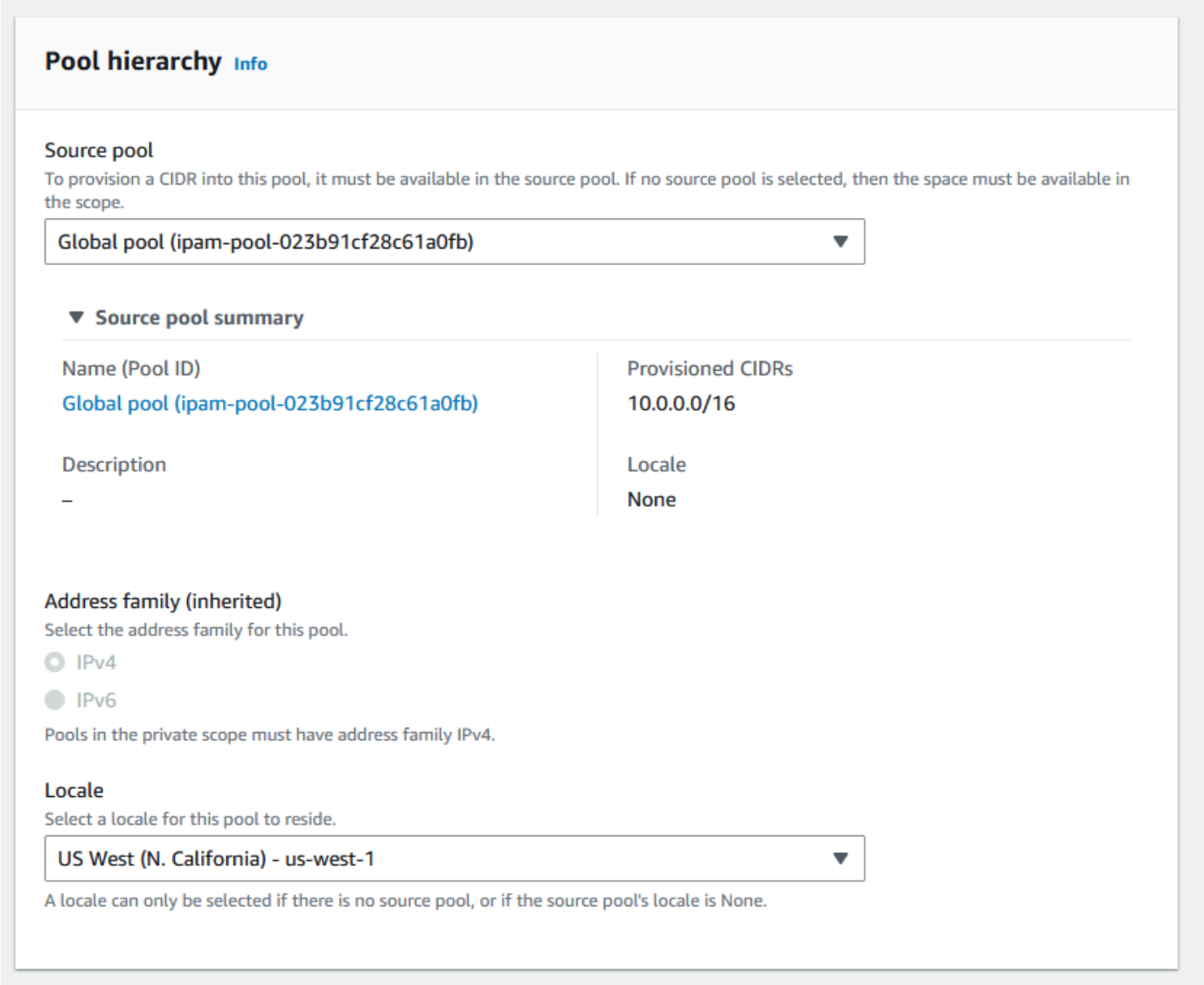
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez la portée privée.



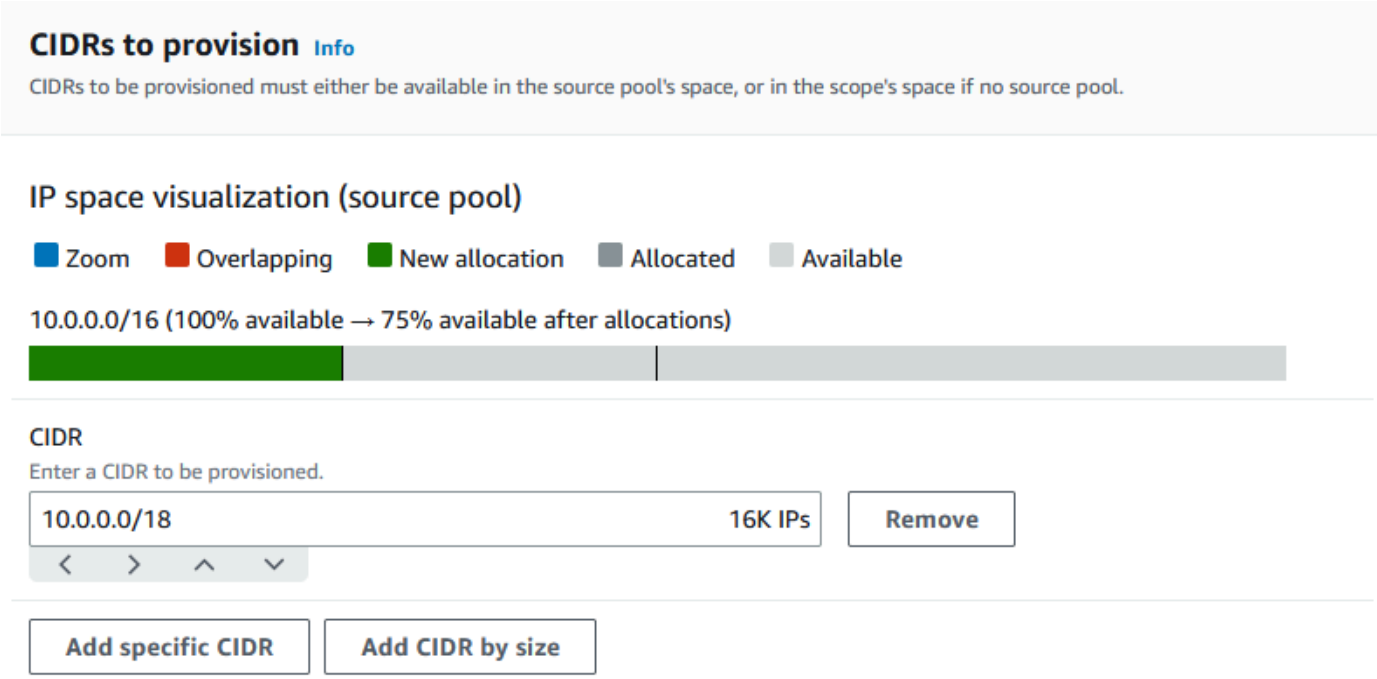
4. Sélectionnez Create pool (Créer un groupe).
5. Sous Portée IPAM, laissez la portée privée sélectionnée.
6. (Facultatif) Ajoutez une valeur Balise de nom du groupe et une description pour le groupe, tel que Groupe régional us-west-1.



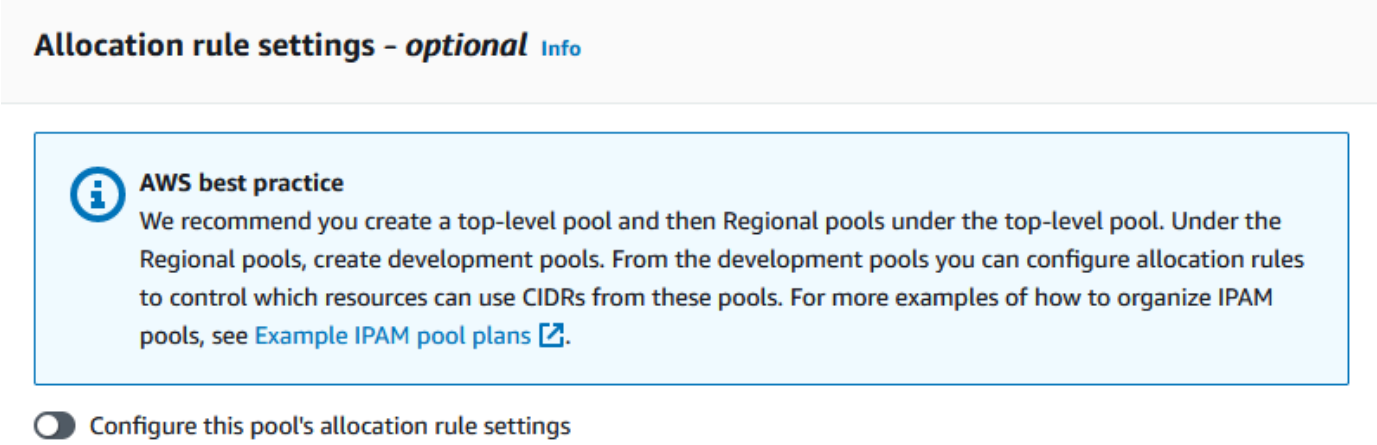
7. Sous Source, sélectionnez Groupe IPAM puis le groupe de niveau supérieur (« Groupe global ») que vous avez créé dans Étape 3 : Création d'un groupe IPAM de niveau supérieur. Ensuite, sous Régions, choisissez us-west-1.



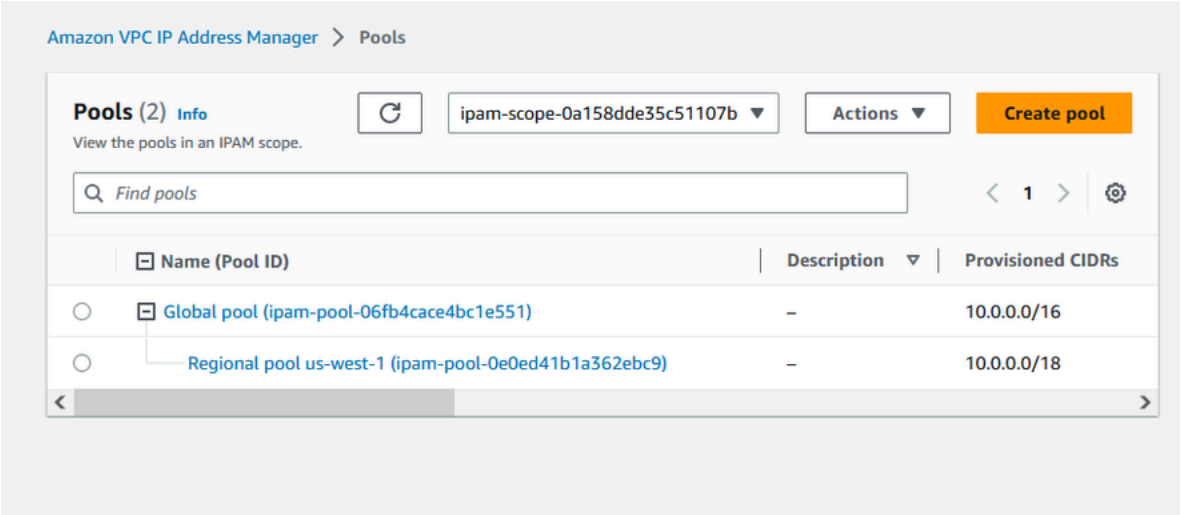
8. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
9. Sous CIDR à provisionner, saisissez 10.0.0.0/18, ce qui donnera à ce groupe environ 16 000 adresses IP disponibles.



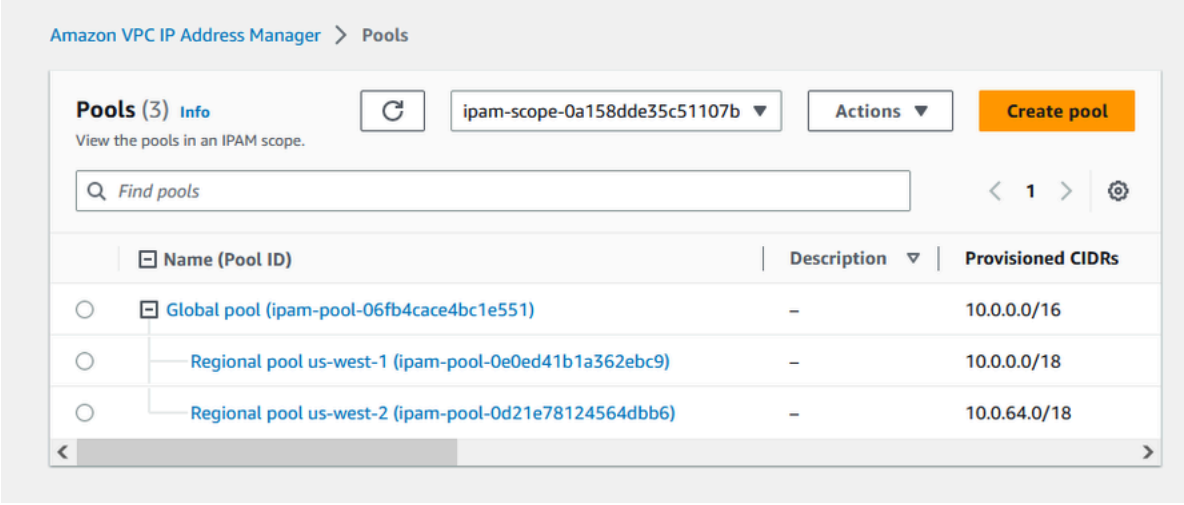
10. Laissez l'option Configurer les paramètres des règles d'allocation de ce groupe désactivées. Vous n'allouerez pas de CIDR aux VPC directement à partir de ce groupe. Au lieu de cela, vous les allouerez à partir d'un sous-groupe que vous créerez à partir de ce groupe.



11. Sélectionnez Create pool (Créer un groupe).
12. Revenez à la vue Groupes pour voir la hiérarchie des groupes IPAM que vous avez créés.



13. Répétez les étapes de cette section et créez un deuxième groupe régional dans la Région us-west-2 avec le CIDR 10.0.64.0/18 provisionné. À l'issue de ce processus, vous disposerez de trois groupes dans une hiérarchie similaire à celle-ci :

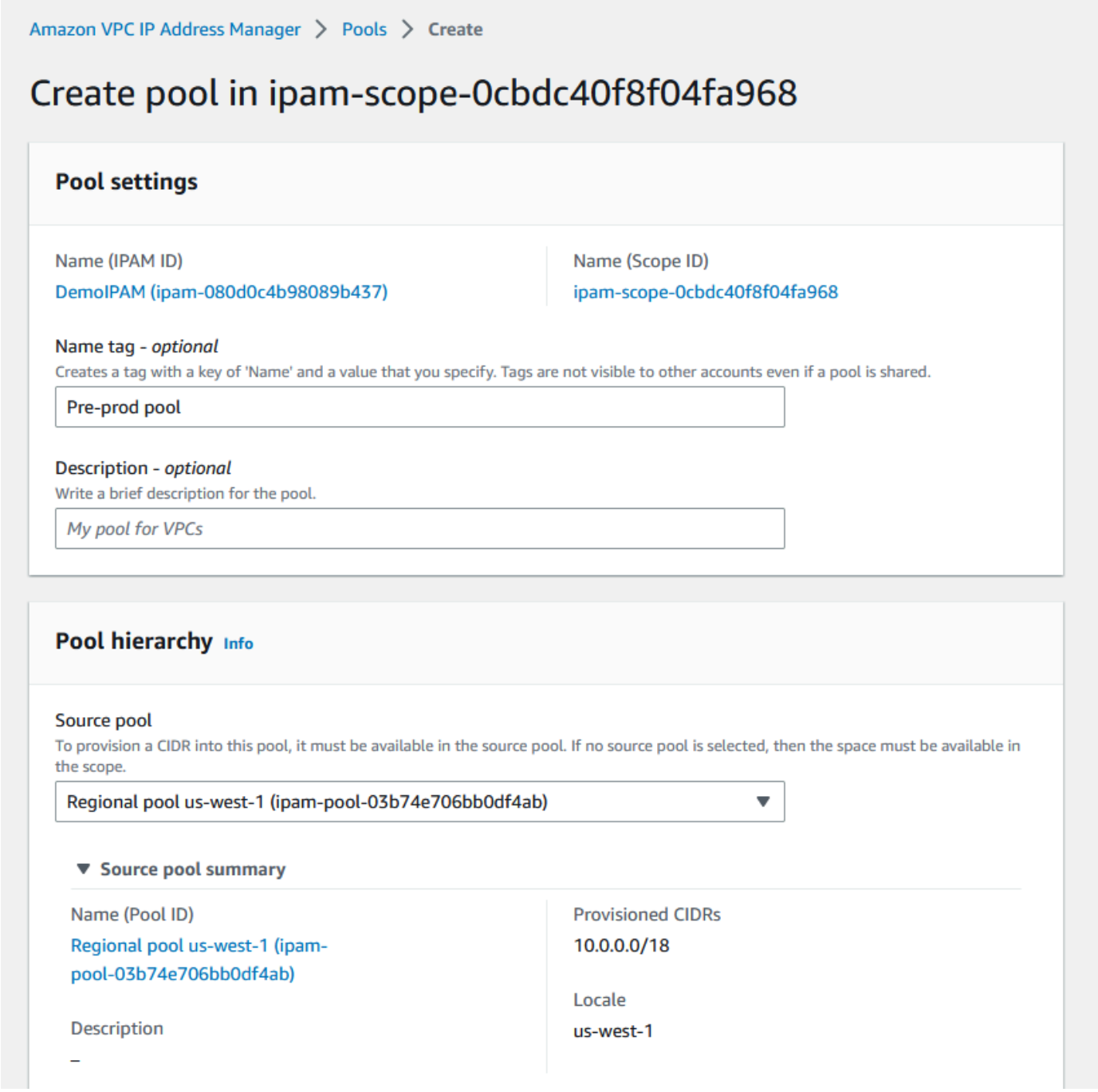


Étape 5 : création d'un groupe de développement de pré-production

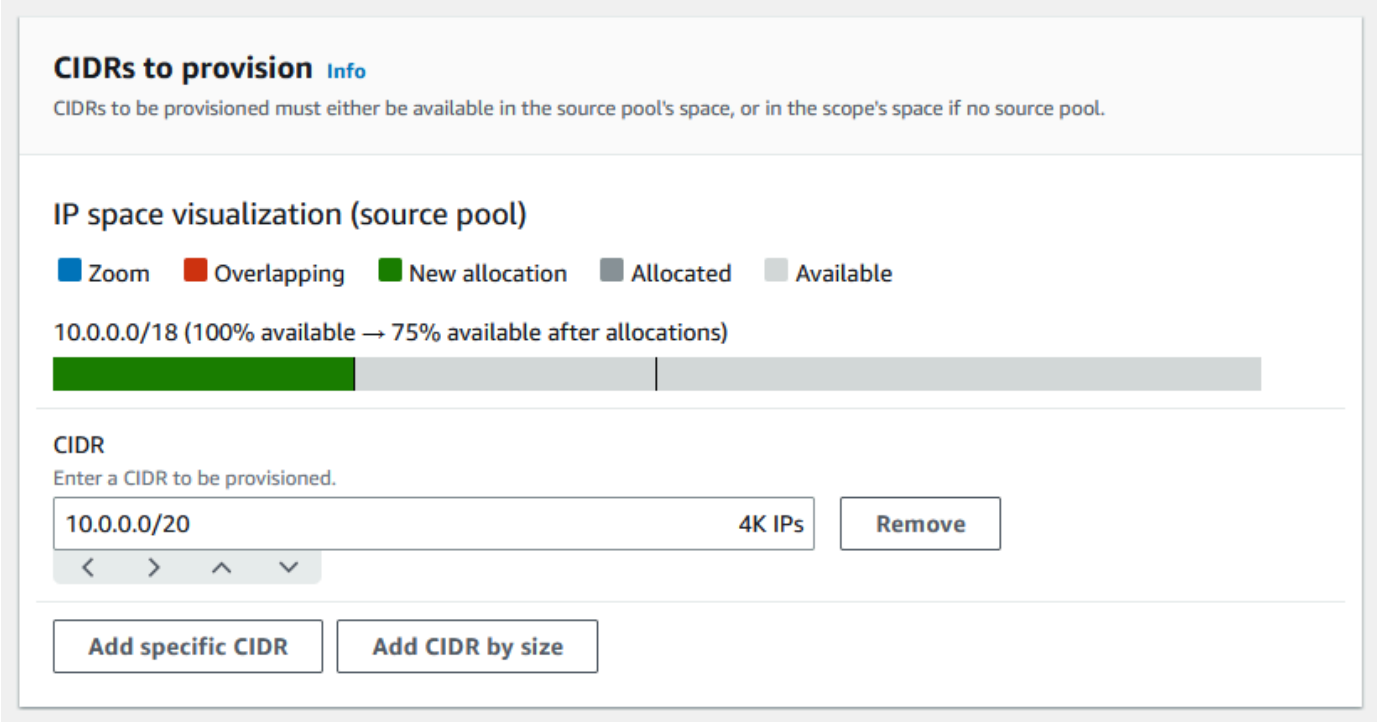
Suivez les étapes de cette section pour créer un groupe de développement pour les ressources de pré-production au sein de l'un de vos groupes régionaux.

Pour créer un groupe de développement de pré-production

1. De la même manière que dans la section précédente, à l'aide du compte administrateur IPAM, créez un groupe appelé Groupe pre-prod, mais cette fois, utilisez le groupe régional us-west-1 comme groupe source.

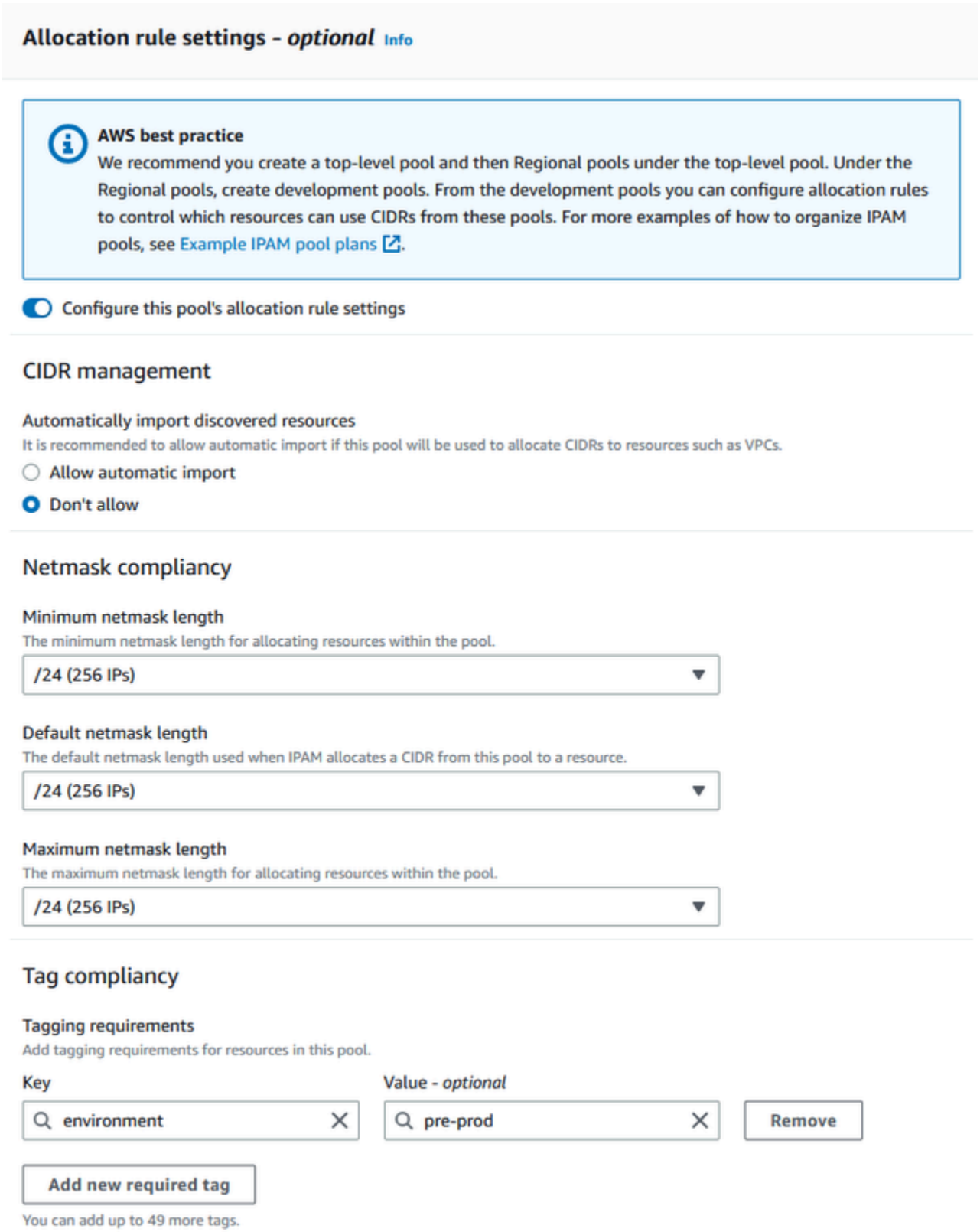


2. Spécifiez un CIDR 10.0.0.0/20 à provisionner, ce qui donnera à ce groupe environ 4 000 adresses IP.



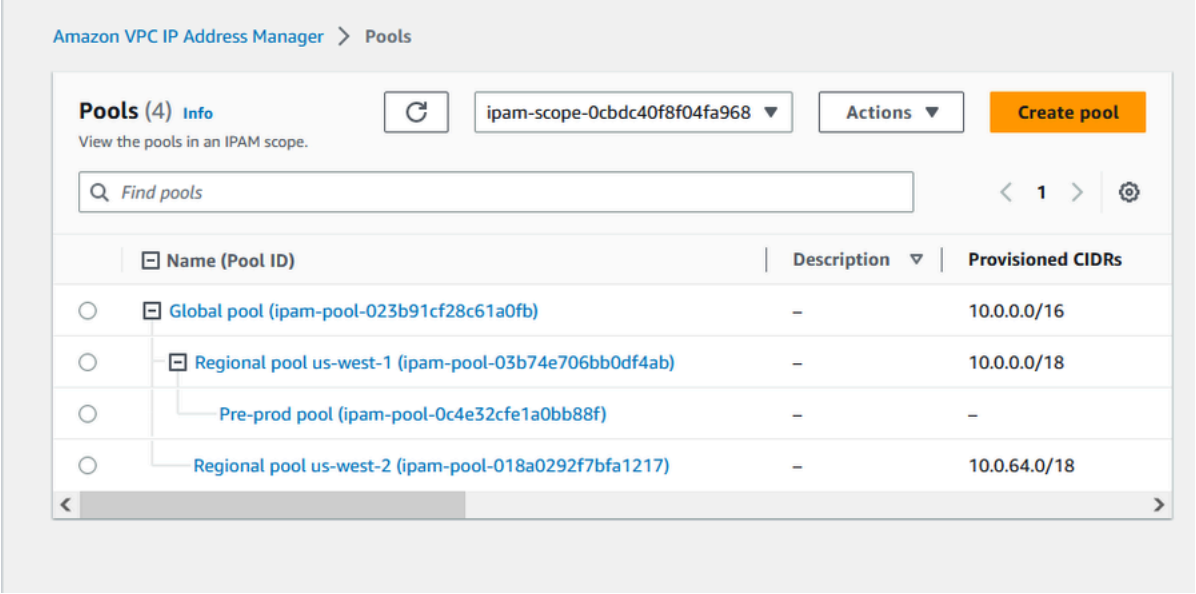
3. Activez l'option Configurer les paramètres des règles d'allocation de ce groupe. Procédez comme suit :

   1. Sous Gestion du CIDR, pour Importer automatiquement les ressources découvertes, laissez l'option par défaut Ne pas autoriser sélectionnée. Cette option permet à IPAM d'importer automatiquement les CIDR de ressources qu'il découvre dans la région du groupe. Une description détaillée de cette option n'entre pas dans le cadre de ce didacticiel, mais vous pouvez en savoir plus sur cette option dans Création d'un groupe IPv4 de niveau supérieur.
   2. Sous Conformité du masque réseau, choisissez /24 pour la longueur minimale, par défaut et maximale du masque réseau. Une description détaillée de cette option n'entre pas dans le cadre de ce didacticiel, mais vous pouvez en savoir plus sur cette option dans Création d'un groupe IPv4 de niveau supérieur. Il est important de noter que le VPC que vous créerez ultérieurement avec un CIDR à partir de ce groupe sera limité à /24 en fonction de ce que nous avons défini ici.
   3. Sous Conformité des balises, saisissez environment/pre-prod. Cette balise sera nécessaire pour que les VPC puissent allouer de l'espace à partir du groupe. Nous vous montrerons plus tard comment cela fonctionne.



4. Sélectionnez Create pool (Créer un groupe).

5. La hiérarchie des groupes inclut désormais un sous-groupe supplémentaire sous le groupe régional us-west-1 :



Vous êtes maintenant prêt à partager le groupe IPAM avec un autre compte membre de votre organisation et à permettre à ce compte d'allouer un CIDR à partir du groupe afin de créer un VPC.

Étape 6 : partage du groupe IPAM

Suivez les étapes de cette section pour partager le groupe IPAM de pré-production en utilisant AWS Resource Access Manager (RAM).

Cette section comprend deux sous-sections :

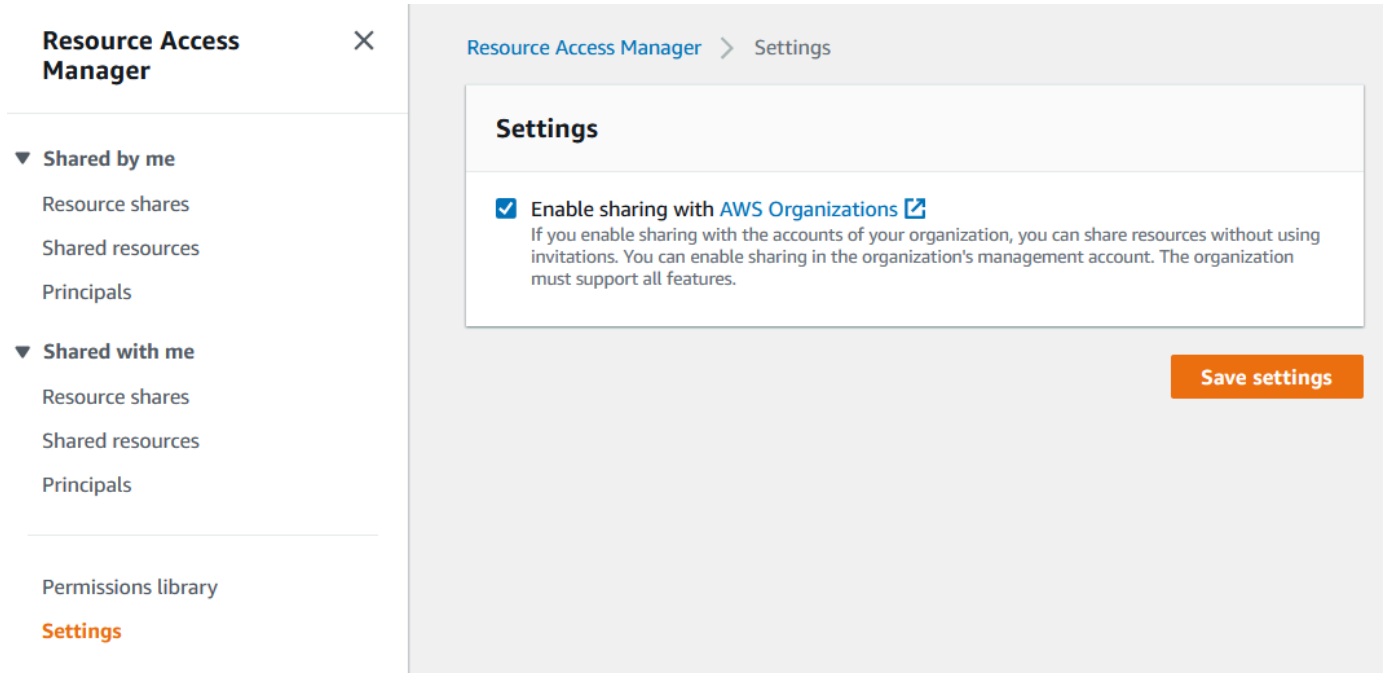
- Étape 6.1. Activer le partage des ressources dans AWS RAM : cette étape doit être réalisée par le compte de gestion AWS Organizations.
- Étape 6.2. Partager d'un groupe IPAM à l'aide deAWS RAM : cette étape doit être réalisée par l'administrateur IPAM.

Étape 6.1. Activer le partage des ressources dans AWS RAM

Après avoir créé votre IPAM, vous souhaiterez partager des groupes d'adresses IP avec d'autres comptes de votre organisation. Avant de partager un groupe IPAM, suivez les étapes de cette section pour activer le partage des ressources avec AWS RAM.

Pour activer le partage des ressources

1. À l'aide du compte de gestion AWS Organizations, ouvrez la console AWS RAM à l'adresse suivante : https://console.aws.amazon.com/ram/.
2. Dans le volet de navigation de gauche, choisissez Paramètres, choisissez Activer le partage avec AWS Organizations, puis choisissez Enregistrer les paramètres.



Vous pouvez désormais partager un groupe IPAM avec d'autres membres de l'organisation.

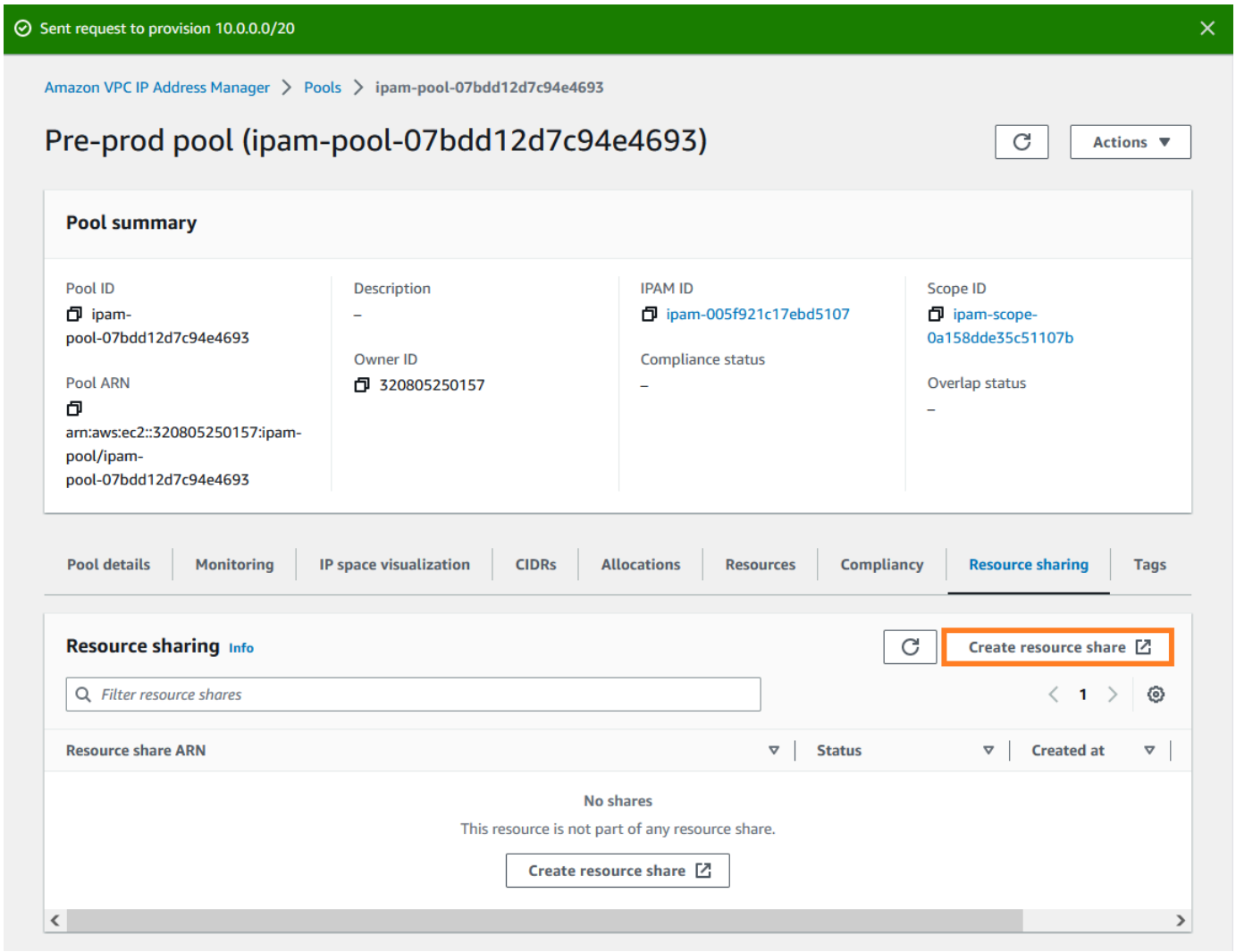
Étape 6.2. Partager d'un groupe IPAM à l'aide deAWS RAM

Dans cette section, vous partagerez le groupe de développement de pré-production avec un autre compte membre AWS Organizations. Pour obtenir des instructions complètes sur le partage de groupes IPAM, y compris des informations sur les autorisations IAM requises, consultez Partage d'un groupe IPAM à l'aide d'AWS RAM.

Pour partager un groupe IPAM à l'aide de AWS RAM

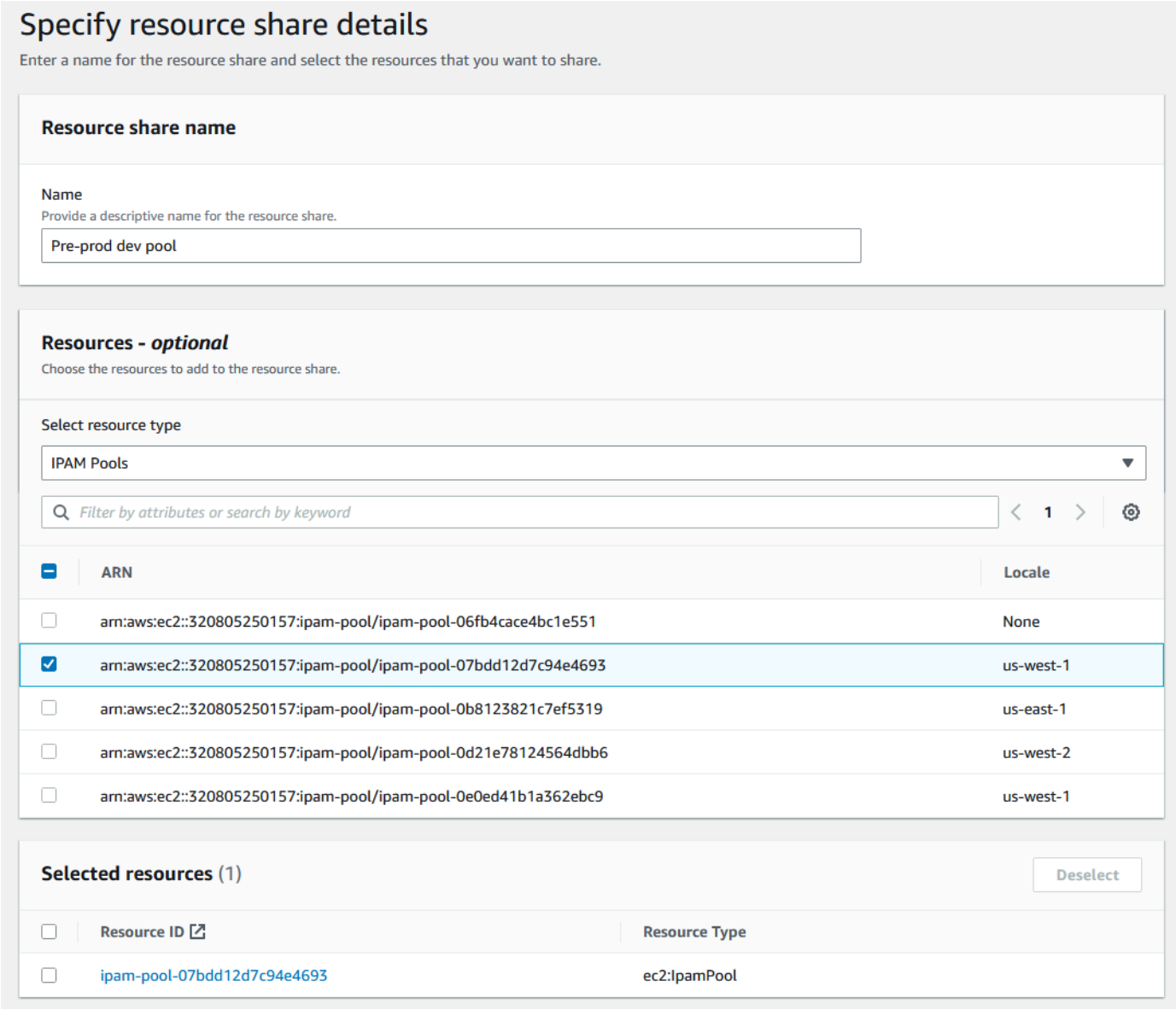
1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez la portée privée, choisissez le groupe IPAM de pré-production, puis choisissez Actions > Afficher les détails.

4. Sous Resource sharing (Partage de ressources), sélectionnez Create resource share (Créer un partage de ressources). La console AWS RAM s'ouvre. Vous partagerez le groupe en utilisant AWS RAM.
5. Sélectionnez Create a resource share (Créer un partage de ressources).

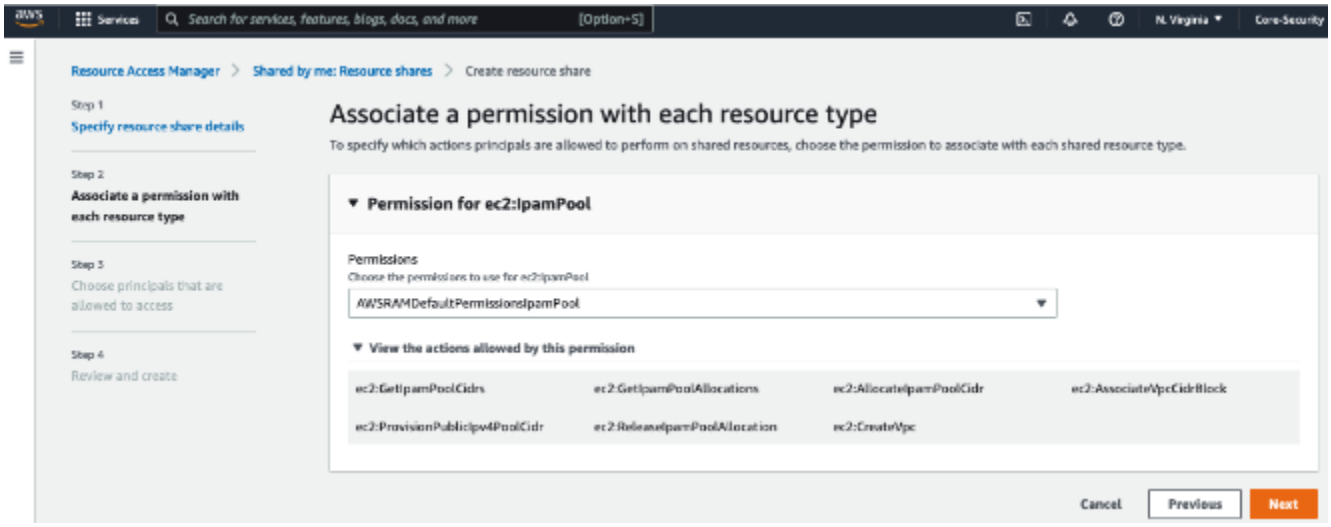


La console AWS RAM s'ouvre.

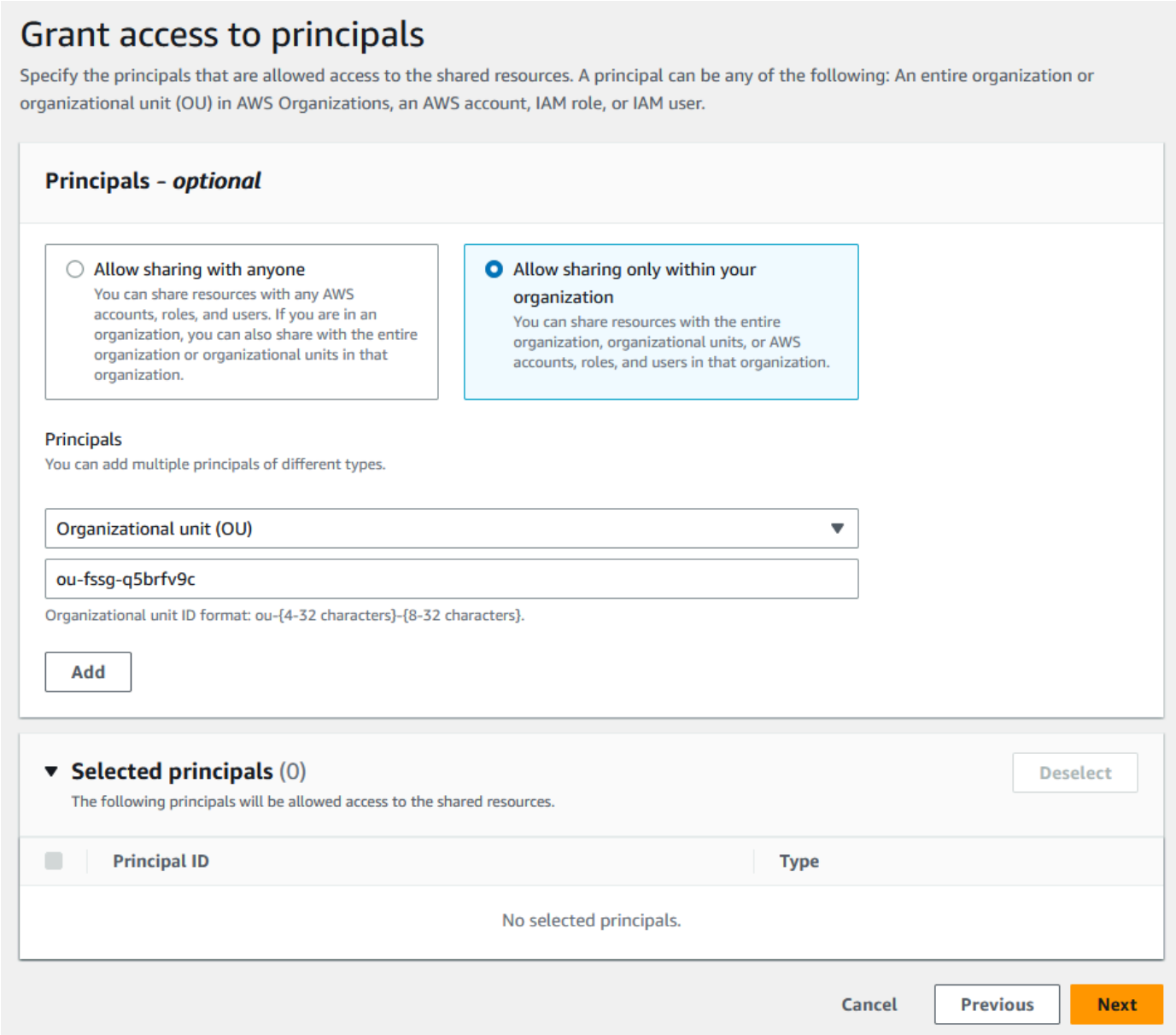
6. Dans la console AWS RAM, sélectionnez à nouveau Créer un partage de ressources.
7. Ajoutez un Nom pour la ressource partagée.
8. Sous Sélectionner le type de ressource, choisissez Groupes IPAM, puis choisissez l'ARN du groupe de développement de pré-production.



9. Choisissez Next (Suivant).
10. Laissez l'autorisation AWSRAMDefaultPermissionsIpamPool sélectionnée par défaut. Les détails des options d'autorisation ne sont pas abordés dans ce didacticiel, mais vous pouvez en savoir plus sur ces options dans Partage d'un groupe IPAM à l'aide d'AWS RAM.



11. Choisissez Next (Suivant).
12. Sous Principaux, sélectionnez Autoriser le partage uniquement au sein de votre organisation. Saisissez l'identifiant de votre unité d'organisation AWS Organizations (comme indiqué dans Comment AWS Organizations s'intègre à IPAM), puis choisissez Ajouter.



13. Choisissez Next (Suivant).
14. Examinez les options de partage de ressources et les principaux avec lesquels vous procéderez au partage, puis sélectionnez Créer.

Maintenant que le groupe a été partagé, passez à l'étape suivante pour créer un VPC avec un CIDR alloué à partir d'un groupe IPAM.

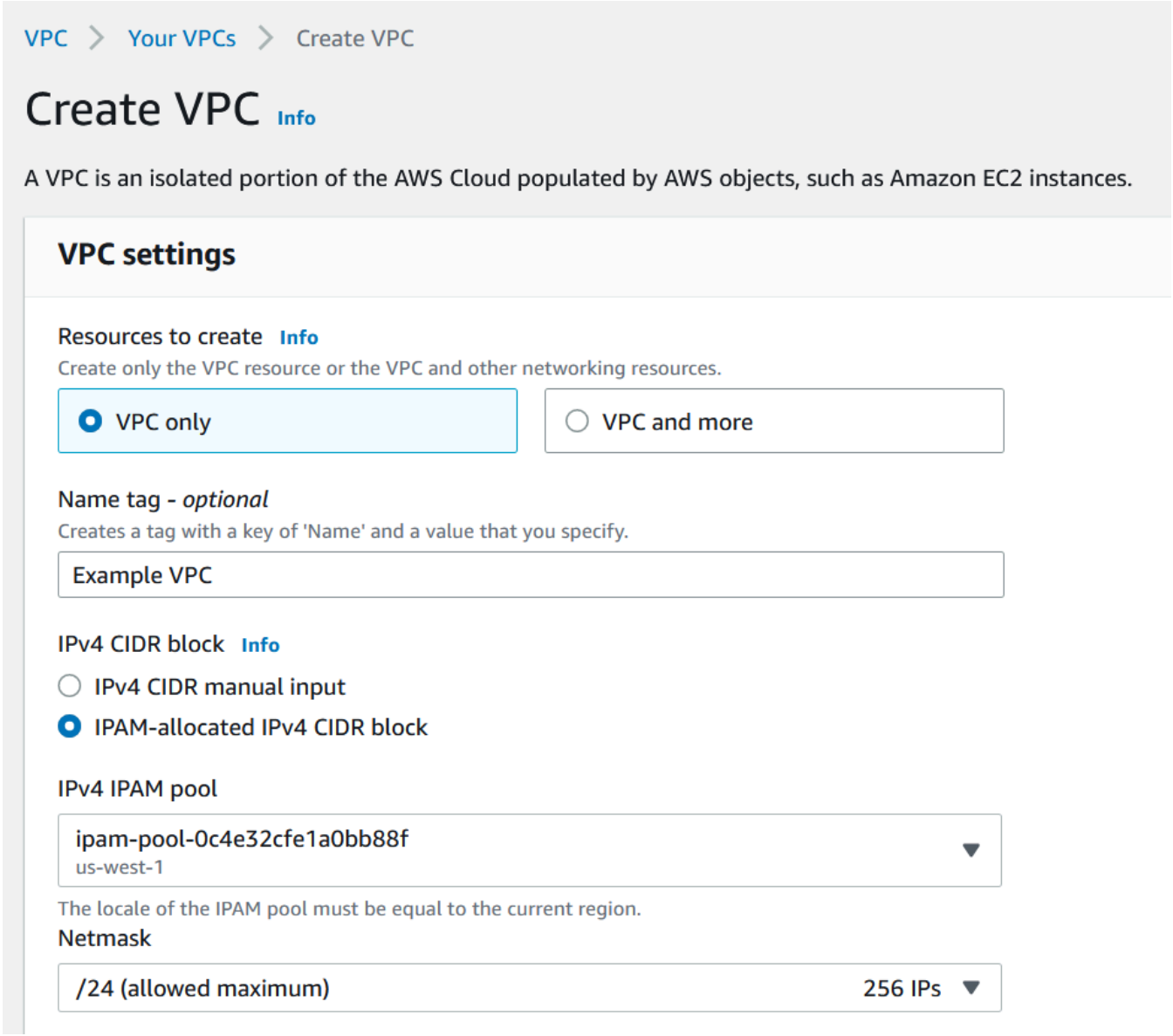
Étape 7 : création d'un VPC avec un CIDR alloué à partir d'un groupe IPAM

Suivez les étapes de cette section pour créer un VPC avec un CIDR alloué à partir du groupe de pré-production. Cette étape doit être effectuée par le compte membre de l'UO avec laquelle le groupe

IPAM a été partagé dans la section précédente (appelée example-member-account-2 dans Comment AWS Organizations s'intègre à IPAM). Pour plus d'informations sur les autorisations IAM requises pour créer des VPC, consultez les exemples de politiques Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

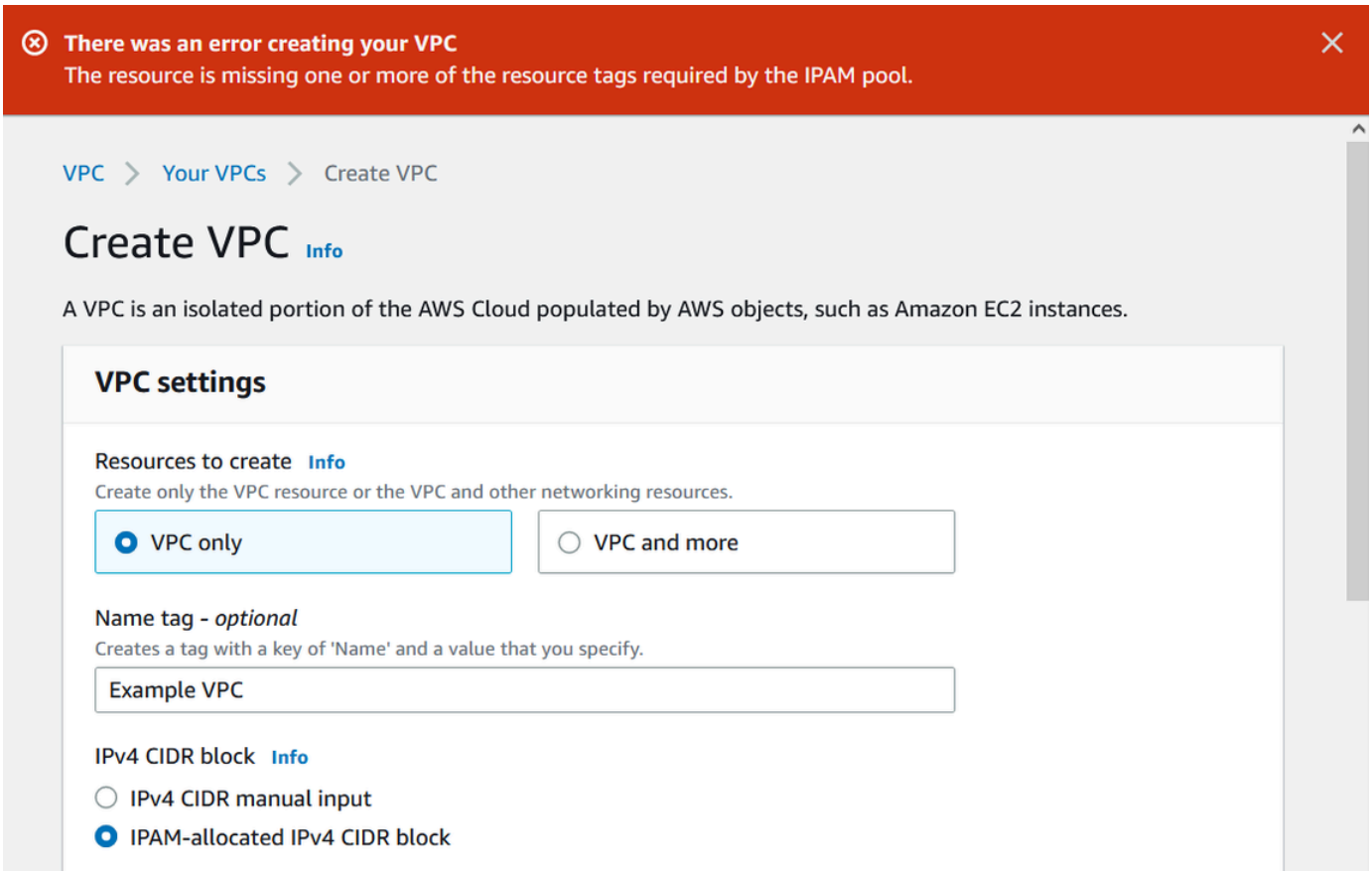
Pour créer un VPC avec un CIDR alloué à partir d'un groupe IPAM

1. En utilisant le compte membre, ouvrez la console VPC à l'adresse https://console.aws.amazon.com/vpc/ en tant que compte membre que vous utiliserez comme compte de développeur.
2. Sélectionnez Create VPC (Créer un VPC).
3. Procédez comme suit :
    1. Saisissez un nom, tel que Exemple VPC.
    2. Choisissez le bloc d'adresse CIDR IPv4 alloué à IPAM.
    3. Sous groupe IPAM IPv4, choisissez l'identifiant du groupe de pré-production.
    4. Choisissez la longueur du masque réseau. Comme vous avez limité la longueur du masque réseau disponible pour ce groupe à /24 (dans Étape 5 : création d'un groupe de développement de pré-production), la seule option de masque réseau disponible est /24.

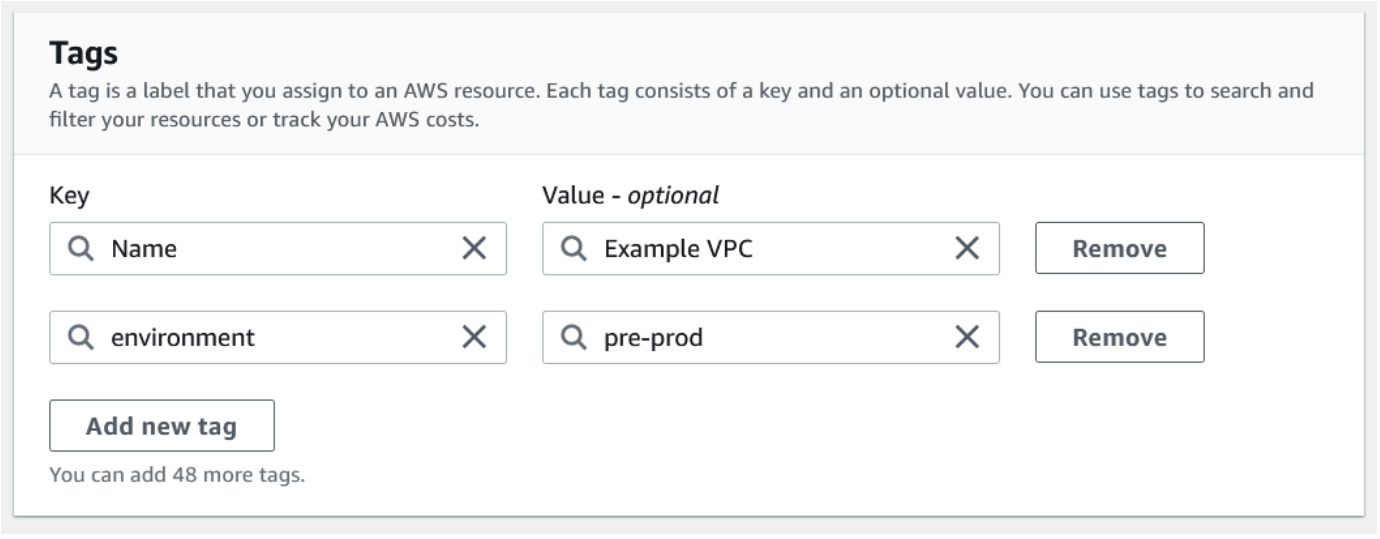


4. À des fins de démonstration, sous Balises, n'ajoutez aucune balise supplémentaire pour le moment. Lorsque vous avez créé le groupe de pré-production (dans 5. Créer un groupe de développement de pré-production), vous avez ajouté une règle d'allocation qui exigeait que tous les VPC créés avec des CIDR issus de ce groupe soient dotés d'une balise environment/pre-prod. Laissez la balise environment/pre-prod désactivée pour le moment afin de voir qu'un message d'erreur apparaît vous indiquant qu'une balise requise n'a pas été ajoutée.
5. Sélectionnez Create VPC (Créer un VPC).
6. Un message d'erreur s'affiche vous indiquant qu'une balise obligatoire n'a pas été ajoutée. L'erreur apparaît parce que vous avez défini une règle d'allocation lorsque vous avez créé le groupe de pré-production (in Étape 5 : création d'un groupe de développement de pré-

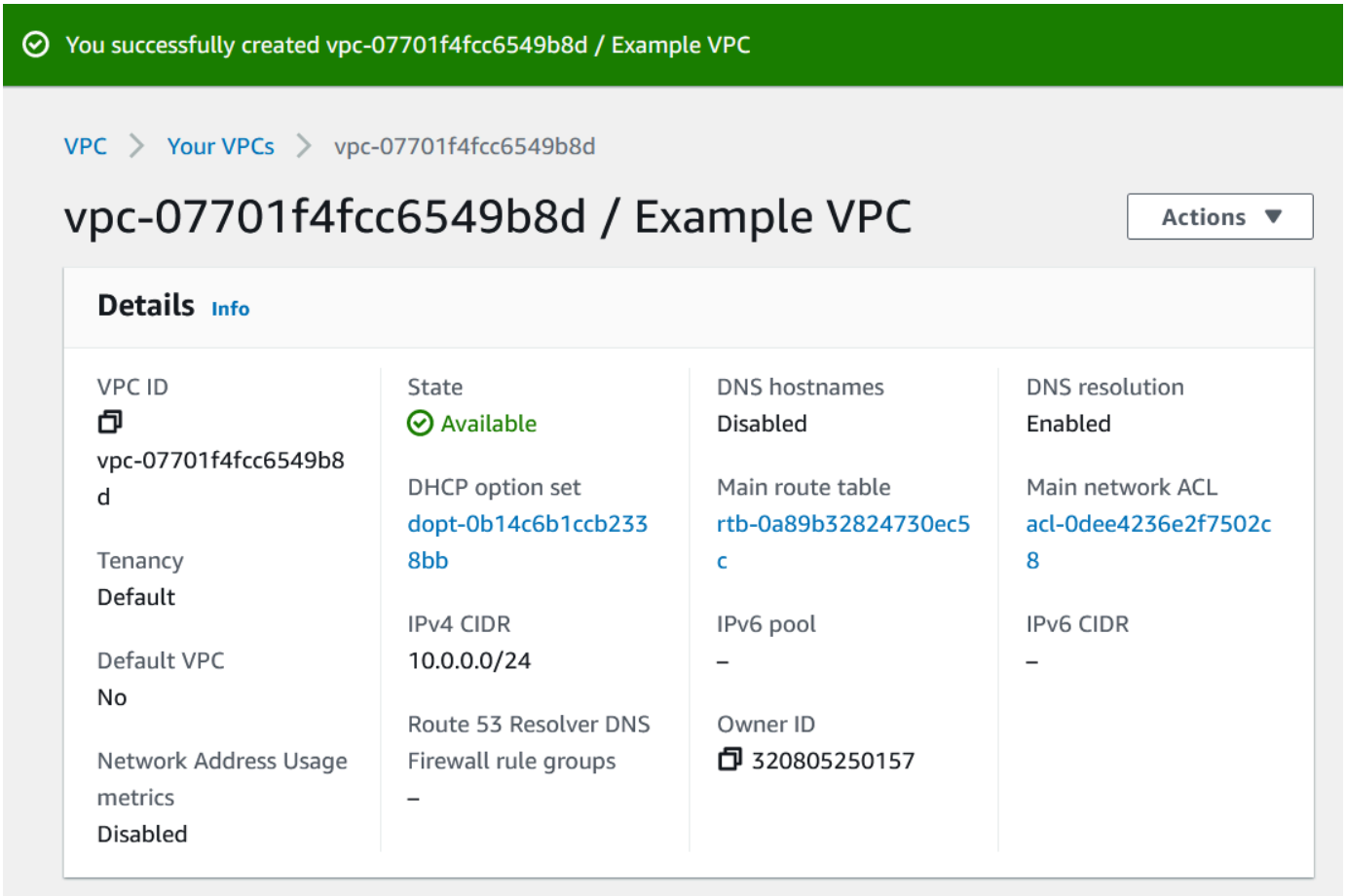
production). La règle d'allocation exigeait que tous les VPC créés avec des CIDR à partir de ce groupe soient dotés d'une balise environment/pre-prod.



7. Maintenant, sous Balises, ajoutez la balise environment/pre-prod et sélectionnez à nouveau Créer un VPC.



8. Le VPC est correctement créé et il est conforme à la règle de balisage du groupe de pré-production :



Dans le volet Ressources de la console IPAM, l'administrateur IPAM pourra voir et gérer le VPC et le CIDR qui lui est alloué. Notez qu'il faut un certain temps pour que le VPC apparaisse dans le volet Ressources.

Étape 8 : nettoyage

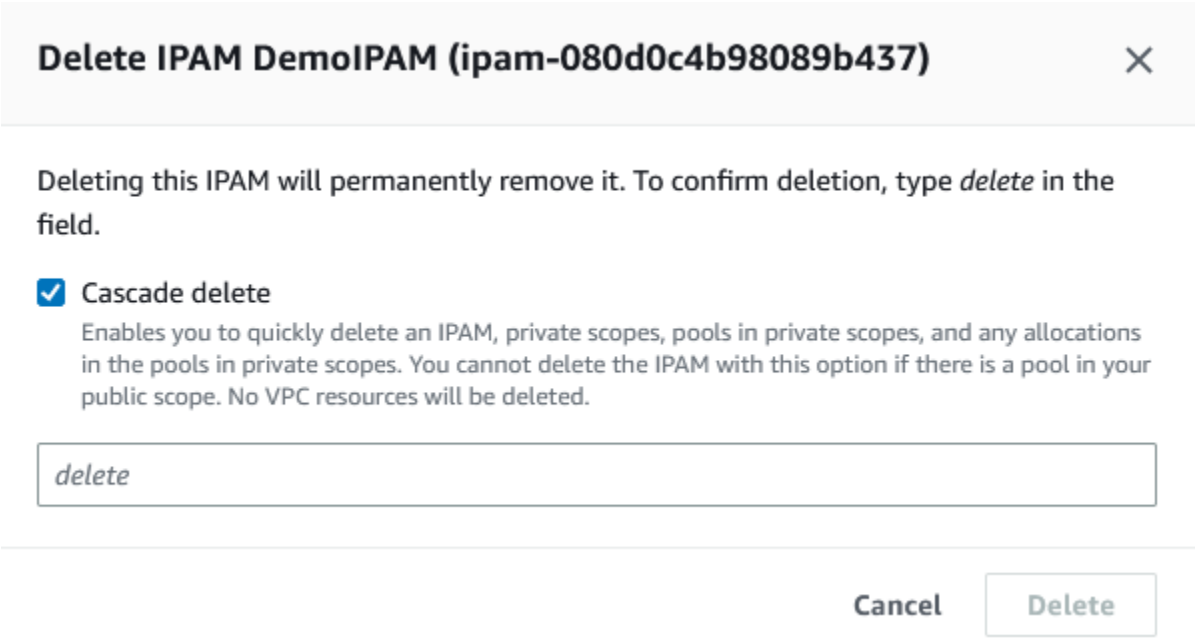
Dans ce didacticiel, vous avez créé un IPAM avec un administrateur délégué, créé plusieurs groupes et autorisé un compte membre de votre organisation à allouer un CIDR VPC à partir d'un groupe.

Suivez les étapes de cette section pour nettoyer les ressources que vous avez créées dans ce didacticiel.

Pour nettoyer les ressources créées dans ce didacticiel

1. En utilisant le compte membre qui a créé le VPC d'exemple, supprimez le VPC. Pour des instructions détaillées, veuillez consulter Supprimer votre VPC dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

2. En utilisant le compte administrateur IPAM, supprimez le partage de ressources de l'exemple dans la console AWS RAM. Pour obtenir des instructions détaillées, consultez Supprimer un partage de ressources dans AWSAWS RAM dans le Guide de l'utilisateur AWS Resource Access Manager.
3. En utilisant le compte administrateur IPAM, connectez-vous à la console RAM et désactivez le partage avec AWS Organizations que vous avez activé dans Étape 6.1. Activer le partage des ressources dans AWS RAM.
4. En utilisant le compte administrateur IPAM, supprimez l'exemple d'IPAM en le sélectionnant dans la console IPAM, puis en choisissant Actions > Supprimer. Pour obtenir des instructions complètes, veuillez consulter Suppression d'un IPAM.
5. Lorsque vous êtes invité à supprimer l'IPAM, choisissez Supprimer en cascade. Cela supprimera toutes les portées et tous les groupes de l'IPAM avant de le supprimer.



6. Saisissez supprimer et choisissez Supprimer.
7. À l'aide du compte de gestion AWS Organizations, connectez-vous à la console IPAM, choisissez Paramètres et supprimez le compte de l'administrateur délégué.
8. (Facultatif) Lorsque vous intégrez IPAM à AWS Organizations, IPAM crée automatiquement un rôle lié au service dans chaque compte membre. En utilisant chaque compte membre AWS Organizations, connectez-vous à IAM et supprimez le rôle lié au service AWSServiceRoleForIPAM dans chaque compte membre.
9. Le nettoyage est terminé.

Didacticiel : créer un IPAM et des groupes en utilisant la AWS CLI

Suivez les étapes de ce didacticiel pour utiliser la AWS CLI afin de créer un IPAM, de créer des groupes d'adresses IP et d'allouer un VPC avec un CIDR à partir d'un groupe IPAM.

L'exemple suivant illustre la hiérarchie de la structure de groupes que vous allez créer en suivant les étapes de cette section :

- IPAM opérant dans Région 1 AWS et Région 2 AWS
  - Portée privée
    - Groupe de niveau supérieur
      - Groupe régional dans Région 2 AWS
        - Groupe de développement
          - Allocation pour un VPC

> **Note**
>
> Dans cette section, vous allez créer un IPAM. Par défaut, vous ne pouvez créer qu'un IPAM. Pour de plus amples informations, veuillez consulter Quotas pour votre IPAM. Si vous avez déjà délégué un compte IPAM et créé un IPAM, vous pouvez ignorer les étapes 1 et 2.

Table des matières

- Étape 1 : activation d'IPAM dans votre organisation
- Étape 2 : création d'un IPAM
- Étape 3 : création d'un groupe d'adresses IPv4
- Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur
- Étape 5. Création d'un groupe régional avec un CIDR provenant du groupe de niveau supérieur
- Étape 6 : approvisionnement d'un CIDR au groupe régional
- Étape 7. Création d'un partage RAM pour activer les attributions IP entre les comptes
- Étape 8. Création d'un VPC
- Étape 9. Nettoyage

Étape 1 : activation d'IPAM dans votre organisation

Cette étape est facultative. Effectuez cette étape pour activer IPAM dans votre organisation et configurer votre IPAM délégué à l'aide d'AWS CLI. Pour plus d'informations sur le rôle du compte IPAM, consultez Intégrer l'IPAM aux comptes d'une organisation AWS.

Cette demande doit être faite à partir d'un compte de gestion AWS Organizations. Lorsque vous exécutez la commande suivante, vérifiez que vous utilisez un rôle avec une stratégie IAM autorisant les actions suivantes :

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

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

La sortie suivante doit s'afficher. Elle indique que l'activation a réussi.

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

Étape 2 : création d'un IPAM

Suivez les étapes de cette section pour créer un IPAM et afficher des informations supplémentaires sur les portées créées. Vous utiliserez cet IPAM lorsque vous créerez des groupes et que vous provisionnerez des plages d'adresses IP pour ces groupes lors d'étapes ultérieures.

> **Note**
>
> L'option OperatingRegions (Régions d'exploitation) détermine les Régions AWS pour lesquelles les groupes IPAM peuvent être utilisés. Pour plus d'informations sur les Régions d'opération, consultez Création d'un IPAM.

Pour créer un IPAM à l'aide d'AWS CLI

1. Exécutez la commande suivante pour créer l'instance IPAM.

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

Lorsque vous créez un IPAM, AWS effectue automatiquement les actions suivantes :

- Renvoi d'un ID de ressource globalement unique (`IpamId`) pour l'IPAM.
- Création d'une portée publique par défaut (`PublicDefaultScopeId`) et d'une portée privée par défaut (`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. Exécutez la commande suivante pour afficher des informations supplémentaires relatives aux portées. La portée publique est destinée aux adresses IP qui seront accessibles via l'Internet public. La portée privée est destinée aux adresses IP qui ne seront pas accessibles via l'Internet public.

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

Les portées disponibles sont indiquées dans la sortie. Vous allez utiliser l'ID de portée privée à l'étape suivante.


```
{
    "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
        }
    ]
}
```


Étape 3 : création d'un groupe d'adresses IPv4

Suivez les étapes de cette section pour créer un groupe d'adresses IPv4.

> **Important**
>
> Vous n'utiliserez pas l'option `--locale` sur ce groupe de niveau supérieur. Vous définirez l'option locale plus tard sur le groupe Régional. L'option locale est la Région AWS dans laquelle vous souhaitez qu'un groupe soit disponible pour les allocations CIDR. En raison

de l'absence de paramètres pour l'option locale sur le groupe de niveau supérieur, les paramètres seront définis par défaut sur `None`. Si un groupe possède une option locale de `None`, le groupe ne sera pas disponible pour les ressources VPC dans aucune Région AWS. Vous pouvez uniquement allouer manuellement de l'espace pour adresse IP dans le groupe pour réserver de l'espace.

Pour créer un groupe d'adresses IPv4 pour toutes vos ressources AWS utilisant AWS CLI

1. Exécutez la commande suivante pour créer un groupe d'adresses IPv4. Utilisez l'ID de portée privée de l'IPAM que vous avez créé à l'étape précédente.

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

   Dans la sortie, le groupe affichera l'état `create-in-progress`.

```
{
    "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. Exécutez la commande suivante jusqu'à ce que l'état `create-complete` apparaisse dans la sortie.

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

L'exemple de sortie suivant illustre le bon état.

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

Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur

Suivez les étapes de cette section pour provisionner un CIDR au groupe de niveau supérieur, puis vérifier que le CIDR est provisionné. Pour de plus amples informations, veuillez consulter Approvisionnement de CIDR à un groupe.

Pour provisionner un bloc d'adresse CIDR au groupe à l'aide d'AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

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

Dans la sortie, vous pouvez vérifier l'état de l'approvisionnement.

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

2. Exécutez la commande suivante jusqu'à ce que l'état `provisioned` apparaisse dans la sortie.

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

L'exemple de sortie suivant illustre le bon état.

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

Étape 5. Création d'un groupe régional avec un CIDR provenant du groupe de niveau supérieur

Lorsque vous créez un groupe IPAM, celui-ci appartient par défaut à la Région AWS de l'IPAM. Lorsque vous créez un VPC, le groupe duquel il provient doit se trouver dans la même Région que le VPC. Vous pouvez utiliser l'option `--locale` lorsque vous créez un groupe pour le rendre disponible pour les services d'une Région autre que la Région de l'IPAM. Suivez les étapes de cette section pour créer un groupe régional dans un autre paramètre régional.

Pour créer un groupe avec un CIDR provenant du groupe précédent à l'aide d'AWS CLI

1. Exécutez la commande suivante pour créer le groupe et insérer un espace avec un CIDR disponible connu provenant du groupe précédent.

```
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
```

Dans la sortie, vous verrez l'ID du groupe que vous avez créé. Vous aurez besoin de cet ID à la prochaine étape.

```
{
    "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. Exécutez la commande suivante jusqu'à ce que l'état `create-complete` apparaisse dans la sortie.

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

Dans la sortie, vous verrez les groupes que vous avez dans votre IPAM. Dans ce tutoriel, nous avons créé un groupe de niveau supérieur et un groupe régional. Vous verrez donc les deux.

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

Étape 6 : approvisionnement d'un CIDR au groupe régional

Suivez les étapes de cette section pour attribuer un bloc d'adresse CIDR au groupe et vérifier qu'il a été correctement provisionné.

Pour attribuer un bloc d'adresse CIDR au groupe régional à l'aide d'AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

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

La sortie indiquera l'état du groupe.

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

2. Exécutez la commande suivante jusqu'à ce que l'état `provisioned` apparaisse dans la sortie.

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

L'exemple de sortie suivant illustre le bon état.

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

3. Exécutez la commande suivante pour interroger le groupe de niveau supérieur afin d'afficher les allocations. Le groupe régional est considéré comme une allocation au sein du groupe de niveau supérieur.

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

Dans la sortie, le groupe régional est indiqué comme une allocation dans le groupe de niveau supérieur.

```
{
```

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

Étape 7. Création d'un partage RAM pour activer les attributions IP entre les comptes

Cette étape est facultative. Vous ne pouvez effectuer cette étape que si vous avez terminé Intégrer l'IPAM aux comptes d'une organisation AWS.

La création d'un partage AWS RAM pour un groupe IPAM permet d'activer les attributions IP entre les comptes. Le partage RAM n'est disponible que dans votre Région AWS d'origine. Notez que vous créez ce partage dans la même Région que l'IPAM, et non dans la Région locale du groupe. Toutes les opérations administratives sur les ressources de l'IPAM sont effectuées par l'intermédiaire de la région d'origine votre IPAM. L'exemple de ce tutoriel crée un partage unique pour un groupe unique, mais vous pouvez ajouter plusieurs groupes à un seul partage. Pour plus d'informations, y compris une explication des options que vous devez saisir, consultez Partage d'un groupe IPAM à l'aide d'AWS RAM.

Exécutez la commande suivante pour créer un partage de ressources.

```
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
```

La sortie montre que le groupe a été créé.

```
{
    "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
    }
}
```

Étape 8. Création d'un VPC

Exécutez la commande suivante pour créer un VPC et attribuer un bloc d'adresse CIDR au VPC à partir du groupe de votre nouvel IPAM.

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

La sortie montre que le VPC a été créé.

```
{
    "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
    }
}
```

Étape 9. Nettoyage

Suivez les étapes de cette section pour supprimer les ressources IPAM que vous avez créées dans ce tutoriel.

1. Supprimer le VPC.

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

2. Supprimez le partage RAM du groupe IPAM.

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

3. Désactivez le CIDR du groupe régional.

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

4. Désactivez le CIDR du groupe de niveau supérieur.

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

5. Supprimez l'IPAM.

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

Didacticiel : affichez l'historique des adresses IP à l'aide de AWS CLI

Les scénarios de cette section vous montrent comment analyser et auditer l'utilisation des adresses IP à l'aide de l'AWS CLI. Pour obtenir des informations générales sur l'utilisation de l'AWS CLI, voirUtilisation deAWS CLIdans leAWSGuide de l'utilisateur de l'interface de ligne de commande.

Table des matières

- Présentation
- Scénarios

Présentation

IPAM retient automatiquement les données de surveillance des adresses IP pendant trois ans maximum. Vous pouvez utiliser les données historiques pour analyser et auditer vos politiques de routage et de sécurité réseau. Vous pouvez rechercher des informations historiques pour les types de ressources suivants :

- VPC
- Sous-réseaux VPC
- Adresses IP élastiques
- Instances EC2 en cours d'exécution
- Interfaces réseau EC2 connectées à des instances

Important

Bien qu'IPAM ne contrôle pas les instances Amazon EC2 ou les interfaces réseau EC2, reliées aux instances, vous pouvez utiliser la fonction d'historique de recherche d'IP pour rechercher des données historiques sur des CIDR d'interface réseau et d'instance EC2.

Note

- Les commandes de ce didacticiel doivent être exécutées à l'aide du compte propriétaire de l'IPAM et duAWSRégion qui héberge l'IPAM.
- Les enregistrements des modifications apportées aux CIDR sont capturés dans des instantanés périodiques, ce qui signifie que l'affichage ou la mise à jour des enregistrements peut prendre un certain temps, et les valeurs de SampledStartTime et SampledEndTime peuvent différer des heures réelles de leur apparition.

Scénarios

Les scénarios de cette section vous montrent comment analyser et auditer l'utilisation des adresses IP à l'aide de l'AWS CLI. Pour plus d'informations sur les valeurs mentionnées dans ce didacticiel, telles que l'heure de fin et l'heure de début échantillonnées, voirAfficher l'historique des adresses IP.

Scénario 1 : Quelles ressources ont été associées **10.2.1.155/32** entre 1 h et 21 h 00 le 27 décembre 2021 (UTC) ?

1. Exécutez la commande suivante :

```
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. Affichez les résultats de l'analyse. Dans l'exemple ci-dessous, le CIDR a été alloué à une interface réseau et à une instance EC2 au cours de la période. Remarque : une absence de valeur SampledEndTime signifie que le dossier est toujours actif. Pour plus d'informations sur les valeurs affichées dans la sortie suivante, consultez Afficher l'historique des adresses IP.

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

Si l'ID du propriétaire de l'instance à laquelle une interface réseau est attachée diffère de l'ID propriétaire de l'interface réseau (comme c'est le cas pour les passerelles NAT, les interfaces réseau Lambda dans les VPC et autresAWSservices), le `ResourceOwnerId` est `amazon-`

aws plutôt que l'ID de compte du propriétaire de l'interface réseau. L'exemple suivant montre l'enregistrement d'un CIDR associé à une passerelle NAT :

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

Scénario 2 : Quelles ressources ont été associées **10.2.1.0/24** entre le 1er décembre 2021 et le 27 décembre 2021 (UTC) ?

1. Exécutez la commande suivante :

```
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. Affichez les résultats de l'analyse. Dans l'exemple ci-dessous, le CIDR a été alloué à un sous-réseau et VPC au cours de la période. Remarque : une absence de valeur SampledEndTime signifie que le dossier est toujours actif. Pour plus d'informations sur les valeurs affichées dans la sortie suivante, consultez Afficher l'historique des adresses IP.

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


Scénario 3 : Quelles ressources ont été associées **2605:9cc0:409::/56** entre le 1er décembre 2021 et le 27 décembre 2021 (UTC) ?

1. Exécutez la commande suivante, où —region est la région d'origine IPAM :

```
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. Affichez les résultats de l'analyse. Dans l'exemple ci-dessous, le CIDR a été alloué à deux VPC différents au cours de la période dans une région située en dehors de la région d'origine de l'IPAM. Remarque : une absence de valeur SampledEndTime signifie que le dossier est toujours actif. Pour plus d'informations sur les valeurs affichées dans la sortie suivante, consultez Afficher l'historique des adresses IP.


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

Scénario 4 : Quelles ressources ont été associées **10.0.0.0/24** au cours des dernières 24 heures (en supposant que l'heure actuelle soit minuit le 27 décembre 2021 (UTC)) ?

1. Exécutez la commande suivante :

```
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. Affichez les résultats de l'analyse. Dans l'exemple ci-dessous, le CIDR a été alloué à plusieurs sous-réseaux et VPC au cours de la période. Remarque : une absence de valeur SampledEndTime signifie que le dossier est toujours actif. Pour plus d'informations sur les valeurs affichées dans la sortie suivante, consultez Afficher l'historique des adresses IP.

```
{
```

```
    "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"
        }
    ]
}
```

Scénario 5 : Quelles ressources sont actuellement associées avec **`10.2.1.155/32`** ?

1. Exécutez la commande suivante :

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

2. Affichez les résultats de l'analyse. Dans l'exemple ci-dessous, le CIDR a été alloué à une interface réseau et à une instance EC2 pendant la période. Remarque : une absence de valeur SampledEndTime signifie que le dossier est toujours actif. Pour plus d'informations sur les valeurs affichées dans la sortie suivante, consultez Afficher l'historique des adresses IP.

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

Scénario 6 : Quelles ressources sont actuellement associées avec **10.2.1.0/24** ?

1. Exécutez la commande suivante :

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

2. Affichez les résultats de l'analyse. Dans l'exemple ci-dessous, le CIDR a été alloué à un VPC et sous-réseau au cours de la période. Seuls les résultats qui correspondent exactement à ce résultat /24Les CIDR sont retournés, pas tous /32 au sein du/24CIDR. Remarque : une absence de valeur SampledEndTime signifie que le dossier est toujours actif. Pour plus d'informations sur les valeurs affichées dans la sortie suivante, consultez Afficher l'historique des adresses IP.

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

Scénario 7 : Quelles ressources sont actuellement associées avec **`54.0.0.9/32`** ?

Dans cet exemple, `54.0.0.9/32` est attribué à une adresse IP élastique qui ne fait pas partie de l'AWSOrganization intégrée à votre IPAM.

1. Exécutez la commande suivante :

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

2. Depuis que `54.0.0.9/32` est attribué à une adresse IP élastique qui ne fait pas partie de l'AWSOrganization intégrée à l'IPAM dans cet exemple, aucun dossier n'est renvoyé.

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

Didacticiel : apporter votre ASN à l'IPAM

Si vos applications utilisent des adresses IP fiables et des numéros de système autonome (ASN) que vos partenaires ou clients ont autorisés sur leur réseau, vous pouvez exécuter ces applications AWS sans demander à vos partenaires ou clients de modifier leurs listes d'autorisation.

Un numéro de système autonome (ASN) est un numéro globalement unique qui permet d'identifier un groupe de réseaux sur Internet et d'échanger des données de routage avec d'autres réseaux de manière dynamique à l'aide du Protocole Border Gateway. Les fournisseurs de services Internet (FSI), par exemple, utilisent des ASN pour identifier la source du trafic réseau. Toutes les organisations n'achètent pas leur propre ASN, mais celles qui le font peuvent apporter leur ASN à. AWS

Le numéro de système autonome (BYOASN) vous permet de publier les adresses IP auxquelles vous accédez AWS avec votre propre ASN public au lieu de l'ASN. AWS Lorsque vous utilisez le BYOASN, le trafic provenant de votre adresse IP transporte votre ASN au lieu de l' AWS ASN, et vos charges de travail sont accessibles aux clients ou aux partenaires qui ont autorisé le trafic répertorié en fonction de votre adresse IP et de votre ASN.

Important

- Effectuez ce didacticiel en utilisant le compte administrateur IPAM dans la région d'accueil de votre IPAM.
- Ce didacticiel part du principe que vous possédez l'ASN public que vous souhaitez apporter à IPAM et que vous avez déjà apporté un CIDR BYOIP AWS et l'avez provisionné dans un pool de votre périmètre public. Vous pouvez apporter un ASN à l'IPAM à tout moment, mais pour l'utiliser, vous devez l'associer à un CIDR que vous avez ajouté à votre compte. AWS Ce tutoriel suppose que vous l'avez déjà fait. Pour plus d'informations, consultez Didacticiel : apporter vos adresses IP à IPAM.
- Vous pouvez changer sans délai entre votre propre ASN publicitaire ou un AWS ASN, mais vous êtes limité à passer d'un AWS ASN à votre propre ASN une fois par heure.
- Si votre CIDR BYOIP est publié actuellement, vous n'avez pas à le retirer de la publicité pour l'associer à votre ASN.

Conditions préalables à l'onboarding de votre ASN

Vous aurez besoin des éléments suivants pour suivre ce didacticiel :

- Votre ASN public de 2 ou 4 octets.
- Si vous avez déjà apporté une plage d'adresses IP à AWS withDidacticiel : apporter vos adresses IP à IPAM, vous avez besoin de la plage CIDR d'adresses IP. Vous aurez également besoin d'une clé privée. Vous pouvez utiliser la clé privée que vous avez créée lorsque vous avez introduit la plage d'adresses IP CIDR AWS ou vous pouvez créer une nouvelle clé privée comme décrit dans Création d'une clé privée et génération d'un certificat X.509 dans le guide de l'utilisateur EC2.
- Lorsque vous apportez une plage d'adresses IP à AWS withDidacticiel : apporter vos adresses IP à IPAM, vous créez un certificat X.509 et vous le téléchargez dans l'enregistrement RDAP de votre RIR. Vous devez charger le même certificat que vous avez créé dans le registre RDAP de votre RIR pour l'ASN. Veillez à inclure le `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` avant et après la partie encodée. Tout ce contenu doit se trouver sur une seule et longue ligne. La procédure de mise à jour de RDAP dépend de votre RIR :
  - Pour ARIN, utilisez le portail du gestionnaire de compte pour ajouter le certificat dans la section « Commentaires publics » pour l'objet « Informations réseau » représentant votre ASN à

l'aide de l'option « Modifier l'ASN ». Ne l'ajoutez pas à la section des commentaires de votre organisation.

- Pour RIPE, ajoutez le certificat en tant que nouveau champ « descr » à l'objet « aut-num » représentant votre ASN. Vous les trouverez généralement dans la section « Mes ressources » du portail de la base de données RIPE. Ne l'ajoutez pas dans la section des commentaires de votre organisation ni dans le champ « remarques » de l'objet « aut-num ».
- Pour l'APNIC, envoyez le certificat par e-mail à l'adresse helpdesk@apnic.net afin de l'ajouter manuellement au champ « remarques » de votre ASN. Envoyez l'e-mail en utilisant le contact autorisé APNIC pour l'ASN.

Étapes du didacticiel

Effectuez les étapes ci-dessous à l'aide de la AWS console ou du AWS CLI.

AWS Management Console

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation de gauche, sélectionnez IPAMs.
3. Choisissez votre IPAM.
4. Choisissez l'onglet BYOASNs, puis Provisionner BYOASNs.
5. Saisissez l'ASN. Par conséquent, le champ Message est automatiquement renseigné avec le message que vous devrez vous connecter à l'étape suivante.

   - Le format du message est le suivant, où ACCOUNT est votre numéro de AWS compte, ASN est l'ASN que vous apportez à IPAM et YYYYMMDD est la date d'expiration du message (qui par défaut est le dernier jour du mois suivant). Exemple :

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

6. Copiez le message et remplacez la date d'expiration par votre propre valeur si vous le souhaitez.
7. Signez le message à l'aide de la clé privée. Exemple :

   ```
   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. Sous Signature, entrez la signature.
9. (Facultatif) Pour configurer un autre ASN, choisissez Provisionner un autre ASN. Vous pouvez provisionner jusqu'à 5 ASN. Pour augmenter ce quota, consultez Quotas pour votre IPAM.
10. Choisissez Provisionner.
11. Consultez le processus de provisionnement dans l'onglet BYOASNs. Attendez que l'État passe de Provisionnement en attente à Provisionné. Les BYOASN dont l'état est de Provisionnement échoué sont automatiquement supprimés au bout de 7 jours. Une fois que l'ASN est correctement provisionné, vous pouvez l'associer à un CIDR BYOIP.
12. Dans le panneau de navigation de gauche, choisissez Groupes.
13. Choisissez votre portée publique. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
14. Choisissez un groupe régional auquel un CIDR BYOIP est provisionné. Le Service du groupe doit être défini sur EC2 et un paramètre régional doit être choisi.
15. Choisissez l'onglet CIDRs et sélectionnez un CIDR BYOIP.
16. Choisissez Actions > Gérer les associations BYOASN.
17. Sous Associated ByoASN, choisissez l'ASN auquel vous avez accédé. AWS Si vous avez plusieurs ASN, vous pouvez associer plusieurs ASN au CIDR BYOIP. Vous pouvez associer autant d'ASN que vous pouvez apporter à IPAM. Notez que vous pouvez apporter jusqu'à 5 ASN à l'IPAM par défaut. Pour plus d'informations, consultez Quotas pour votre IPAM.
18. Choisissez Associer.
19. Attendez que l'association d'ASN soit terminée. Une fois que l'ASN est correctement associé au CIDR BYOIP, vous pouvez à nouveau publier le CIDR BYOIP.
20. Choisissez l'onglet CIDRs pour groupe.
21. Sélectionnez le CIDR BYOIP et cliquez sur Actions >Publicité. Par conséquent, vos options d'ASN sont affichées : l'ASN Amazon et tous les ASN que vous avez apportés à IPAM.
22. Sélectionnez l'ASN que vous avez apporté à l'IPAM et choisissez Publicité CIDR. Par conséquent, le CIDR BYOIP est annoncé et la valeur dans la colonne Publicité passe de Retiré à Publié. La colonne Numéro de système autonome affiche l'ASN associé au CIDR.
23. (facultatif) Si vous décidez de reconvertir l'association d'ASN en Amazon ASN, sélectionnez le CIDR BYOIP, puis choisissez à nouveau Actions > Publicité. Cette fois, choisissez l'ASN Amazon. Vous pouvez revenir à l'ASN Amazon à tout moment, mais vous ne pouvez passer à un ASN personnalisé qu'une fois par heure.

Le didacticiel est terminé.

Nettoyage

1. Dissocier l'ASN du CIDR BYOIP

   - Pour retirer le CIDR BYOIP de la publicité, dans votre groupe dans la portée publique, choisissez le CIDR BYOIP et choisissez Actions > Retirer de la publicité.
   - Pour dissocier l'ASN du CIDR, choisissez Actions > Gérer les associations BYOASN.

2. Déprovisionner l'ASN

   - Pour déprovisionner l'ASN, sous l'onglet BYOASNs, choisissez l'ASN, puis choisissez Déprovisionner l'ASN. Par conséquent, l'ASN est déprovisionné. Les BYOASN dont l'état est de Déprovisionné sont automatiquement supprimés au bout de 7 jours.

Le nettoyage est terminé.

Command line

1. Fournissez votre ASN en incluant votre ASN et votre message d'autorisation. La signature est le message signé avec votre clé privée.

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

2. Décrivez votre ASN pour suivre le processus de provisionnement. Si la demande aboutit, l'ProvisionStatusensemble devrait être provisionné au bout de quelques minutes.

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

3. Associez votre ASN à votre CIDR BYOIP. Tout ASN personnalisé à partir duquel vous souhaitez faire de la publicité doit d'abord être associé à votre CIDR.

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

4. Décrivez votre CIDR pour suivre le processus d'association.

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

5. Publiez votre CIDR avec votre ASN. Si le CIDR est déjà publié, cela remplacera l'ASN d'origine d'Amazon par le vôtre.

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

6. Décrivez votre CIDR pour voir l'état de l'ASN passer d'associé à publié.

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

Le didacticiel est terminé.

Nettoyage

1. Effectuez l’une des actions suivantes :

   - Pour retirer uniquement votre publicité ASN et recommencer à utiliser les ASN Amazon tout en maintenant le CIDR annoncé, vous devez appeler advertise-byoip-cidr avec la AWS valeur spéciale du paramètre asn. Vous pouvez revenir à l'ASN Amazon à tout moment, mais vous ne pouvez passer à un ASN personnalisé qu'une fois par heure.

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

   - Pour retirer simultanément votre publicité CIDR et ASN, vous pouvez appeler. withdraw-byoip-cidr

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

2. Pour nettoyer votre ASN, vous devez d'abord le dissocier de votre CIDR BYOIP.

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

3. Une fois que votre ASN est dissocié de tous les CIDR BYOIP auxquels vous l'avez associé, vous pouvez le déprovisionner.

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

4. Le CIDR BYOIP peut également être déprovisionné une fois que toutes les associations ASN ont été supprimées.

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

5. Confirmez le déprovisionnement.

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

Le nettoyage est terminé.

Didacticiel : apporter vos adresses IP à IPAM

Les didacticiels de cette section vous expliquent comment intégrer un espace d'adresse IP public AWS et comment gérer cet espace avec IPAM.

La gestion de l'espace d'adressage IP public avec IPAM présente les avantages suivants :

- Améliore l'utilisation des adresses IP publiques dans votre organisation : vous pouvez utiliser IPAM pour partager l'espace d'adressage IP entre des comptes AWS . Si vous n'utilisez pas IPAM, vous ne pouvez pas partager votre espace IP public entre les comptes AWS Organizations.
- Simplifie le processus d'attribution d'un espace IP public à AWS : vous pouvez utiliser IPAM pour intégrer l'espace d'adresses IP public une seule fois, puis utiliser IPAM pour distribuer vos adresses IP publiques entre les régions. Sans IPAM, vous devez intégrer vos adresses IP publiques pour chaque AWS région.

⚠ Important

- Avant de commencer ce didacticiel, suivez les étapes décrites dans la section Conditions d'intégration requises pour votre plage d'adresses BYOIP dans le guide de l'utilisateur Amazon EC2.

  Lorsque vous créez les ROA, pour les CIDR IPv4, vous devez définir la longueur maximale d'un préfixe d'adresse IP sur `/24`. Pour les CIDR IPv6, si vous les ajoutez à un groupe annoncé, la longueur maximale d'un préfixe d'adresse IP doit être `/48`. Cela vous garantit une flexibilité totale pour répartir votre adresse IP publique entre AWS les régions. L'IPAM applique la longueur maximale que vous avez définie. La longueur maximale est la plus

petite annonce de longueur de préfixe que vous autorisez pour cet acheminement. Par exemple, si vous apportez un bloc d'adresse CIDR `/20` dans AWS, en définissant la longueur maximale sur `/24`, vous pouvez diviser un grand bloc comme vous le souhaitez (par exemple avec `/21`, `/22` ou`/24`) et distribuer ces blocs d'adresse CIDR plus petits dans n'importe quelle Région. Si vous définissez la longueur maximale sur `/23`, vous ne serez pas en mesure de diviser et de publier un bloc `/24` à partir du bloc plus grand. Notez également que `/24` est le plus petit bloc IPv4 et `/48` le plus petit bloc IPv6 que vous pouvez publier depuis une Région vers Internet.

- Une fois que vous avez transféré une plage d'adresses IPv4 AWS, vous pouvez utiliser toutes les adresses IP de la plage, y compris la première adresse (adresse réseau) et la dernière adresse (adresse de diffusion).

Table des matières

- Apportez votre propre CIDR IPv4 public à IPAM à l'aide de la console de AWS gestion et de la CLI AWS
- Apportez votre propre CIDR IPv4 public à IPAM en utilisant uniquement la CLI AWS

Apportez votre propre CIDR IPv4 public à IPAM à l'aide de la console de AWS gestion et de la CLI AWS

Procédez comme suit pour transférer un CIDR IPv4 ou IPv6 à IPAM à l'aide de la console de AWS gestion et de la CLI. AWS

⚠ Important

- Avant de commencer ce didacticiel, suivez les étapes décrites dans la section Conditions d'intégration requises pour votre plage d'adresses BYOIP dans le guide de l'utilisateur Amazon EC2.

  Lorsque vous créez les ROA, pour les CIDR IPv4, vous devez définir la longueur maximale d'un préfixe d'adresse IP sur `/24`. Pour les CIDR IPv6, si vous les ajoutez à un groupe annoncé, la longueur maximale d'un préfixe d'adresse IP doit être `/48`. Cela vous garantit une flexibilité totale pour répartir votre adresse IP publique entre AWS les régions. L'IPAM applique la longueur maximale que vous avez définie. La longueur maximale est la plus petite annonce de longueur de préfixe que vous autorisez pour cet acheminement. Par

exemple, si vous apportez un bloc d'adresse CIDR `/20` dans AWS, en définissant la longueur maximale sur `/24`, vous pouvez diviser un grand bloc comme vous le souhaitez (par exemple avec `/21`, `/22` ou`/24`) et distribuer ces blocs d'adresse CIDR plus petits dans n'importe quelle Région. Si vous définissez la longueur maximale sur `/23`, vous ne serez pas en mesure de diviser et de publier un bloc `/24` à partir du bloc plus grand. Notez également que `/24` est le plus petit bloc IPv4 et `/48` le plus petit bloc IPv6 que vous pouvez publier depuis une Région vers Internet.

- Une fois que vous avez introduit une plage d'adresses IPv4 AWS, vous pouvez utiliser toutes les adresses IP de la plage, y compris la première adresse (adresse réseau) et la dernière adresse (adresse de diffusion).

Table des matières

- Apportez votre propre CIDR IPv4 à IPAM à l'aide de la console de AWS gestion et de la CLI AWS
- Apportez votre propre CIDR IPv6 sur IPAM à l'aide du AWS Console de gestion

Apportez votre propre CIDR IPv4 à IPAM à l'aide de la console de AWS gestion et de la CLI AWS

Procédez comme suit pour transférer un CIDR IPv4 vers IPAM et allouer une adresse IP élastique (EIP) à l'aide de la console de AWS gestion et de la CLI. AWS

Important

- Vous ne pouvez pas provisionner ou publier des plages d’adresses BYOIP dans les zones locales pour le moment.
- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :
  - Intégrer l'IPAM aux comptes d'une organisation AWS.
  - Création d'un IPAM.
- Chaque étape de ce didacticiel doit être effectuée par l'un des trois comptes AWS Organizations :
  - Le compte de gestion

- Le compte de membre configuré pour être votre administrateur IPAM dansIntégrer l'IPAM aux comptes d'une organisation AWS. Dans ce tutoriel, ce compte sera appelé compte IPAM.
- Le compte membre de votre organisation qui allouera des CIDR à partir d'un groupe IPAM. Dans ce tutoriel, ce compte sera appelé compte IPAM.

Table des matières

- Étape 1 : Création de profils AWS CLI nommés et de rôles IAM
- Étape 2 : Création d'un groupe IPAM niveau supérieur
- Étape 3. Création d'un groupe régional dans le groupe de niveau supérieur
- Étape 4 : Partager le groupe régional
- Étape 5 : création d'un groupe IPv4 public
- Étape 6 : allocation du CIDR IPv4 public à votre groupe IPv4 public
- Étape 7 : création d'une adresse IP Elastic à partir du groupe IPv4 public
- Étape 8 : association de l'adresse IP Elastic à une instance EC2
- Étape 9 : publication du CIDR
- Étape 10 : nettoyage

Étape 1 : Création de profils AWS CLI nommés et de rôles IAM

Pour suivre ce didacticiel en tant qu' AWS utilisateur unique, vous pouvez utiliser des profils AWS CLI nommés pour passer d'un rôle IAM à un autre. Les profils nommés sont des ensembles de paramètres et d'informations d'identification auxquels vous vous référez lorsque vous utilisez l'option `--profile` associée à l' AWS CLI. Pour plus d'informations sur la création de rôles IAM et de profils nommés pour les AWS comptes, consultez la section Utilisation d'un rôle IAM dans la AWS CLI du guide de l'utilisateur AWS d'Identity and Access Management.

Créez un rôle et un profil nommé pour chacun des trois AWS comptes que vous utiliserez dans ce didacticiel :

- Un profil appelé le compte `management-account` de gestion des AWS Organizations.
- Un profil appelé `ipam-account` pour le compte membre AWS des Organizations configuré pour être votre administrateur IPAM.

- Un profil appelait `member-account` le compte membre AWS Organizations de votre organisation qui allouera les CIDR à partir d'un pool IPAM.

Une fois que vous avez créé les rôles IAM et les profils nommés, revenez à cette page et passez à l'étape suivante. Vous remarquerez dans le reste de ce didacticiel que les exemples de AWS CLI commandes utilisent l'`--profile`option avec l'un des profils nommés pour indiquer quel compte doit exécuter la commande.

Étape 2 : Création d'un groupe IPAM niveau supérieur

Suivez les étapes de cette section pour créer un groupe IPAM de niveau supérieur.

Cette étape doit être réalisée par le compte IPAM.

Création d'un groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Choisissez la portée Public. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Sélectionnez Create pool (Créer un groupe).
5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une Description du groupe.
6. Sous Source, choisissez Portée IPAM.
7. SousAddress family (Famille d'adresses), choisissezIPv4.
8. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
9. SousLocale (paramètre régional), choisissezAucun.

   Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les

paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP.

L'intégration IPAM avec BYOIP nécessite que les paramètres régionaux soient définis sur le groupe utilisé pour le CIDR BYOIP. Puisque nous allons créer un groupe IPAM de niveau supérieur contenant un groupe régional et que nous allons allouer de l'espace à une adresse IP élastique à partir du groupe régional, vous définirez les paramètres régionaux sur le groupe régional, et non sur le groupe de niveau supérieur. Vous ajouterez les paramètres régionaux au groupe régional lorsque vous le créerez à une étape ultérieure.

> **Note**
>
> Si vous créez un groupe unique uniquement et non un groupe de niveau supérieur comportant des groupes régionaux, vous devez choisir un paramètre régional pour ce groupe afin que le groupe soit disponible pour les allocations.

10. Sous Source IP publique, sélectionnez l'une des options suivantes :

    - BYOIP : vous fournissez votre propre plage d'adresses IPv4 ou IPv6 (BYOIP) à ce groupe.
    - Propriété d’Amazon : vous souhaitez qu’Amazon provisionne une plage d’adresses IPv6 à ce groupe.

11. Effectuez l’une des actions suivantes :

    - Si vous avez choisi BYOIP à l'étape précédente, sous CIDR à provisionner, sélectionnez un CIDR à provisionner pour le groupe. Notez que lors de l'approvisionnement d'un CIDR IPv4 à un groupe au sein du groupe de niveau supérieur, le CIDR IPv4 minimum que vous pouvez approvisionner est `/24`; les CIDR plus spécifiques (tels que `/25`) ne sont pas autorisés. Vous devez inclure le CIDR, le message BYOIP et la signature de certificat dans la demande afin que nous puissions vérifier que vous êtes propriétaire de l'espace public. Pour obtenir la liste des conditions préalables BYOIP, y compris comment obtenir ce message BYOIP et cette signature de certificat, voirApportez votre propre CIDR IPv4 public à IPAM à l'aide de la console de AWS gestion et de la CLI AWS.

> **Important**
>
> Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'approvisionnement pour les gammes pouvant faire l'objet d'une publicité publique peut prendre jusqu'à une semaine.

- Si vous avez choisi Propriété d'Amazon, sous Longueur du masque de réseau, sélectionnez une longueur de masque réseau comprise entre `/40` et `/52`. La valeur par défaut est `/52`.

12. Laissez l'option Configurer les paramètres des règles d'allocation de ce groupe non sélectionnée.
13. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
14. Sélectionnez Create pool (Créer un groupe).

Vérifiez que ce CIDR a été provisionné avant de continuer. Vous pouvez voir l'état de l'approvisionnement dans l'onglet CIDRdans la page des détails du groupe.

Étape 3. Création d'un groupe régional dans le groupe de niveau supérieur

Création d'un groupe régional dans le groupe de niveau supérieur L'intégration IPAM avec BYOIP nécessite que les paramètres régionaux soient définis sur le groupe utilisé pour le CIDR BYOIP. Vous ajouterez les paramètres régionaux au groupe régional lorsque vous le créerez dans cette section. Le `Locale`doit être l'une des régions d'exploitation que vous avez configurées lorsque vous avez créé l'IPAM.

Cette étape doit être réalisée par le compte IPAM.

Création d'un groupe dans un groupe de niveau supérieur

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Si vous ne souhaitez pas utiliser la portée privée par défaut, dans le menu déroulant en haut du panneau de contenu, choisissez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Sélectionnez Create pool (Créer un groupe).

5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une Description du groupe.
6. Sous Source, sélectionnez le groupe de niveau supérieur que vous avez créé dans la section précédente.
7. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
8. Sous Paramètres régionaux, choisissez les paramètres régionaux du groupe. Dans ce didacticiel, nous allons utiliser `us-east-2`comme paramètre régional pour le groupe régional. Les options disponibles proviennent des Régions d'exploitation que vous avez sélectionnées lors de la création de votre IPAM.

   Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP. Le choix d'un paramètre régional garantit qu'il n'y a aucune dépendance entre les Régions entre votre groupe et les ressources qui y sont allouées.
9. Sous Service, choisissez EC2 (EIP/VPC). Le service que vous sélectionnez détermine le AWS service pour lequel le CIDR sera publicisé. Actuellement, la seule option est EC2 (EIP/VPC), ce qui signifie que les CIDR alloués à partir de ce groupe pourront être annoncés pour le service Amazon EC2 (pour les adresses IP Elastic) et le service Amazon VPC (pour les CIDR associés aux VPC).
10. Sous CIDR à allouer, choisissez un CIDR à allouer pour le groupe. Notez que lors de l'approvisionnement d'un CID à un groupe au sein du groupe de niveau supérieur, le CIDR IPv4 minimum que vous pouvez approvisionner est `/24`; les CIDR plus spécifiques (tels que `/25`) ne sont pas autorisés. Après avoir créé le premier pool régional, vous pouvez créer des pools plus petits (tels que`/25`) au sein du pool régional.
11. Activez l’option Configurer les paramètres des règles d’allocation de ce groupe. Vous disposez ici des mêmes options de règle d'allocation que lorsque vous avez créé le groupe de premier niveau. Consultez Création d'un groupe IPv4 de niveau supérieur pour obtenir une explication des options disponibles lorsque vous créez des groupes. Les règles d'allocation du groupe

régional ne sont pas héritées du groupe de niveau supérieur. Si vous n'appliquez aucune règle ici, aucune règle d'allocation ne sera définie pour le groupe.

12. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
13. Lorsque vous avez fini de configurer votre groupe, choisissez Create pool (Créer un groupe).

Vérifiez que ce CIDR a été provisionné avant de continuer. Vous pouvez voir l'état de l'approvisionnement dans l'onglet CIDRdans la page des détails du groupe.

Étape 4 : Partager le groupe régional

Suivez les étapes décrites dans cette section pour partager le pool IPAM à l'aide de AWS Resource Access Manager (RAM).

Activer le partage des ressources dans AWS RAM

Après avoir créé votre IPAM, partagez le groupe régional avec d'autres comptes de votre organisation. Avant de partager un pool IPAM, suivez les étapes décrites dans cette section pour activer le partage de ressources avec AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`management-account`**option.

Pour activer le partage des ressources

1. À l'aide du compte AWS Organizations de gestion, ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram/.
2. Dans le volet de navigation de gauche, choisissez Paramètres, sélectionnez Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

Vous pouvez désormais partager un groupe IPAM avec d'autres membres de l'organisation.

Partagez un pool IPAM à l'aide de AWS RAM

Dans cette section, vous allez partager le pool régional avec un autre compte AWS Organizations membre. Pour obtenir des instructions complètes sur le partage de groupes IPAM, y compris des informations sur les autorisations IAM requises, consultez Partage d'un groupe IPAM à l'aide d'AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`ipam-account`**option.

Pour partager un pool IPAM à l'aide de AWS RAM

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez l'étendue privée, choisissez le pool IPAM, puis choisissez Actions > Afficher les détails.
4. Sous Resource sharing (Partage de ressources), sélectionnez Create resource share (Créer un partage de ressources). La AWS RAM console s'ouvre. Vous partagez le pool en utilisant AWS RAM.
5. Sélectionnez Create a resource share (Créer un partage de ressources).
6. Dans la AWS RAM console, choisissez à nouveau Créer un partage de ressources.
7. Ajoutez un Nom pour la ressource partagée.
8. Sous Sélectionner le type de ressource, choisissez les pools IPAM, puis l'ARN du pool que vous souhaitez partager.
9. Choisissez Suivant.
10. Choisissez l'AWSRAMPermissionIpamPoolByoipCidrImportautorisation. Les détails des options d'autorisation ne sont pas abordés dans ce didacticiel, mais vous pouvez en savoir plus sur ces options dans Partage d'un groupe IPAM à l'aide d'AWS RAM.
11. Choisissez Suivant.
12. Dans Principaux > Sélectionner le type de principal, choisissez Compte AWS , saisissez l'ID du compte qui transmettra une plage d'adresses IP à IPAM, puis choisissez Ajouter.
13. Choisissez Suivant.
14. Examinez les options de partage de ressources et les principaux avec lesquels vous procéderez au partage, puis sélectionnez Créer.
15. Pour autoriser le compte **`member-account`** à allouer les CIDR de l'adresse IP à partir du groupe IPAM, créez un deuxième partage de ressources avec `AWSRAMDefaultPermissionsIpamPool` et créez un deuxième partage de ressources. La valeur pour `--resource-arns` est l'ARN du groupe IPAM que vous avez créé dans la section précédente. La valeur de `--principals` est l'ID de compte du**`member-account`**. La valeur pour `--permission-arns` est l'ARN de l'autorisation `AWSRAMDefaultPermissionsIpamPool`.

Étape 5 : création d'un groupe IPv4 public

La création d'un groupe IPv4 public est une étape requise afin de fournir une adresse IPv4 publique à AWS à gérer avec IPAM. Cette étape doit être effectuée par le compte membre qui fournira une adresse IP élastique.

> **Important**
>
> - Cette étape doit être effectuée par le compte membre en utilisant le AWS CLI.
> - Les pools IPv4 publics et les pools IPAM sont gérés par des ressources distinctes dans. AWS Les groupes IPv4 publics sont des ressources de compte unique qui vous permettent de convertir vos CIDR publics en adresses IP Elastic. Les groupes IPAM vous permettent d'allouer votre espace public à des groupes IPv4 publics.

Pour créer un pool IPv4 public à l'aide du AWS CLI

- Exécutez la commande suivante pour provisionner le CIDR. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option `Locale` que vous avez choisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

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

  Dans la sortie, vous verrez apparaître l'ID du groupe IPv4 public. Vous aurez besoin de cet ID à la prochaine étape.

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

Étape 6 : allocation du CIDR IPv4 public à votre groupe IPv4 public

Provisionnez le CIDR IPv4 public à votre groupe IPv4 public. La valeur pour `--region` doit correspondre à la valeur `Locale` que vous avez choisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP. `--netmask-length` est la quantité d'espace du groupe IPAM que vous souhaitez apporter à votre groupe publique. La valeur ne peut pas être supérieure à la longueur du

masque réseau du groupe IPAM. Le préfixe IPv4 le moins spécifique que vous pouvez apporter est `/24`.

> **Note**
>
> Si vous apportez une plage de CIDR `/24` à IPAM pour la partager au sein d'une organisation AWS , vous pouvez attribuer des préfixes plus petits à plusieurs groupes IPAM, par exemple `/27` (avec `-- netmask-length 27`), plutôt que de provisionner l'intégralité du CIDR `/24` (avec `-- netmask-length 24`) comme indiqué dans ce didacticiel.

> **Important**
>
> Cette étape doit être effectuée par le compte membre en utilisant le AWS CLI.

Pour créer un pool IPv4 public à l'aide du AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

```
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
```

   Dans la sortie, vous verrez apparaître le CIDR provisionné.

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

2. Exécutez la commande suivante pour afficher le CIDR provisionné dans le groupe IPv4 public.

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

Dans la sortie, vous verrez apparaître le CIDR provisionné. Par défaut, le CIDR n'est pas publié, ce qui signifie qu'il n'est pas accessible publiquement sur Internet. Vous aurez la possibilité de définir ce CIDR comme publié dans la dernière étape de ce tutoriel.


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


Une fois que vous avez créé le groupe IPv4 public, pour afficher le groupe IPv4 public alloué dans le groupe régional IPAM, ouvrez la console IPAM et affichez l'allocation dans le groupe régional sousAllocationsouRessources.

Étape 7 : création d'une adresse IP Elastic à partir du groupe IPv4 public

Suivez les étapes décrites dans la section Allouer une adresse IP élastique dans le guide de l'utilisateur Amazon EC2 pour créer une adresse IP élastique (EIP) à partir du pool IPv4 public. Lorsque vous ouvrez EC2 dans la console de AWS gestion, la AWS région dans laquelle vous allouez l'EIP doit correspondre à l'`Locale`option que vous avez choisie lors de la création du pool qui sera utilisé pour le CIDR BYOIP.

Cette étape doit être effectuée par le compte membre. Si vous utilisez le AWS CLI, utilisez l'`--profile` **`member-account`**option.

Étape 8 : association de l'adresse IP Elastic à une instance EC2

Suivez les étapes décrites dans Associer une adresse IP élastique à une instance ou à une interface réseau dans le guide de l'utilisateur Amazon EC2 pour associer l'EIP à une instance EC2. Lorsque vous ouvrez EC2 dans la console de AWS gestion, la AWS région à laquelle vous associez l'EIP doit correspondre à l'`Locale`option que vous avez choisie lors de la création du pool qui sera utilisé pour le CIDR BYOIP. Dans ce tutoriel, il s'agit de votre groupe régional.

Cette étape doit être effectuée par le compte membre. Si vous utilisez le AWS CLI, utilisez l'`--profile` **`member-account`**option.

Étape 9 : publication du CIDR

Les étapes de cette section doivent être réalisées par le compte IPAM. Une fois que vous avez associé l'adresse IP élastique (EIP) à une instance ou à Elastic Load Balancer, vous pouvez commencer à annoncer le CIDR que vous avez apporté et qui se trouve dans un pool sur AWS lequel le Service EC2 (EIP/VPC) est configuré. Dans ce didacticiel, il s'agit de votre groupe régional. Par défaut, le CIDR n'est pas publié, ce qui signifie qu'il n'est pas accessible publiquement sur Internet.

Cette étape doit être réalisée par le compte IPAM.

Pour publier le CIDR

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Choisissez la portée Public. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Choisissez le groupe régional que vous avez créé dans ce didacticiel.
5. Cliquez sur l'onglet CIDR.
6. Sélectionnez le CIDR BYOIP et cliquez sur Actions >Publicité.
7. Cliques sur Publicité CIDR.

Par conséquent, le CIDR BYOIP est annoncé et la valeur dans la colonne Publicité passe deRetiré à Annoncé.

Étape 10 : nettoyage

Suivez les étapes de cette section pour nettoyer les ressources que vous avez provisionnées et créées dans ce tutoriel.

Étape 1 : Retirez le CIDR de la publicité

Cette étape doit être réalisée par le compte IPAM.

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Choisissez la portée Public.
4. Choisissez le groupe régional que vous avez créé dans ce didacticiel.
5. Cliquez sur l'onglet CIDR.
6. Sélectionnez le CIDR BYOIP et cliquez sur Actions >Enlever de la publicité.
7. Cliquez sur Enlever CIDR.

Par conséquent, le CIDR BYOIP n'est plus annoncé et la valeur dans la colonne Publicité passe de Annoncé à Retiré.

Étape 2 : Dissocier une adresse IP élastique

Cette étape doit être effectuée par le compte membre. Si vous utilisez le AWS CLI, utilisez l'`--profile` **`member-account`**option.

- Suivez les étapes décrites dans Dissocier une adresse IP élastique dans le guide de l'utilisateur Amazon EC2 pour dissocier l'EIP. Lorsque vous ouvrez EC2 dans la console de AWS gestion, la AWS région dans laquelle vous dissociez l'EIP doit correspondre à l'`Locale`option que vous avez choisie lors de la création du pool qui sera utilisé pour le CIDR BYOIP. Dans ce tutoriel, il s'agit de votre groupe régional.

Étape 3 : Affectation de l'adresse IP élastique

Cette étape doit être effectuée par le compte membre. Si vous utilisez le AWS CLI, utilisez l'`--profile` **`member-account`**option.

- Suivez les étapes décrites dans la section Libérer une adresse IP élastique dans le guide de l'utilisateur Amazon EC2 pour libérer une adresse IP élastique (EIP) depuis le pool IPv4 public. Lorsque vous ouvrez EC2 dans la console de AWS gestion, la AWS région dans laquelle vous allouez l'EIP doit correspondre à l'`Locale`option que vous avez choisie lors de la création du pool qui sera utilisé pour le CIDR BYOIP.

Étape 4 : désapprovisionnement du CIDR IPv4 public à votre groupe IPv4 public

> **Important**
>
> Cette étape doit être effectuée par le compte membre en utilisant le AWS CLI.

1. Affichez vos CIDR BYOIP.

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

Dans la sortie, vous verrez apparaître les adresses IP dans votre CIDR BYOIP.

```
{
    "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. Exécutez la commande suivante pour libérer la dernière adresse IP du CIDR à partir du groupe IPv4 public. Saisissez l'adresse IP avec un masque de réseau de `/32`.

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

Dans la sortie, vous verrez le CIDR désactivé.

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

> **Important**
>
> Vous devez réexécuter cette commande pour chaque adresse IP de la plage d'adresses CIDR. Si votre CIDR est un `/24`, vous devrez exécuter cette commande pour désapprovisionner chacune des 256 adresses IP du CIDR `/24`.

3. Consultez à nouveau vos CIDR BYOIP et vérifiez qu'il n'y a plus d'adresses provisionnées. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à la Région de votre IPAM.

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

Dans la sortie, vous verrez le nombre d'adresses IP dans votre groupe IPv4 public.

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

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

> **Note**
>
> IPAM peut prendre un certain temps pour découvrir que les allocations publiques de groupe IPv4 ont été supprimées. Vous ne pouvez pas continuer à nettoyer et à désactiver le CIDR du groupe IPAM tant que vous ne voyez pas que l'allocation a été supprimée d'IPAM.

Étape 5 : Supprimer le groupe public IPv4

Cette étape doit être effectuée par le compte membre.

- Exécutez la commande suivante pour supprimer le CIDR provisionné dans le groupe IPv4 public. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option `Locale` que vous avez choisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP. Dans ce tutoriel, il s'agit de votre groupe régional. Cette étape doit être effectuée à l'aide de la AWS CLI.

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

  Dans la sortie, vous verrez la valeur de retourvrai.

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

  Une fois que vous avez supprimé le groupe, pour afficher l'allocation non gérée par IPAM, ouvrez la console IPAM et affichez les détails du groupe régional sousAllocations.

Étape 6 : suppression des partages RAM et désactivation de l'intégration de la RAM avec AWS Organizations

Cette étape doit être effectuée par le compte IPAM et le compte de gestion respectivement. Si vous utilisez le AWS CLI pour supprimer les partages de RAM et désactiver l'intégration de RAM, utilisez les `--profile management-account` options `--profile ipam-account` et.

- Suivez les étapes décrites dans les sections Suppression d'un partage de ressources dans la AWS RAM et Désactivation du partage de ressources avec AWS les organisations dans le guide de l'utilisateur de la AWS RAM, dans cet ordre, pour supprimer les partages de RAM et désactiver l'intégration de la RAM avec AWS les organisations.

Étape 7 : Désaprovisionner les CIDR du groupe régional et du groupe de niveau supérieur

Cette étape doit être réalisée par le compte IPAM. Si vous utilisez le AWS CLI pour partager le pool, utilisez l'`--profile ipam-account`option.

- Suivez les étapes de Pour désapprovisionner un CIDR de groupepour désaprovisionner les CIDR du groupe régional, puis du groupe de niveau supérieur, dans cet ordre.

Étape 8 : Supprimer le groupe régional et le groupe de niveau supérieur

Cette étape doit être réalisée par le compte IPAM. Si vous utilisez le AWS CLI pour partager le pool, utilisez l'`--profile ipam-account`option.

- Suivez les étapes de Suppression d'un groupepour supprimer le groupe régional et ensuite le groupe de niveau supérieur, dans cet ordre.

Apportez votre propre CIDR IPv6 sur IPAM à l'aide du AWS Console de gestion

Suivez les étapes de ce didacticiel pour transférer un CIDR IPv6 à IPAM et allouer un VPC avec le CIDR en utilisant à la fois la console de gestion et le AWS . AWS CLI

> **Important**
>
> - Vous ne pouvez pas provisionner ou publier des plages d’adresses BYOIP dans les zones locales pour le moment.

- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :
  - Intégrer l'IPAM aux comptes d'une organisation AWS.
  - Création d'un IPAM.
- Chaque étape de ce didacticiel doit être effectuée par l'un des trois comptes AWS Organizations :
  - Le compte de gestion
  - Le compte de membre configuré pour être votre administrateur IPAM dansIntégrer l'IPAM aux comptes d'une organisation AWS. Dans ce tutoriel, ce compte sera appelé compte IPAM.
  - Le compte membre de votre organisation qui allouera des CIDR à partir d'un groupe IPAM. Dans ce tutoriel, ce compte sera appelé compte IPAM.

Table des matières

- Étape 1 : Création d'un groupe IPAM de niveau supérieur
- Étape 2. Création d'un groupe régional dans le groupe de niveau supérieur
- Étape 3. Partager le groupe régional
- Étape 4 : création d'un VPC
- Étape 5 : publication du CIDR
- Étape 6 : nettoyage

Étape 1 : Création d'un groupe IPAM de niveau supérieur

Puisque vous allez créer un pool IPAM de haut niveau contenant un pool régional, et que nous allons allouer de l'espace à une ressource du pool régional, vous allez définir les paramètres régionaux sur le pool régional et non sur le pool de niveau supérieur. Vous ajouterez les paramètres régionaux au groupe régional lorsque vous le créerez à une étape ultérieure. L'intégration IPAM avec BYOIP nécessite que les paramètres régionaux soient définis sur le groupe utilisé pour le CIDR BYOIP.

Cette étape doit être réalisée par le compte IPAM.

Création d'un groupe

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.

2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Choisissez la portée Public. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Sélectionnez Create pool (Créer un groupe).
5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une Description du groupe.
6. Sous Source, choisissez Portée IPAM.
7. SousAddress family (Famille d'adresses), choisissezIPv6.

   Lorsque vous choisissez IPv6, une option de bascule apparaît qui vous permet de contrôler s'il est AWS possible d'annoncer publiquement les CIDR de ce pool. Conservez cette option activée.
8. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
9. Assurez que Autoriser les CIDR de ce groupe à être publiquement publicésest sélectionné.
10. SousLocale (paramètre régional), choisissezAucun. Vous définirez les paramètres régionaux sur le groupe régional.

    Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP.

    > **Note**
    >
    > Si vous créez un groupe unique uniquement et non un groupe de niveau supérieur comportant des groupes régionaux, vous devez choisir un paramètre régional pour ce groupe afin que le groupe soit disponible pour les allocations.
11. Sous Source IP publique, BYOIP est sélectionné par défaut.

12. Sous CIDR à allouer, choisissez un CIDR à allouer pour le groupe. Notez que lorsque vous fournissez un CIDR IPv6 à un pool au sein du pool de niveau supérieur, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR pouvant faire l'objet d'une publicité publique et /60 pour les CIDR non publicisés. Vous devez inclure le CIDR, le message BYOIP et la signature de certificat dans la demande afin que nous puissions vérifier que vous êtes propriétaire de l'espace public. Pour obtenir la liste des conditions préalables BYOIP, y compris comment obtenir ce message BYOIP et cette signature de certificat, voirApportez votre propre CIDR IPv4 public à IPAM à l'aide de la console de AWS gestion et de la CLI AWS.

    > **Important**
    >
    > Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'approvisionnement pour les gammes pouvant faire l'objet d'une publicité publique peut prendre jusqu'à une semaine.

13. Laissez l'option Configurer les paramètres des règles d'allocation de ce groupe non sélectionnée.
14. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
15. Sélectionnez Create pool (Créer un groupe).

Vérifiez que ce CIDR a été provisionné avant de continuer. Vous pouvez voir l'état de l'approvisionnement dans l'onglet CIDRdans la page des détails du groupe.

Étape 2. Création d'un groupe régional dans le groupe de niveau supérieur

Création d'un groupe régional dans le groupe de niveau supérieur Un paramètre régional est obligatoire sur le groupe ; il doit s'agir de l'une des Régions d'exploitation que vous avez configurées lors de la création de l'IPAM.

Cette étape doit être réalisée par le compte IPAM.

Création d'un groupe dans un groupe de niveau supérieur

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Si vous ne souhaitez pas utiliser la portée privée par défaut, dans le menu déroulant en haut du panneau

de contenu, choisissez la portée que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.

4. Sélectionnez Create pool (Créer un groupe).
5. (Facultatif) Ajoutez une valeur Name tag (Étiquette de nom) du groupe et une description du groupe.
6. Sous Source, sélectionnez le groupe de niveau supérieur que vous avez créé dans la section précédente.
7. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée. Pour plus d'informations sur l'utilisation de cette option pour planifier l'espace IP de sous-réseau dans un VPC, consultez Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau.
8. Choisissez les paramètres régionaux du groupe. La sélection d'un paramètre régional garantit qu'il n'y a aucune dépendance régionale entre votre groupe et les ressources qui y sont allouées. Les options disponibles proviennent des Régions d'exploitation que vous avez sélectionnées lors de la création de votre IPAM. Dans ce didacticiel, nous allons utiliser `us-east-2`comme paramètre régional pour le groupe régional.

   Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP.
9. Sous Service, choisissez EC2 (EIP/VPC). Le service que vous sélectionnez détermine le AWS service pour lequel le CIDR sera publicisé. Actuellement, la seule option est EC2 (EIP/VPC), ce qui signifie que les CIDR alloués à partir de ce pool seront publicisés pour le service Amazon EC2 et le service Amazon VPC (pour les CIDR associés aux VPC).
10. Sous CIDR à allouer, choisissez un CIDR à allouer pour le groupe. Notez que lorsque vous fournissez un CIDR IPv6 à un pool au sein du pool de niveau supérieur, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR pouvant faire l'objet d'une publicité publique et /60 pour les CIDR non publicisés.
11. Activez Configurer les paramètres des règles d’allocation de ce groupe et choisissez des règles d’allocation facultatives pour ce groupe :

- Importer automatiquement les ressources découvertes : cette option n'est pas disponible si la valeur Locale (Paramètre régional) est définie sur None (Aucun). Si cette option est sélectionnée, IPAM recherchera en permanence les ressources dans la plage CIDR de ce groupe et les importera automatiquement sous forme d'allocations dans votre IPAM. Notez ce qui suit :
  - Les CIDR qui seront alloués à ces ressources ne doivent pas déjà être alloués à d'autres ressources pour que l'importation réussisse.
  - IPAM importera un CIDR indépendamment de sa conformité avec les règles d'allocation du groupe, de sorte qu'une ressource puisse être importée puis marquée comme non conforme.
  - Si IPAM découvre plusieurs CIDR qui se chevauchent, IPAM n'importera que le plus grand CIDR.
  - Si IPAM découvre plusieurs CIDR avec des CIDR correspondants, IPAM n'importera qu'un seul d'entre eux de manière aléatoire.
- Longueur minimale du masque réseau : la longueur minimale du masque réseau requise pour que les allocations CIDR dans ce groupe IPAM soient conformes et le bloc d'adresse CIDR de la plus grande taille pouvant être alloué à partir du groupe. La longueur minimale du masque réseau doit être inférieure à la longueur maximale du masque réseau. Les longueurs possibles du masque réseau pour les adresses IPv4 sont `0` - `32`. Les longueurs possibles du masque réseau pour les adresses IPv6 sont `0` - `128`.
- Longueur du masque réseau par défaut : longueur de masque réseau par défaut pour les allocations ajoutées à ce groupe.
- Longueur maximale du masque réseau : longueur maximale du masque réseau requise pour les allocations CIDR dans ce groupe. Cette valeur dicte le bloc d'adresse CIDR de la plus petite taille pouvant être alloué à partir du groupe. Assurez-vous que cette valeur est minimale**`/48`**.
- Exigences d'étiquette : étiquettes requises pour que les ressources allouent de l'espace à partir du groupe. Si les étiquettes des ressources ont été modifiées après l'allocation de l'espace ou si les règles d'étiquette des allocations sont modifiées sur le groupe, la ressource peut être marquée comme non conforme.
- Paramètres régionaux : paramètres régionaux requis pour les ressources qui utilisent des CIDR de ce groupe. Les ressources importées automatiquement qui ne possèdent pas ces paramètres régionaux seront marquées non conformes. Les ressources qui ne sont pas

automatiquement importées dans le groupe ne seront pas autorisées à allouer de l'espace à partir du groupe à moins qu'elles ne se trouvent dans ces paramètres régionaux.

12. (Facultatif) Choisissez Tags (Étiquettes) pour le groupe.
13. Lorsque vous avez fini de configurer votre groupe, choisissez Create pool (Créer un groupe).

Vérifiez que ce CIDR a été provisionné avant de continuer. Vous pouvez voir l'état de l'approvisionnement dans l'onglet CIDRdans la page des détails du groupe.

Étape 3. Partager le groupe régional

Suivez les étapes décrites dans cette section pour partager le pool IPAM à l'aide de AWS Resource Access Manager (RAM).

Activer le partage des ressources dans AWS RAM

Après avoir créé votre IPAM, partagez le groupe régional avec d'autres comptes de votre organisation. Avant de partager un pool IPAM, suivez les étapes décrites dans cette section pour activer le partage de ressources avec AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`management-account`**option.

Pour activer le partage des ressources

1. À l'aide du compte AWS Organizations de gestion, ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram/.
2. Dans le volet de navigation de gauche, choisissez Paramètres, sélectionnez Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

Vous pouvez désormais partager un groupe IPAM avec d'autres membres de l'organisation.

Partagez un pool IPAM à l'aide de AWS RAM

Dans cette section, vous allez partager le pool régional avec un autre compte AWS Organizations membre. Pour obtenir des instructions complètes sur le partage de groupes IPAM, y compris des informations sur les autorisations IAM requises, consultez Partage d'un groupe IPAM à l'aide d'AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`ipam-account`**option.

Pour partager un pool IPAM à l'aide de AWS RAM

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez l'étendue privée, choisissez le pool IPAM, puis choisissez Actions > Afficher les détails.
4. Sous Resource sharing (Partage de ressources), sélectionnez Create resource share (Créer un partage de ressources). La AWS RAM console s'ouvre. Vous partagez le pool en utilisant AWS RAM.
5. Sélectionnez Create a resource share (Créer un partage de ressources).
6. Dans la AWS RAM console, choisissez à nouveau Créer un partage de ressources.
7. Ajoutez un Nom pour la ressource partagée.
8. Sous Sélectionner le type de ressource, choisissez les pools IPAM, puis l'ARN du pool que vous souhaitez partager.
9. Choisissez Suivant.
10. Choisissez l'AWSRAMPermissionIpamPoolByoipCidrImportautorisation. Les détails des options d'autorisation ne sont pas abordés dans ce didacticiel, mais vous pouvez en savoir plus sur ces options dans Partage d'un groupe IPAM à l'aide d'AWS RAM.
11. Choisissez Suivant.
12. Dans Principaux > Sélectionner le type de principal, choisissez Compte AWS , saisissez l'ID du compte qui transmettra une plage d'adresses IP à IPAM, puis choisissez Ajouter.
13. Choisissez Suivant.
14. Examinez les options de partage de ressources et les principaux avec lesquels vous procéderez au partage, puis sélectionnez Créer.
15. Pour autoriser le compte **`member-account`** à allouer les CIDR de l'adresse IP à partir du groupe IPAM, créez un deuxième partage de ressources avec `AWSRAMDefaultPermissionsIpamPool` et créez un deuxième partage de ressources. La valeur pour `--resource-arns` est l'ARN du groupe IPAM que vous avez créé dans la section précédente. La valeur de `--principals` est l'ID de compte du**`member-account`**. La valeur pour `--permission-arns` est l'ARN de l'autorisation `AWSRAMDefaultPermissionsIpamPool`.

Étape 4 : création d'un VPC

Suivez les étapes décrites dans la section Création d'un VPC du Guide de l'utilisateur Amazon VPC.

Cette étape doit être effectuée par le compte membre.

> **Note**
>
> - Lorsque vous ouvrez un VPC dans la console de AWS gestion, la AWS région dans laquelle vous créez le VPC doit correspondre à l'`Locale`option que vous avez choisie lors de la création du pool qui sera utilisé pour le CIDR BYOIP.
> - Lorsque vous arrivez à l'étape du choix de CIDR pour le VPC, vous aurez la possibilité d'utiliser un CIDR à partir d'un groupe IPAM. Choisissez le groupe régional que vous avez créé dans ce didacticiel.

Lorsque vous créez le VPC, AWS alloue un CIDR dans le pool IPAM au VPC. Vous pouvez afficher l'allocation dans IPAM en choisissant un groupe dans le panneau de contenu de la console IPAM et en affichant l'onglet Allocations du groupe.

Étape 5 : publication du CIDR

Les étapes de cette section doivent être réalisées par le compte IPAM. Une fois que vous avez créé le VPC, vous pouvez commencer à annoncer le CIDR que vous avez apporté et AWS qui se trouve dans le pool sur lequel le Service EC2 (EIP/VPC) est configuré. Dans ce didacticiel, il s'agit de votre groupe régional. Par défaut, le CIDR n'est pas publié, ce qui signifie qu'il n'est pas accessible publiquement sur Internet.

Cette étape doit être réalisée par le compte IPAM.

Pour publier le CIDR

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Choisissez la portée Public. Pour plus d'informations sur les portées, consultez Fonctionnement d'IPAM.
4. Choisissez le groupe régional que vous avez créé dans ce didacticiel.

5. Cliquez sur l'onglet CIDR.
6. Sélectionnez le CIDR BYOIP et cliquez sur Actions >Publicité.
7. Cliques sur Publicité CIDR.

Par conséquent, le CIDR BYOIP est annoncé et la valeur dans la colonne Publicité passe deRetiré à Annoncé.

Étape 6 : nettoyage

Suivez les étapes de cette section pour nettoyer les ressources que vous avez provisionnées et créées dans ce tutoriel.

Étape 1 : Retirez le CIDR de la publicité

Cette étape doit être réalisée par le compte IPAM.

1. Ouvrez la console IPAM à partir de l'adresse https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Par défaut, lorsque vous créez un groupe, la portée privée par défaut est sélectionnée. Choisissez la portée Public.
4. Choisissez le groupe régional que vous avez créé dans ce didacticiel.
5. Cliquez sur l'onglet CIDR.
6. Sélectionnez le CIDR BYOIP et cliquez sur Actions >Enlever de la publicité.
7. Cliquez sur Enlever CIDR.

Par conséquent, le CIDR BYOIP n’est plus annoncé et la valeur dans la colonne Publicité passe deAnnoncé à Retiré.

Étape 2 : Supprimer le VPC.

Cette étape doit être effectuée par le compte membre.

- Suivez les étapes deSuppression d'un VPCdans leGuide de l'utilisateur d'un VPC Amazonpour supprimer le VPC. Lorsque vous ouvrez un VPC dans la console de AWS gestion, la AWS région dans laquelle le VPC est supprimé doit correspondre à l'`Locale`option que vous avez choisie lors de la création du pool qui sera utilisé pour le CIDR BYOIP. Dans ce didacticiel, il s'agit de votre groupe régional.

Lorsque vous supprimez le VPC, il faut du temps à IPAM pour découvrir que la ressource a été supprimée et pour décaler le CIDR alloué au VPC. Vous ne pouvez pas passer à l'étape suivante du nettoyage tant que l'IPAM n'a pas supprimé l'allocation du pool dans les détails du pool.Allocationsonglet.

Étape 3 : Supprimer les partages de RAM et désactiver l'intégration de la RAM avec AWS Organizations

Cette étape doit être effectuée par le compte IPAM et le compte de gestion respectivement.

- Suivez les étapes décrites dans les sections Suppression d'un partage de ressources dans la AWS RAM et Désactivation du partage de ressources avec AWS les organisations dans le guide de l'utilisateur de la AWS RAM, dans cet ordre, pour supprimer les partages de RAM et désactiver l'intégration de la RAM avec AWS les organisations.

Étape 4 : Désaprovisionner les CIDR du groupe régional et du groupe de niveau supérieur

Cette étape doit être réalisée par le compte IPAM.

- Suivez les étapes de Pour désapprovisionner un CIDR de groupepour désaprovisionner les CIDR du groupe régional, puis du groupe de niveau supérieur, dans cet ordre.

Étape 5 : Supprimer le groupe régional et le groupe de niveau supérieur

Cette étape doit être réalisée par le compte IPAM.

- Suivez les étapes de Suppression d'un groupepour supprimer le groupe régional et ensuite le groupe de niveau supérieur, dans cet ordre.

Apportez votre propre CIDR IPv4 public à IPAM en utilisant uniquement la CLI AWS

Suivez ces étapes pour transférer un CIDR IPv4 ou IPv6 à IPAM en utilisant uniquement la CLI. AWS

Important

- Avant de commencer ce didacticiel, suivez les étapes décrites dans la section Conditions d'intégration requises pour votre plage d'adresses BYOIP dans le guide de l'utilisateur Amazon EC2.

  Lorsque vous créez les ROA, pour les CIDR IPv4, vous devez définir la longueur maximale d'un préfixe d'adresse IP sur `/24`. Pour les CIDR IPv6, si vous les ajoutez à un groupe annoncé, la longueur maximale d'un préfixe d'adresse IP doit être `/48`. Cela vous garantit une flexibilité totale pour répartir votre adresse IP publique entre AWS les régions. L'IPAM applique la longueur maximale que vous avez définie. La longueur maximale est la plus petite annonce de longueur de préfixe que vous autorisez pour cet acheminement. Par exemple, si vous apportez un bloc d'adresse CIDR `/20` dans AWS, en définissant la longueur maximale sur `/24`, vous pouvez diviser un grand bloc comme vous le souhaitez (par exemple avec `/21`, `/22` ou`/24`) et distribuer ces blocs d'adresse CIDR plus petits dans n'importe quelle Région. Si vous définissez la longueur maximale sur `/23`, vous ne serez pas en mesure de diviser et de publier un bloc `/24` à partir du bloc plus grand. Notez également que `/24` est le plus petit bloc IPv4 et `/48` le plus petit bloc IPv6 que vous pouvez publier depuis une Région vers Internet.
- Une fois que vous avez introduit une plage d'adresses IPv4 AWS, vous pouvez utiliser toutes les adresses IP de la plage, y compris la première adresse (adresse réseau) et la dernière adresse (adresse de diffusion).

Table des matières

- Apportez votre propre CIDR IPv4 public à IPAM en utilisant uniquement la CLI AWS
- Apportez votre propre CIDR IPv6 à l'IPAM en utilisant uniquement la CLI AWS

Apportez votre propre CIDR IPv4 public à IPAM en utilisant uniquement la CLI AWS

Suivez ces étapes pour fournir un CIDR IPv4 à IPAM et allouer une adresse IP Elastic (EIP) avec le CIDR à l’aide de AWS CLI uniquement.

Important

- Vous ne pouvez pas provisionner ou publier des plages d'adresses BYOIP dans les zones locales pour le moment.
- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :
  - Intégrer l'IPAM aux comptes d'une organisation AWS.
  - Création d'un IPAM.
- Chaque étape de ce didacticiel doit être effectuée par l'un des trois comptes AWS Organizations :
  - Le compte de gestion
  - Le compte de membre configuré pour être votre administrateur IPAM dansIntégrer l'IPAM aux comptes d'une organisation AWS. Dans ce tutoriel, ce compte sera appelé compte IPAM.
  - Le compte membre de votre organisation qui allouera des CIDR à partir d'un groupe IPAM. Dans ce tutoriel, ce compte sera appelé compte IPAM.

Table des matières

- Étape 1 : Création de profils AWS CLI nommés et de rôles IAM
- Étape 2 : création d'un IPAM
- Étape 3 : Création d'un groupe IPAM de niveau supérieur
- Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur
- Étape 5 : Création d'un groupe régional dans le groupe de niveau supérieur
- Étape 6 : approvisionnement d'un CIDR au groupe régional
- Étape 7. Partager le groupe régional
- Étape 8 : création d'un groupe IPv4 public
- Étape 9 : allocation du CIDR IPv4 public à votre groupe IPv4 public
- Étape 10 : création d'une adresse IP Elastic à partir du groupe IPv4 public
- Étape 11 : publication du CIDR
- Étape 12 : nettoyage

Étape 1 : Création de profils AWS CLI nommés et de rôles IAM

Pour suivre ce didacticiel en tant qu' AWS utilisateur unique, vous pouvez utiliser des profils AWS CLI nommés pour passer d'un rôle IAM à un autre. Les profils nommés sont des ensembles de paramètres et d'informations d'identification auxquels vous vous référez lorsque vous utilisez l'option `--profile` associée à l' AWS CLI. Pour plus d'informations sur la création de rôles IAM et de profils nommés pour les AWS comptes, consultez la section Utilisation d'un rôle IAM dans la AWS CLI du guide de l'utilisateur AWS d'Identity and Access Management.

Créez un rôle et un profil nommé pour chacun des trois AWS comptes que vous utiliserez dans ce didacticiel :

- Un profil appelé le compte `management-account` de gestion des AWS Organizations.
- Un profil appelé `ipam-account` pour le compte membre AWS des Organizations configuré pour être votre administrateur IPAM.
- Un profil appelait `member-account` le compte membre AWS Organizations de votre organisation qui allouera les CIDR à partir d'un pool IPAM.

Une fois que vous avez créé les rôles IAM et les profils nommés, revenez à cette page et passez à l'étape suivante. Vous remarquerez dans le reste de ce didacticiel que les exemples de AWS CLI commandes utilisent l'`--profile`option avec l'un des profils nommés pour indiquer quel compte doit exécuter la commande.

Étape 2 : création d'un IPAM

Cette étape est facultative. Si vous avez déjà créé un IPAM avec les Régions d'exploitation de `us-east-1` et `us-west-2` créées, vous pouvez ignorer cette étape. Créez un IPAM et spécifiez une Région d'exploitation de `us-east-1` et `us-west-2`. Vous devez sélectionner une Région d'exploitation pour pouvoir utiliser l'option des paramètres régionaux lorsque vous créez votre groupe IPAM. L'intégration IPAM avec BYOIP nécessite que les paramètres régionaux soient définis sur le groupe utilisé pour le CIDR BYOIP.

Cette étape doit être réalisée par le compte IPAM.

Exécutez la commande suivante :

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

Dans la sortie, vous verrez l'IPAM que vous avez créé. Provisionnez un bloc d'adresse CIDR au groupe de niveau supérieur. Vous aurez besoin de votre ID de portée publique à l'étape suivante. Vous utilisez la portée publique, car les CIDR BYOIP sont des adresses IP publiques ; c'est à cela que la portée publique est destinée.


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


Étape 3 : Création d'un groupe IPAM de niveau supérieur

Suivez les étapes de cette section pour créer un groupe IPAM de niveau supérieur.

Cette étape doit être réalisée par le compte IPAM.

Pour créer un pool d'adresses IPv4 pour toutes vos AWS ressources à l'aide du AWS CLI

1. Exécutez la commande suivante pour créer un groupe IPAM. Utilisez l'ID de portée publique de l'IPAM que vous avez créé à l'étape précédente.

   Cette étape doit être réalisée par le compte IPAM.

   ```
   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
   ```

Dans la sortie, vous verrez apparaître `create-in-progress`, qui indique que la création du groupe est en cours.

```
{
    "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. Exécutez la commande suivante jusqu'à ce que l'état `create-complete` apparaisse dans la sortie.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

L'exemple de sortie suivant illustre l'état du groupe.

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

Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur

Allouez un bloc d'adresse CIDR au groupe de niveau supérieur. Notez que lors de l'approvisionnement d'un CIDR IPv4 à un groupe au sein du groupe de niveau supérieur, le CIDR IPv4 minimum que vous pouvez approvisionner est `/24`; les CIDR plus spécifiques (tels que `/25`) ne sont pas autorisés. Vous devez inclure le CIDR, le message BYOIP et la signature de certificat dans la demande afin que nous puissions vérifier que vous êtes propriétaire de l'espace public. Pour obtenir la liste des conditions préalables BYOIP, y compris comment obtenir ce message BYOIP et cette signature de certificat, voir Apportez votre propre CIDR IPv4 public à IPAM en utilisant uniquement la CLI AWS.

Cette étape doit être réalisée par le compte IPAM.

> **Important**
>
> Vous devez uniquement ajouter `--cidr-authorization-context` lorsque vous provisionnez le CIDR BYOIP au groupe de niveau supérieur. Pour le groupe régional au sein du groupe de niveau supérieur, vous pouvez omettre l'option `--cidr-authorization-context`. Une fois que vous avez intégré votre BYOIP à IPAM, vous n'êtes pas obligé d'effectuer une validation de propriété lorsque vous divisez le BYOIP entre les Régions et les comptes.

Pour fournir un bloc CIDR au pool à l'aide du AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

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

Dans la sortie, vous verrez le CIDR en attente d'approvisionnement.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Vérifiez que ce CIDR a été provisionné avant de continuer.

> **Important**
>
> Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'approvisionnement pour les gammes pouvant faire l'objet d'une publicité publique peut prendre jusqu'à une semaine.

Exécutez la commande suivante jusqu'à ce que l'état `provisioned` apparaisse dans la sortie.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

L'exemple de sortie suivant illustre l'état.

```
{
```

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

Étape 5 : Création d'un groupe régional dans le groupe de niveau supérieur

Créez un groupe régional dans le groupe de niveau supérieur. `--locale` est obligatoire sur le groupe ; il doit s'agir de l'une des Régions d'exploitation que vous avez configurées lors de la création de l'IPAM. Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour les allocations. Par exemple, vous pouvez uniquement allouer un CIDR à un VPC à partir d'un groupe IPAM qui partage un paramètre régional avec la Région du VPC. Notez que lorsque vous avez choisi un paramètre régional pour un groupe, vous ne pouvez pas le modifier. Si la région d'accueil de l'IPAM n'est pas disponible en raison d'une panne et que les paramètres régionaux du groupe sont différents de ceux de la région d'accueil de l'IPAM, le groupe peut toujours être utilisé pour allouer des adresses IP.

Cette étape doit être réalisée par le compte IPAM.

La sélection d'un paramètre régional garantit qu'il n'y a aucune dépendance régionale entre votre groupe et les ressources qui y sont allouées. Les options disponibles proviennent des Régions d'exploitation que vous avez sélectionnées lors de la création de votre IPAM. Dans ce didacticiel, nous allons utiliser `us-west-2`comme paramètre régional pour le groupe régional.

> **Important**
>
> Lorsque vous créez le groupe, vous devez inclure `--aws-service ec2`. Le service que vous sélectionnez détermine le AWS service pour lequel le CIDR sera publicisé. Actuellement, la seule option est `ec2`, ce qui signifie que les CIDR alloués à partir de ce groupe pourront être annoncés pour le service Amazon EC2 (pour les adresses IP Elastic) et le service Amazon VPC (pour les CIDR associés aux VPC).

Pour créer un groupe régional à l'aide de l' AWS CLI

1. Exécutez la commande suivante pour créer le groupe.

```
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
```

Dans la sortie, vous verrez IPAM en cours de création du groupe.

```
{
     "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. Exécutez la commande suivante jusqu'à ce que l'état de `create-complete` apparaisse dans la sortie.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Dans la sortie, vous verrez les groupes que vous avez dans votre IPAM. Dans ce tutoriel, nous avons créé un groupe de niveau supérieur et un groupe régional. Vous verrez donc les deux.

Étape 6 : approvisionnement d'un CIDR au groupe régional

Provisionnez un bloc d'adresse CIDR au groupe régional. Notez que lors de l'approvisionnement d'un CID à un groupe au sein du groupe de niveau supérieur, le CIDR IPv4 minimum que vous pouvez approvisionner est `/24`; les CIDR plus spécifiques (tels que `/25`) ne sont pas autorisés. Après avoir créé le premier pool régional, vous pouvez créer des pools plus petits (tels que`/25`) au sein du pool régional.

Cette étape doit être réalisée par le compte IPAM.

Pour attribuer un bloc CIDR au pool régional à l'aide du AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

   ```
   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
   ```

   Dans la sortie, vous verrez le CIDR en attente d'approvisionnement.

   ```
   {
       "IpamPoolCidr": {

           "Cidr": "130.137.245.0/24",

           "State": "pending-provision"

       }

   }
   ```

2. Exécutez la commande suivante jusqu'à ce que l'état de `provisioned` apparaisse dans la sortie.

   ```
   aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   L'exemple de sortie suivant illustre le bon état.

   ```
   {
       "IpamPoolCidrs": [
           {
   ```

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

Étape 7. Partager le groupe régional

Suivez les étapes décrites dans cette section pour partager le pool IPAM à l'aide de AWS Resource Access Manager (RAM).

Activer le partage des ressources dans AWS RAM

Après avoir créé votre IPAM, partagez le groupe régional avec d'autres comptes de votre organisation. Avant de partager un pool IPAM, suivez les étapes décrites dans cette section pour activer le partage de ressources avec AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`management-account`**option.

Pour activer le partage des ressources

1. À l'aide du compte AWS Organizations de gestion, ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram/.
2. Dans le volet de navigation de gauche, choisissez Paramètres, sélectionnez Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

Vous pouvez désormais partager un groupe IPAM avec d'autres membres de l'organisation.

Partagez un pool IPAM à l'aide de AWS RAM

Dans cette section, vous allez partager le pool régional avec un autre compte AWS Organizations membre. Pour obtenir des instructions complètes sur le partage de groupes IPAM, y compris des informations sur les autorisations IAM requises, consultez Partage d'un groupe IPAM à l'aide d'AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`ipam-account`**option.

Pour partager un pool IPAM à l'aide de AWS RAM

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.

2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez l'étendue privée, choisissez le pool IPAM, puis choisissez Actions > Afficher les détails.
4. Sous Resource sharing (Partage de ressources), sélectionnez Create resource share (Créer un partage de ressources). La AWS RAM console s'ouvre. Vous partagez le pool en utilisant AWS RAM.
5. Sélectionnez Create a resource share (Créer un partage de ressources).
6. Dans la AWS RAM console, choisissez à nouveau Créer un partage de ressources.
7. Ajoutez un Nom pour la ressource partagée.
8. Sous Sélectionner le type de ressource, choisissez les pools IPAM, puis l'ARN du pool que vous souhaitez partager.
9. Choisissez Suivant.
10. Choisissez l'AWSRAMPermissionIpamPoolByoipCidrImportautorisation. Les détails des options d'autorisation ne sont pas abordés dans ce didacticiel, mais vous pouvez en savoir plus sur ces options dans Partage d'un groupe IPAM à l'aide d'AWS RAM.
11. Choisissez Suivant.
12. Dans Principaux > Sélectionner le type de principal, choisissez Compte AWS , saisissez l'ID du compte qui transmettra une plage d'adresses IP à IPAM, puis choisissez Ajouter.
13. Choisissez Suivant.
14. Examinez les options de partage de ressources et les principaux avec lesquels vous procéderez au partage, puis sélectionnez Créer.
15. Pour autoriser le compte **`member-account`** à allouer les CIDR de l'adresse IP à partir du groupe IPAM, créez un deuxième partage de ressources avec `AWSRAMDefaultPermissionsIpamPool` et créez un deuxième partage de ressources. La valeur pour `--resource-arns` est l'ARN du groupe IPAM que vous avez créé dans la section précédente. La valeur de `--principals` est l'ID de compte du**`member-account`**. La valeur pour `--permission-arns` est l'ARN de l'autorisation `AWSRAMDefaultPermissionsIpamPool`.

Étape 8 : création d'un groupe IPv4 public

La création d'un groupe IPv4 public est une étape requise afin de fournir une adresse IPv4 publique à AWS à gérer avec IPAM. Cette étape est généralement effectuée par un autre AWS compte qui souhaite fournir une adresse IP élastique.

Cette étape doit être effectuée par le compte membre.

> **Important**
>
> Les pools IPv4 publics et les pools IPAM sont gérés par des ressources distinctes dans. AWS Les groupes IPv4 publics sont des ressources de compte unique qui vous permettent de convertir vos CIDR publics en adresses IP Elastic. Les groupes IPAM vous permettent d'allouer votre espace public à des groupes IPv4 publics.

Pour créer un pool IPv4 public à l'aide du AWS CLI

- Exécutez la commande suivante pour provisionner le CIDR. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

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

  Dans la sortie, vous verrez apparaître l'ID du groupe IPv4 public. Vous aurez besoin de cet ID à la prochaine étape.

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

Étape 9 : allocation du CIDR IPv4 public à votre groupe IPv4 public

Provisionnez le CIDR IPv4 public à votre groupe IPv4 public. La valeur pour `--region` doit correspondre à la valeur `--locale` que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

Cette étape doit être effectuée par le compte membre.

Pour créer un pool IPv4 public à l'aide du AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

```
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
```

Dans la sortie, vous verrez apparaître le CIDR provisionné.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. Exécutez la commande suivante pour afficher le CIDR provisionné dans le groupe IPv4 public.

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-
account
```

Dans la sortie, vous verrez apparaître le CIDR provisionné. Par défaut, le CIDR n'est pas publié, ce qui signifie qu'il n'est pas accessible publiquement sur Internet. Vous aurez la possibilité de définir ce CIDR comme publié dans la dernière étape de ce tutoriel.

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

Étape 10 : création d'une adresse IP Elastic à partir du groupe IPv4 public

Créez une adresse IP Elastic (EIP) à partir du groupe IPv4 public. Lorsque vous exécutez les commandes dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

Cette étape doit être effectuée par le compte membre.

Pour créer un EIP à partir du pool IPv4 public à l'aide du AWS CLI

1. Exécutez la commande suivante pour créer l'EIP.

```
aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
ec2-0019eed22a684e0b2 --profile member-account
```

   Dans la sortie, vous verrez l'allocation.

```
{
    "PublicIp": "130.137.245.100",
    "AllocationId": "eipalloc-0db3405026756dbf6",
    "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

2. Exécutez la commande suivante pour afficher l'allocation EIP gérée dans IPAM.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   La sortie affiche l'allocation dans IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
```

```
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Étape 11 : publication du CIDR

Les étapes de cette section doivent être réalisées par le compte IPAM. Une fois que vous avez associé l'adresse IP élastique (EIP) à une instance ou à Elastic Load Balancer, vous pouvez commencer à annoncer le CIDR que vous avez apporté et qui AWS se trouve dans le pool défini. `--aws-service ec2` Dans ce didacticiel, il s'agit de votre groupe régional. Par défaut, le CIDR n'est pas publié, ce qui signifie qu'il n'est pas accessible publiquement sur Internet. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

Cette étape doit être réalisée par le compte IPAM.

Commencez à faire de la publicité pour le CIDR à l'aide du AWS CLI

- Exécutez la commande suivante pour publier le CIDR.

  ```
  aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
  profile ipam-account
  ```

  Dans la sortie, vous verrez que le CIDR est publié.

  ```
  {
      "ByoipCidr": {
          "Cidr": "130.137.245.0/24",
          "State": "advertised"
      }
  }
  ```

Étape 12 : nettoyage

Suivez les étapes de cette section pour nettoyer les ressources que vous avez provisionnées et créées dans ce tutoriel. Lorsque vous exécutez les commandes dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

Nettoyez à l'aide du AWS CLI

1. Affichez l'allocation EIP gérée dans IPAM.

   Cette étape doit être réalisée par le compte IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   La sortie affiche l'allocation dans 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. Arrêtez de faire connaître le CIDR IPv4.

   Cette étape doit être réalisée par le compte IPAM.

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
   profile ipam-account
   ```

   Dans la sortie, vous verrez que l'état du CIDR est passé de advertised (publié) à provisioned(provisionné).

   ```
   {
       "ByoipCidr": {
           "Cidr": "130.137.245.0/24",
           "State": "provisioned"
       }
   }
   ```

3. Libérez les adresses IP Elastic.

Cette étape doit être effectuée par le compte membre.

```
aws ec2 release-address --region us-west-2 --allocation-
id eipalloc-0db3405026756dbf6 --profile member-account
```

Vous ne verrez aucune sortie lorsque vous exécutez cette commande.

4. Affichez vos CIDR BYOIP.

   Cette étape doit être effectuée par le compte membre.

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

   Dans la sortie, vous verrez apparaître les adresses IP dans votre CIDR BYOIP.

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
               "Description": "",
               "PoolAddressRanges": [
                   {
                       "FirstAddress": "130.137.245.0",
                       "LastAddress": "130.137.245.255",
                       "AddressCount": 256,
                       "AvailableAddressCount": 256
                   }
               ],
               "TotalAddressCount": 256,
               "TotalAvailableAddressCount": 256,
               "NetworkBorderGroup": "us-east-1",
               "Tags": []
           }
       ]
   }
   ```

5. Libérez la dernière adresse IP du CIDR à partir du groupe IPv4 public. Saisissez l'adresse IP avec un masque de réseau de /32. Vous devez réexécuter cette commande pour chaque adresse IP de la plage d'adresses CIDR. Si votre CIDR est un `/24`, vous devrez exécuter cette commande pour désapprovisionner chacune des 256 adresses IP du CIDR `/24`. Lorsque vous

exécutez la commande dans cette section, la valeur de `--region` doit correspondre à la Région de votre IPAM.

Cette étape doit être effectuée par le compte membre.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.255/32 --profile member-account
```

Dans la sortie, vous verrez le CIDR désactivé.

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

6. Consultez à nouveau vos CIDR BYOIP et vérifiez qu'il n'y a plus d'adresses provisionnées. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à la Région de votre IPAM.

   Cette étape doit être effectuée par le compte membre.

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
   ```

   Dans la sortie, vous verrez le nombre d'adresses IP dans votre groupe IPv4 public.

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
               "Description": "",
               "PoolAddressRanges": [],
               "TotalAddressCount": 0,
               "TotalAvailableAddressCount": 0,
               "NetworkBorderGroup": "us-east-1",
               "Tags": []
   ```

```
        }
    ]
}
```

7. Affichez l'allocation EIP qui n’est plus gérée dans IPAM. IPAM peut prendre un certain temps afin de déterminer que l'adresse IP Elastic a été supprimée. Vous ne pouvez pas continuer à nettoyer et à désactiver le CIDR du groupe IPAM tant que vous ne voyez pas que l'allocation a été supprimée d'IPAM. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option --locale que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   La sortie affiche l'allocation dans IPAM.

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

8. Désapprovisionnez le CIDR du groupe régional. Lorsque vous exécutez les commandes de cette étape, la valeur de `--region` doit correspondre à la Région de votre IPAM.

   Cette étape doit être réalisée par le compte IPAM.

```
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
```

   Dans la sortie, vous verrez le CIDR en attente de désapprovisionnement.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }
```

```
}
```

Le désaprovisionnement prend un certain temps. Vérifiez le statut du désaprovisionnement.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Attendez de voir l'état désaprovisionné avant de passer à l'étape suivante.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. Supprimez les partages RAM et désactivez l'intégration de la RAM avec AWS Organizations. Suivez les étapes décrites dans les sections Suppression d'un partage de ressources dans la AWS RAM et Désactivation du partage de ressources avec AWS les organisations dans le guide de l'utilisateur de la AWS RAM, dans cet ordre, pour supprimer les partages de RAM et désactiver l'intégration de la RAM avec AWS les organisations.

   Cette étape doit être effectuée par le compte IPAM et le compte de gestion respectivement. Si vous utilisez le AWS CLI pour supprimer les partages de RAM et désactiver l'intégration de RAM, utilisez les `--profile` **`management-account`** options `--profile` **`ipam-account`** et.

10. Supprimer le groupe régional. Lorsque vous exécutez la commande dans cette étape, la valeur de `--region` doit correspondre à la Région de votre IPAM.

    Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Dans la sortie, vous pouvez voir l'état de suppression.

```
{
   "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
        "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0d8f3646b61ca5987",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "reg-ipv4-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

11. Désapprovisionnez le CIDR du groupe de niveau supérieur. Lorsque vous exécutez les commandes de cette étape, la valeur de `--region` doit correspondre à la Région de votre IPAM.

    Cette étape doit être réalisée par le compte IPAM.

    ```
    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
    ```

    Dans la sortie, vous verrez le CIDR en attente de désapprovisionnement.

    ```
    {
        "IpamPoolCidr": {

            "Cidr": "130.137.245.0/24",

            "State": "pending-deprovision"

        }
    ```

```
}
```

Le désapprovisionnement prend un certain temps. Utilisez la commande suivante pour vérifier le statut de la désapprovisionnement.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Attendez de voir l'état désaprovisionné avant de passer à l'étape suivante.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

12. Supprimer le groupe de niveau supérieur. Lorsque vous exécutez la commande dans cette étape, la valeur de `--region` doit correspondre à la Région de votre IPAM.

    Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Dans la sortie, vous pouvez voir l'état de suppression.

```
{
  "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
```

```
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

13. Supprimez l'IPAM. Lorsque vous exécutez la commande dans cette étape, la valeur de `--region` doit correspondre à la Région de votre IPAM.

    Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    Dans la sortie, vous verrez la réponse IPAM. Cela signifie que l'IPAM a été supprimé.

```
{
    "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"
            }
```

```
        ],
    }
}
```

Apportez votre propre CIDR IPv6 à l'IPAM en utilisant uniquement la CLI AWS

Suivez ces étapes pour fournir un CIDR IPv6 à IPAM et allouer un VPC en utilisant uniquement AWS CLI.

Important

- Vous ne pouvez pas provisionner ou publier des plages d'adresses BYOIP dans les zones locales pour le moment.
- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :
  - Intégrer l'IPAM aux comptes d'une organisation AWS.
  - Création d'un IPAM.
- Chaque étape de ce didacticiel doit être effectuée par l'un des trois comptes AWS Organizations :
  - Le compte de gestion
  - Le compte de membre configuré pour être votre administrateur IPAM dansIntégrer l'IPAM aux comptes d'une organisation AWS. Dans ce tutoriel, ce compte sera appelé compte IPAM.
  - Le compte membre de votre organisation qui allouera des CIDR à partir d'un groupe IPAM. Dans ce tutoriel, ce compte sera appelé compte IPAM.

Table des matières

- Étape 1 : créer des profils AWS CLI nommés et des rôles IAM
- Étape 2 : création d'un IPAM
- Étape 3 : création d'un groupe IPAM
- Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur
- Étape 5 : Création d'un groupe régional dans le groupe de niveau supérieur
- Étape 6 : approvisionnement d'un CIDR au groupe régional

- Étape 7. Partager le groupe régional
- Étape 8 : création d'un VPC à l'aide du CIDR IPv6
- Étape 9 : publication du CIDR
- Étape 10 : nettoyage

Étape 1 : créer des profils AWS CLI nommés et des rôles IAM

Pour suivre ce didacticiel en tant qu' AWS utilisateur unique, vous pouvez utiliser des profils AWS CLI nommés pour passer d'un rôle IAM à un autre. Les profils nommés sont des ensembles de paramètres et d'informations d'identification auxquels vous vous référez lorsque vous utilisez l'option `--profile` associée à l' AWS CLI. Pour plus d'informations sur la création de rôles IAM et de profils nommés pour les AWS comptes, consultez la section Utilisation d'un rôle IAM dans la AWS CLI du guide de l'utilisateur AWS d'Identity and Access Management.

Créez un rôle et un profil nommé pour chacun des trois AWS comptes que vous utiliserez dans ce didacticiel :

- Un profil appelé le compte `management-account` de gestion des AWS Organizations.
- Un profil appelé `ipam-account` pour le compte membre AWS des Organizations configuré pour être votre administrateur IPAM.
- Un profil appelait `member-account` le compte membre AWS Organizations de votre organisation qui allouera les CIDR à partir d'un pool IPAM.

Une fois que vous avez créé les rôles IAM et les profils nommés, revenez à cette page et passez à l'étape suivante. Vous remarquerez dans le reste de ce didacticiel que les exemples de AWS CLI commandes utilisent l'`--profile`option avec l'un des profils nommés pour indiquer quel compte doit exécuter la commande.

Étape 2 : création d'un IPAM

Cette étape est facultative. Si vous avez déjà créé un IPAM avec les Régions d'exploitation de `us-east-1` et `us-west-2` créées, vous pouvez ignorer cette étape. Créez un IPAM et spécifiez une Région d'exploitation de `us-east-1` et `us-west-2`. Vous devez sélectionner une Région d'exploitation pour pouvoir utiliser l'option des paramètres régionaux lorsque vous créez votre groupe IPAM. L'intégration IPAM avec BYOIP nécessite que les paramètres régionaux soient définis sur le groupe utilisé pour le CIDR BYOIP.

Cette étape doit être réalisée par le compte IPAM.

Exécutez la commande suivante :

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

Dans la sortie, vous verrez l'IPAM que vous avez créé. Provisionnez un bloc d'adresse CIDR au groupe de niveau supérieur. Vous aurez besoin de votre ID de portée publique à l'étape suivante.

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

Étape 3 : création d'un groupe IPAM

Puisque vous allez créer un groupe IPAM de niveau supérieur contenant un groupe régional et que nous allons allouer de l'espace à une ressource (un VPC) à partir du groupe régional, vous définirez les paramètres régionaux sur le groupe régional, et non sur le groupe de niveau supérieur. Vous ajouterez les paramètres régionaux au groupe régional lorsque vous le créerez à une étape ultérieure. L'intégration IPAM avec BYOIP nécessite que les paramètres régionaux soient définis sur le groupe utilisé pour le CIDR BYOIP.

Cette étape doit être réalisée par le compte IPAM.

Choisissez si vous souhaitez que ce CIDR de pool IPAM soit publicisé AWS sur Internet (`--publicly-advertisable`ou). `--no-publicly-advertisable`

> **Note**
>
> Notez que l'ID de portée doit équivaloir à l'ID de portée publique et que la famille d'adresses doit être `ipv6`.

Pour créer un pool d'adresses IPv6 pour toutes vos AWS ressources à l'aide du AWS CLI

1. Exécutez la commande suivante pour créer un groupe IPAM. Utilisez l'ID de portée publique de l'IPAM que vous avez créé à l'étape précédente.

   ```
   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
   ```

   Dans la sortie, vous verrez apparaître `create-in-progress`, qui indique que la création du groupe est en cours.

   ```
   {
       "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. Exécutez la commande suivante jusqu'à ce que l'état `create-complete` apparaisse dans la sortie.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

L'exemple de sortie suivant illustre l'état du groupe.

```
{
    "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": []

    }

}
```

Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur

Allouez un bloc d'adresse CIDR au groupe de niveau supérieur. Notez que lorsque vous fournissez un CIDR IPv6 à un pool au sein du pool de niveau supérieur, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR pouvant faire l'objet d'une publicité publique et /60 pour les CIDR non publicisés. Vous devez inclure le CIDR, le message BYOIP et la signature de certificat dans la demande afin que nous puissions vérifier que vous êtes propriétaire de l'espace public. Pour obtenir la liste des conditions préalables BYOIP, y compris comment obtenir ce message BYOIP et cette signature de certificat, voir Apportez votre propre CIDR IPv4 public à IPAM en utilisant uniquement la CLI AWS.

Vous devez uniquement ajouter `--cidr-authorization-context` lorsque vous provisionnez le CIDR BYOIP au groupe de niveau supérieur. Pour le groupe régional au sein du groupe de niveau supérieur, vous pouvez omettre l'option `--cidr-authorization-context`.

Cette étape doit être réalisée par le compte IPAM.

Pour fournir un bloc CIDR au pool à l'aide du AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

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

Dans la sortie, vous verrez le CIDR en attente d'approvisionnement.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "pending-provision"

    }

}
```

2. Vérifiez que ce CIDR a été provisionné avant de continuer.

> **Important**
>
> Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'approvisionnement pour les gammes pouvant faire l'objet d'une publicité publique peut prendre jusqu'à une semaine.

Exécutez la commande suivante jusqu'à ce que l'état `provisioned` apparaisse dans la sortie.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

L'exemple de sortie suivant illustre l'état.

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

Étape 5 : Création d'un groupe régional dans le groupe de niveau supérieur

Créez un groupe régional dans le groupe de niveau supérieur. `--locale` est obligatoire sur le groupe ; il doit s'agir de l'une des Régions d'exploitation que vous avez configurées lors de la création de l'IPAM.

Cette étape doit être réalisée par le compte IPAM.

> **Important**
>
> Lorsque vous créez le groupe, vous devez inclure `--aws-service ec2`. Le service que vous sélectionnez détermine le AWS service pour lequel le CIDR sera publicisé. Actuellement, la seule option est la `ec2` suivante : les CIDR alloués à partir de ce pool seront publicisables pour le service Amazon EC2 et le service Amazon VPC (pour les CIDR associés aux VPC).

Pour créer un groupe régional à l'aide de l' AWS CLI

1. Exécutez la commande suivante pour créer le groupe.

```
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
```

   Dans la sortie, vous verrez IPAM en cours de création du groupe.

```
{
    "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. Exécutez la commande suivante jusqu'à ce que l'état de `create-complete` apparaisse dans la sortie.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Dans la sortie, vous verrez les groupes que vous avez dans votre IPAM. Dans ce tutoriel, nous avons créé un groupe de niveau supérieur et un groupe régional. Vous verrez donc les deux.

Étape 6 : approvisionnement d'un CIDR au groupe régional

Provisionnez un bloc d'adresse CIDR au groupe régional. Notez que lorsque vous approvisionnez le CIDR à un pool au sein du pool de niveau supérieur, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR pouvant faire l'objet d'une publicité publique et /60 pour les CIDR non publicisés.

Cette étape doit être réalisée par le compte IPAM.

Pour attribuer un bloc CIDR au pool régional à l'aide du AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

Dans la sortie, vous verrez le CIDR en attente d'approvisionnement.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
```

```
}
```

2. Exécutez la commande suivante jusqu'à ce que l'état de `provisioned` apparaisse dans la sortie.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

L'exemple de sortie suivant illustre le bon état.

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

Étape 7. Partager le groupe régional

Suivez les étapes décrites dans cette section pour partager le pool IPAM à l'aide de AWS Resource Access Manager (RAM).

Activer le partage des ressources dans AWS RAM

Après avoir créé votre IPAM, partagez le groupe régional avec d'autres comptes de votre organisation. Avant de partager un pool IPAM, suivez les étapes décrites dans cette section pour activer le partage de ressources avec AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`management-account`**option.

Pour activer le partage des ressources

1. À l'aide du compte AWS Organizations de gestion, ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram/.
2. Dans le volet de navigation de gauche, choisissez Paramètres, sélectionnez Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

Vous pouvez désormais partager un groupe IPAM avec d'autres membres de l'organisation.

Partagez un pool IPAM à l'aide de AWS RAM

Dans cette section, vous allez partager le pool régional avec un autre compte AWS Organizations membre. Pour obtenir des instructions complètes sur le partage de groupes IPAM, y compris des informations sur les autorisations IAM requises, consultez Partage d'un groupe IPAM à l'aide d'AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'`--profile` **`ipam-account`**option.

Pour partager un pool IPAM à l'aide de AWS RAM

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez l'étendue privée, choisissez le pool IPAM, puis choisissez Actions > Afficher les détails.
4. Sous Resource sharing (Partage de ressources), sélectionnez Create resource share (Créer un partage de ressources). La AWS RAM console s'ouvre. Vous partagez le pool en utilisant AWS RAM.
5. Sélectionnez Create a resource share (Créer un partage de ressources).
6. Dans la AWS RAM console, choisissez à nouveau Créer un partage de ressources.
7. Ajoutez un Nom pour la ressource partagée.
8. Sous Sélectionner le type de ressource, choisissez les pools IPAM, puis l'ARN du pool que vous souhaitez partager.
9. Choisissez Suivant.
10. Choisissez l'AWSRAMPermissionIpamPoolByoipCidrImportautorisation. Les détails des options d'autorisation ne sont pas abordés dans ce didacticiel, mais vous pouvez en savoir plus sur ces options dans Partage d'un groupe IPAM à l'aide d'AWS RAM.
11. Choisissez Suivant.
12. Dans Principaux > Sélectionner le type de principal, choisissez Compte AWS , saisissez l'ID du compte qui transmettra une plage d'adresses IP à IPAM, puis choisissez Ajouter.
13. Choisissez Suivant.
14. Examinez les options de partage de ressources et les principaux avec lesquels vous procéderez au partage, puis sélectionnez Créer.
15. Pour autoriser le compte **`member-account`** à allouer les CIDR de l'adresse IP à partir du groupe IPAM, créez un deuxième partage de ressources avec

`AWSRAMDefaultPermissionsIpamPool` et créez un deuxième partage de ressources. La valeur pour `--resource-arns` est l'ARN du groupe IPAM que vous avez créé dans la section précédente. La valeur de `--principals` est l'ID de compte du**`member-account`**. La valeur pour `--permission-arns` est l'ARN de l'autorisation `AWSRAMDefaultPermissionsIpamPool`.

Étape 8 : création d'un VPC à l'aide du CIDR IPv6

Créez un VPC à l'aide de l'ID de groupe IPAM. Vous devez associer un bloc d'adresse CIDR IPv4 au VPC et utiliser l'option `--cidr-block` ou la demande échouera. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP.

Cette étape doit être effectuée par le compte membre.

Pour créer un VPC avec le CIDR IPv6 à l'aide du AWS CLI

1. Exécutez la commande suivante pour provisionner le CIDR.

```
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
```

   Dans la sortie, vous verrez le VPC en cours de création.

```
{
    "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. Affichez l'allocation du VPC dans IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Dans la sortie, vous verrez l'allocation dans IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Étape 9 : publication du CIDR

Une fois que vous avez créé le VPC avec le CIDR alloué dans IPAM, vous pouvez commencer à annoncer le CIDR que vous avez apporté et AWS qui se trouve dans le pool défini. `--aws-service ec2` Dans ce didacticiel, il s'agit de votre groupe régional. Par défaut, le CIDR n'est pas publié, ce

qui signifie qu'il n'est pas accessible publiquement sur Internet. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe régional qui sera utilisé pour le CIDR BYOIP.

Cette étape doit être réalisée par le compte IPAM.

Commencez à faire de la publicité pour le CIDR à l'aide du AWS CLI

- Exécutez la commande suivante pour publier le CIDR.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

  Dans la sortie, vous verrez que le CIDR est publié.

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "advertised"
    }
}
```

Étape 10 : nettoyage

Suivez les étapes de cette section pour nettoyer les ressources que vous avez provisionnées et créées dans ce tutoriel. Lorsque vous exécutez les commandes dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe régional qui sera utilisé pour le CIDR BYOIP.

Nettoyez à l'aide du AWS CLI

1. Exécutez la commande suivante pour afficher l'allocation de VPC gérée dans IPAM.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   La sortie affiche l'allocation dans IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

2. Exécutez la commande suivante pour arrêter la publication du CIDR. Lorsque vous exécutez la commande dans cette étape, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe régional qui sera utilisé pour le CIDR BYOIP.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

   Dans la sortie, vous verrez que l'état du CIDR est passé de advertised (Publié) à provisioned (Provisionné).

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "provisioned"
    }
}
```

3. Exécutez la commande suivante pour supprimer le VPC. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe régional qui sera utilisé pour le CIDR BYOIP.

   Cette étape doit être effectuée par le compte membre.

```
aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
profile member-account
```

Vous ne verrez aucune sortie lorsque vous exécutez cette commande.

4. Exécutez la commande suivante pour afficher l'allocation de VPC dans IPAM. IPAM peut prendre un certain temps pour découvrir que le VPC a été supprimé et supprimer cette allocation. Lorsque vous exécutez les commandes dans cette section, la valeur de `--region` doit correspondre à l'option `--locale` que vous avez saisie lorsque vous avez créé le groupe régional qui sera utilisé pour le CIDR BYOIP.

   Cette étape doit être réalisée par le compte IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   La sortie affiche l'allocation dans IPAM.

   ```
   {
      "IpamPoolAllocations": [

           {

               "Cidr": "2605:9cc0:409::/56",

               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
               "ResourceId": "vpc-00b5573ffc3b31a29",

               "ResourceType": "vpc",

               "ResourceOwner": "123456789012"

           }

       ]

   }
   ```

   Exécutez à nouveau la commande et recherchez l'allocation à supprimer. Vous ne pouvez pas continuer à nettoyer et à désactiver le CIDR du groupe IPAM tant que vous ne voyez pas que l'allocation a été supprimée d'IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

La sortie affiche l'allocation supprimée d'IPAM.

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

5. Supprimez les partages RAM et désactivez l'intégration de la RAM avec AWS Organizations. Suivez les étapes décrites dans les sections Suppression d'un partage de ressources dans la AWS RAM et Désactivation du partage de ressources avec AWS les organisations dans le guide de l'utilisateur de la AWS RAM, dans cet ordre, pour supprimer les partages de RAM et désactiver l'intégration de la RAM avec AWS les organisations.

   Cette étape doit être effectuée par le compte IPAM et le compte de gestion respectivement. Si vous utilisez le AWS CLI pour supprimer les partages de RAM et désactiver l'intégration de RAM, utilisez les `--profile management-account` options `--profile ipam-account` et.

6. Exécutez la commande suivante pour désactiver le CIDR du groupe régional.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   Dans la sortie, vous verrez le CIDR en attente de désapprovisionnement.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   La désactivation prend un certain temps. Continuez à exécuter la commande jusqu'à ce que vous voyez l'état CIDR deprovisioned (désactivé).

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

Dans la sortie, vous verrez le CIDR en attente de désactivation.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "deprovisioned"
    }
}
```

7. Exécutez la commande suivante pour supprimer le groupe régional.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   Dans la sortie, vous pouvez voir l'état de suppression.

```
{
    "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. Exécutez la commande suivante pour désactiver le CIDR du groupe de niveau supérieur.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   Dans la sortie, vous verrez le CIDR en attente de désapprovisionnement.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   Le désapprovisionnement prend un certain temps. Utilisez la commande suivante pour vérifier le statut de la désapprovisionnement.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

   Attendez de voir l'état deprovisioned (désactivé) avant de passer à l'étape suivante.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. Exécutez la commande suivante pour supprimer le groupe de niveau supérieur.

   Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Dans la sortie, vous pouvez voir l'état de suppression.

```
{
    "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. Exécutez la commande suivante pour supprimer l'IPAM.

    Cette étape doit être réalisée par le compte IPAM.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    Dans la sortie, vous verrez la réponse IPAM. Cela signifie que l'IPAM a été supprimé.

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

Didacticiel : transfert d'un CIDR IPv4 BYOIP vers IPAM

Suivez ces étapes pour transférer un CIDR IPv4 existant vers IPAM. Si vous possédez déjà un CIDR BYOIP IPv4 avec AWS, vous pouvez déplacer le CIDR vers IPAM à partir d'un pool IPv4 public. Vous ne pouvez pas déplacer un CIDR IPv6 vers IPAM.

Ce didacticiel part du principe que vous avez déjà réussi à intégrer une plage d'adresses IP à l' AWS aide du processus décrit dans Apporter vos propres adresses IP (BYOIP) dans Amazon EC2 et que vous souhaitez maintenant transférer cette plage d'adresses IP vers IPAM. Si vous introduisez une nouvelle adresse IP AWS pour la première fois, suivez les étapes décrites dansDidacticiel : apporter vos adresses IP à IPAM.

Si vous transférez un groupe IPv4 public vers IPAM, cela n'a aucun impact sur les allocations existantes. Une fois que vous avez transféré un groupe IPv4 public vers IPAM, selon le type de ressource, vous pouvez contrôler les allocations existantes. Pour plus d'informations, consultez Contrôle de l'utilisation du CIDR par ressource.

Important

- Ce didacticiel suppose que vous avez terminé cette procédure en Création d'un IPAM.
- Chaque étape de ce didacticiel doit être effectuée par l'un des deux AWS comptes suivants :
  - Le compte pour l'administrateur IPAM. Dans ce didacticiel, ce compte sera appelé compte IPAM.

- Le compte de votre organisation qui possède le CIDR BYOIP. Dans ce didacticiel, ce compte sera appelé compte du propriétaire CIDR BYOIP.

Table des matières

- Étape 1 : Création de profils AWS CLI nommés et de rôles IAM
- Étape 2 : obtention de l'ID de portée publique de votre IPAM
- Étape 3 : création d'un groupe IPAM
- Étape 4 : partager le pool IPAM à l'aide de AWS RAM
- Étape 5 : transfert d'un CIDR IPV4 BYOIP existant vers IPAM
- Étape 6 : affichage du CIDR dans IPAM
- Étape 7 : nettoyage

Étape 1 : Création de profils AWS CLI nommés et de rôles IAM

Pour suivre ce didacticiel en tant qu' AWS utilisateur unique, vous pouvez utiliser des profils AWS CLI nommés pour passer d'un rôle IAM à un autre. Les profils nommés sont des ensembles de paramètres et d'informations d'identification auxquels vous vous référez lorsque vous utilisez l'option `--profile` associée à l' AWS CLI. Pour plus d'informations sur la création de rôles IAM et de profils nommés pour les AWS comptes, consultez la section Utilisation d'un rôle IAM dans la AWS CLI du guide de l'utilisateur AWS d'Identity and Access Management.

Créez un rôle et un profil nommé pour chacun des trois AWS comptes que vous utiliserez dans ce didacticiel :

- Un profil appelé `ipam-account` pour le AWS compte qui est l'administrateur IPAM.
- Un profil appelait le AWS compte `byoip-owner-account` de votre organisation qui possède le BYOIP CIDR.

Une fois que vous avez créé les rôles IAM et les profils nommés, revenez à cette page et passez à l'étape suivante. Vous remarquerez dans le reste de ce didacticiel que les exemples de AWS CLI commandes utilisent l'`--profile`option avec l'un des profils nommés pour indiquer quel compte doit exécuter la commande.

Étape 2 : obtention de l'ID de portée publique de votre IPAM

Suivez les étapes de cette section pour obtenir l'ID de portée publique de votre IPAM. Cette étape doit être effectuée par le compte **`ipam-account`**.

Exécutez la commande suivante pour obtenir l'ID de portée publique.

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

Dans la sortie, vous verrez l'ID de portée publique. Notez les valeurs de `PublicDefaultScopeId`. Vous en aurez besoin à l'étape suivante.

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

Étape 3 : création d'un groupe IPAM

Suivez les étapes de cette section pour créer un groupe IPAM. Cette étape doit être effectuée par le compte **`ipam-account`**. Le groupe IPAM que vous créez doit être un groupe de niveau supérieur avec l'option `--locale` correspondant à la région AWS du CIDR BYOIP. Vous pouvez uniquement transférer un BYOIP vers un groupe IPAM de niveau supérieur.

> **Important**
>
> Lorsque vous créez le groupe, vous devez inclure `--aws-service ec2`. Le service que vous sélectionnez détermine le AWS service pour lequel le CIDR sera publicisé. Actuellement, la seule option est `ec2`, ce qui signifie que les CIDR alloués à partir de ce groupe pourront être annoncés pour le service Amazon EC2 (pour les adresses IP Elastic) et le service Amazon VPC (pour les CIDR associés aux VPC).

Pour créer un groupe d'adresses IPv4 pour le CIDR BYOIP transféré à l'aide d' AWS CLI

1. Exécutez la commande suivante pour créer un groupe IPAM. Utilisez l'ID de portée publique de l'IPAM que vous avez obtenu à l'étape précédente.

```
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
```

   Dans la sortie, vous verrez apparaître `create-in-progress`, qui indique que la création du groupe est en cours.

```
{
    "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. Exécutez la commande suivante jusqu'à ce que l'état `create-complete` apparaisse dans la sortie.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

L'exemple de sortie suivant illustre l'état du groupe. Vous en aurez besoin OwnerIdà l'étape suivante.

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

Étape 4 : partager le pool IPAM à l'aide de AWS RAM

Suivez les étapes décrites dans cette section pour partager un pool IPAM AWS RAM afin qu'un autre AWS compte puisse transférer un CIDR BYOIP IPV4 existant vers le pool IPAM et utiliser le pool IPAM. Cette étape doit être effectuée par le compte **`ipam-account`**.

Pour partager un groupe d'adresses IPv4 en utilisant AWS CLI

1. Consultez les AWS RAM autorisations disponibles pour les pools IPAM. Vous avez besoin des deux ARN pour effectuer les étapes de cette section.

```
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. Créez un partage de ressources pour permettre au compte **`byoip-owner-account`** d'importer des CIDR BYOIP vers IPAM. La valeur pour `--resource-arns` est l'ARN du groupe IPAM que vous avez créé dans la section précédente. La valeur pour `--principals` est l'identifiant du compte du propriétaire du CIDR BYOIP. La valeur pour `--permission-arns` est l'ARN de l'autorisation `AWSRAMPermissionIpamPoolByoipCidrImport`.

```
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. (Facultatif) Si vous souhaitez autoriser le compte **byoip-owner-account** à allouer des adresses IP CIDR du groupe IPAM à des groupes IPv4 publics une fois le transfert terminé, copiez l'ARN pour `AWSRAMDefaultPermissionsIpamPool` et créez un deuxième partage de ressources. La valeur pour `--resource-arns` est l'ARN du groupe IPAM que vous avez créé dans la section précédente. La valeur pour `--principals` est l'identifiant du compte du propriétaire du CIDR BYOIP. La valeur pour `--permission-arns` est l'ARN de l'autorisation `AWSRAMDefaultPermissionsIpamPool`.

```
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"

        }

}
```


Suite à la création du partage de ressources dans la RAM, le byoip-owner-account compte peut désormais déplacer les CIDR vers IPAM.

Étape 5 : transfert d'un CIDR IPV4 BYOIP existant vers IPAM

Suivez les étapes de cette section pour transférer un CIDR IPv4 BYOIP existant vers IPAM. Cette étape doit être effectuée par le compte **`byoip-owner-account`**.

> **Important**
>
> Une fois que vous avez transféré une plage d'adresses IPv4 AWS, vous pouvez utiliser toutes les adresses IP de la plage, y compris la première adresse (adresse réseau) et la dernière adresse (adresse de diffusion).

Pour transférer le CIDR BYOIP vers IPAM, le propriétaire du CIDR BYOIP doit disposer des autorisations suivantes dans sa stratégie IAM :

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> Vous pouvez utiliser le AWS Management Console ou le AWS CLI pour cette étape.

AWS Management Console

Pour transférer un CIDR BYOIP vers le groupe IPAM :

1. Ouvrez la console IPAM à partir de l'adressehttps://console.aws.amazon.com/ipam/ en tant que compte **`byoip-owner-account`**.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez le groupe de niveau supérieur créé et partagé dans ce tutoriel.
4. Choisissez Actions > Transférer le CIDR BYOIP.
5. Choisissez Transférer le CIDR BYOIP.
6. Choisissez votre CIDR BYOIP.
7. Choisissez Provisionner.

Command line

Utilisez les AWS CLI commandes suivantes pour transférer un CIDR BYOIP vers le pool IPAM à l'aide de : AWS CLI

1. Exécutez la commande suivante pour transférer le CIDR. Assurez-vous que la `--region` valeur est la AWS région du CIDR BYOIP.

```
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
```

Dans la sortie, vous verrez l'approvisionnement CIDR en attente.

```
{
```

```
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "pending-transfer"

    }

}
```

2. Assurez-vous que le CIDR a été transféré. Exécutez la commande suivante jusqu'à ce que l'état `complete-transfer` apparaisse dans la sortie.

```
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
```

L'exemple de sortie suivant illustre l'état.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

Étape 6 : affichage du CIDR dans IPAM

Suivez les étapes de cette section pour afficher le CIDR dans IPAM. Cette étape doit être effectuée par le compte **`ipam-account`**.

Pour afficher le CIDR BYOIP transféré dans le pool IPAM à l'aide du AWS CLI

- Exécutez la commande suivante pour afficher l'allocation gérée dans IPAM. Assurez-vous que la `--region` valeur est la AWS région du CIDR BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

La sortie affiche l'allocation dans IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

Étape 7 : nettoyage

Suivez les étapes de cette section pour supprimer les ressources que vous avez créées dans ce tutoriel. Cette étape doit être effectuée par le compte **ipam-account**.

Pour nettoyer les ressources créées dans ce didacticiel à l'aide du AWS CLI

1. Pour supprimer la ressource partagée du groupe IPAM, exécutez la commande suivante pour obtenir le premier ARN de partage de ressources :

```
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. Copiez l'ARN du partage de ressources et utilisez-le pour supprimer le partage de ressources du groupe IPAM.

```
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. Si vous avez créé un partage de ressources supplémentaire dans Étape 4 : partager le pool IPAM à l'aide de AWS RAM, répétez les deux étapes précédentes pour obtenir l'ARN du deuxième partage de ressources pour `PoolShare2` et supprimer le deuxième partage de ressources.

4. Exécutez la commande suivante pour obtenir l'ID d'allocation du CIDR BYOIP. Assurez-vous que la `--region` valeur correspond à la AWS région du CIDR BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

La sortie affiche l'allocation dans 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. Libérez la dernière adresse IP du CIDR à partir du groupe IPv4 public. Saisissez l'adresse IP avec un masque de réseau de /32. Vous devez réexécuter cette commande pour chaque adresse IP de la plage d'adresses CIDR. Si votre CIDR est un `/24`, vous devrez exécuter cette commande pour désapprovisionner chacune des 256 adresses IP du CIDR `/24`. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à la Région de votre IPAM.

   Cette étape doit être réalisée par le compte **`byoip-owner-account`**.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1  --profile byoip-
owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.255/32
```

   Dans la sortie, vous verrez le CIDR désactivé.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",

    "DeprovisionedAddresses": [

        "130.137.249.255"

    ]

}
```

6. Consultez à nouveau vos CIDR BYOIP et vérifiez qu'il n'y a plus d'adresses provisionnées. Lorsque vous exécutez la commande dans cette section, la valeur de `--region` doit correspondre à la Région de votre IPAM.

   Cette étape doit être réalisée par le compte **`byoip-owner-account`**.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
```

   Dans la sortie, vous verrez le nombre d'adresses IP dans votre groupe IPv4 public.

```
{
```

```
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

7. Exécutez la commande suivante pour supprimer le groupe de niveau supérieur.

```
aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
id ipam-pool-0a03d430ca3f5c035
```

Dans la sortie, vous pouvez voir l'état de suppression.

```
{
    "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"
    }
}
```

Didacticiel : Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau

Suivez ce didacticiel pour planifier l'espace d'adresse IP du VPC afin d'allouer des adresses IP aux sous-réseaux VPC et de surveiller les métriques relatives aux adresses IP au niveau du sous-réseau et du VPC.

> **Note**
>
> Ce didacticiel couvre l'allocation d'un espace d'adresse IPv4 privé dans une portée IPAM privée aux VPC et aux sous-réseaux. Vous pouvez également suivre ce didacticiel à l'aide de la portée publique et d'une plage d'adresses CIDR IPv6 en créant le VPC avec l'option de bloc d'adresse CIDR IPv6 fournie par Amazon dansla console VPC.

La planification de l'espace d'adresse IP VPC pour les sous-réseaux vous permet d'effectuer les opérations suivantes :

- Planifier et organiser les adresses IP de votre VPC pour les allouer aux sous-réseaux : vous pouvez diviser l'espace d'adresses IP du VPC en blocs d'adresse CIDR plus petits et allouer ces blocs d'adresse CIDR à des sous-réseaux ayant des besoins commerciaux différents, par exemple si vous exécutez des charges de travail dans des sous-réseaux de développement ou de production.
- Simplifier les allocations d'adresses IP pour les sous-réseaux VPC : une fois que l'espace d'adresse de votre VPC est planifié et organisé, vous pouvez choisir une longueur de masque réseau plutôt que de saisir manuellement un CIDR. Par exemple, si un développeur crée un sous-réseau pour héberger des charges de travail de développement, il doit choisir un groupe et une longueur de masque réseau pour le sous-réseau et l'IPAM allouera automatiquement le bloc CIDR à votre sous-réseau.

L'exemple suivant illustre la hiérarchie du groupe et la structure de ressources que vous allez créer à l'aide de ce didacticiel :

- Portée privée
  - Groupe de planification des ressources (10.0.0.0/20)
    - Groupe de sous-réseau de développement (10.0.0.0/24)

    - Sous-réseau de développement (10.0.0.0/28)
- Groupe de sous-réseau de production (10.0.0.1/24)
    - Sous-réseau de production (10.0.0.16/28)

> **Important**
>
> - Le groupe de planification des ressources peut être utilisé pour allouer des CIDR à des sous-réseaux ou il peut être utilisé comme groupe source dans lequel vous pouvez créer d'autres groupes. Dans ce didacticiel, nous utilisons le groupe de planification des ressources comme groupe source pour les groupes de sous-réseaux.
> - Vous pouvez créer plusieurs groupes de planification des ressources à l'aide du même VPC si plusieurs CIDR sont provisionnés au VPC ; si deux CIDR sont attribués à un VPC, par exemple, vous pouvez créer deux groupes de planification des ressources, un pour chaque CIDR. Chaque adresse CIDR peut être attribuée à un groupe à la fois.

Étape 1 : Créer un VPC

Suivez les étapes de cette section pour créer un VPC à utiliser pour la planification des adresses IP de sous-réseau. Pour plus d'informations sur les autorisations IAM requises pour créer des VPC, consultez les exemples de politiques Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

> **Note**
>
> Vous pouvez utiliser un VPC existant plutôt que d'en créer un nouveau, mais ce didacticiel se concentre sur le scénario dans lequel le VPC est configuré avec un bloc d'adresse CIDR alloué manuellement, et non avec un bloc d'adresse CIDR alloué automatiquement par l'IPAM.

Pour créer un VPC

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/vpc/.
2. Sélectionnez Create VPC (Créer un VPC).
3. Saisissez un nom pour le VPC, par exemple didacticiel-vpc.

4. Choisissez IPv4 CIDR manual input (Entrée manuelle CIDR IPv4) et saisissez un bloc d'adresse CIDR IPv4. Dans ce didacticiel, nous utilisons 10.0.0.0/20.
5. Ignorez l'option d'ajout d'un bloc d'adresse CIDR IPv6.
6. Sélectionnez Create VPC (Créer un VPC).
7. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
8. Dans le volet de navigation de gauche, choisissez Ressources.
9. Attendez que le VPC que vous avez créé apparaisse. Cela prend un certain temps et vous devrez peut-être rafraîchir la fenêtre pour le voir apparaître. Le VPC doit être découvert par l'IPAM avant de passer à l'étape suivante.

Étape 2 : créer un groupe de planification des ressources

Suivez les étapes de cette section pour créer un groupe de planification des ressources.

Pour créer un groupe de planification des ressources

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez la portée privée.
4. Sélectionnez Create pool (Créer un groupe).
5. Sous Portée IPAM, laissez la portée privée sélectionnée.
6. (Facultatif) Ajoutez Balise de nom pour le groupe, par exemple « Groupe de planification des ressources ».
7. Sous Source, choisissez Portée IPAM.
8. Sous Planification des ressources, choisissez Planifier l'espace IP dans un VPC et choisissez le VPC que vous avez créé à l'étape précédente. Le VPC est la ressource utilisée pour provisionner des CIDR au groupe de planification des ressources.
9. Sous CIDR à provisionner, choisissez le CIDR VPC à provisionner pour le groupe de ressources. Le CIDR que vous provisionnez au groupe de planification des ressources doit correspondre au CIDR fourni au VPC. Dans ce didacticiel, nous utilisons 10.0.0.0/20.
10. Sélectionnez Create pool (Créer un groupe).

11. Une fois le groupe créé, choisissez l'onglet CIDR pour voir l'état du CIDR provisionné. Actualisez la page et attendez que l'état du CIDR passe de Provision en attente à Provisionné avant de passer à l'étape suivante.

Étape 3 : créer des groupes de sous-réseaux

Suivez les étapes de cette section pour créer deux groupes de sous-réseaux qui seront utilisés pour allouer de l'espace IP aux sous-réseaux.

Pour créer des groupes de sous-réseaux

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez la portée privée.
4. Sélectionnez Create pool (Créer un groupe).
5. Sous Portée IPAM, laissez la portée privée sélectionnée.
6. (Facultatif) Ajoutez une Balise de nom pour le groupe, par exemple « groupe de sous-réseaux de développement ».
7. Sous Source, choisissez le Groupe IPAM et sélectionnez le groupe de planification des ressources que vous avez créé à l'étape 3. La famille d'adresses, la configuration de planification des ressources et les paramètres régionaux sont automatiquement hérités du groupe source.
8. Sous CIDR à provisionner, choisissez un CIDR à provisionner pour le groupe. Dans ce didacticiel, nous utilisons 10.0.0.0/24.
9. Sélectionnez Create pool (Créer un groupe).
10. Une fois le groupe créé, choisissez l'onglet CIDR pour voir l'état du CIDR provisionné. Actualisez la page et attendez que l'état du CIDR passe de Provision en attente à Provisionné avant de passer à l'étape suivante.
11. Répétez ce processus pour créer un autre sous-réseau appelé « groupe de sous-réseaux de production ».

À ce stade, si vous souhaitez mettre ce groupe de sous-réseaux à la disposition d'autres comptes AWS, vous pouvez le partager. Pour obtenir des instructions sur la façon de procéder, consultez Partage d'un groupe IPAM à l'aide d'AWS RAM. Revenez ensuite ici pour terminer le didacticiel.

Étape 4 : créer des sous-réseaux

Suivez ces étapes pour créer deux sous-réseaux.

Pour créer des sous-réseaux

1. À l'aide du compte approprié, ouvrez la console VPC à l'adresse suivante : https://console.aws.amazon.com/vpc/.
2. Choisissez Sous-réseaux > Créer un sous-réseau.
3. Choisissez le VPC que vous avez créé au début de ce didacticiel.
4. Entrez un nom pour le sous-réseau, par exemple « didacticiel sous-réseau ».
5. (facultatif) Choisissez une Zone de disponibilité.
6. Sous Bloc d'adresse CIDR IPv4, choisissez le Bloc d'adresse CIDR IPv4 alloué par IPam, puis choisissez le groupe de sous-réseaux de développement et un masque réseau /28.
7. Choisissez Create subnet (Créer un sous-réseau).
8. Répétez ce processus pour créer un autre sous-réseau. Cette fois, choisissez le groupe de sous-réseaux de production et un masque réseau /28.
9. Revenez à la console IPAM et choisissez Ressources dans le panneau de navigation de gauche.
10. Recherchez les groupes de sous-réseaux que vous avez créés et attendez que les sous-réseaux que vous avez créés apparaissent en dessous. Cela prend un certain temps et vous devrez peut-être rafraîchir la fenêtre pour le voir apparaître.

Le didacticiel est terminé. Vous pouvez créer des groupes de sous-réseaux supplémentaires selon vos besoins ou vous pouvez lancer une instance EC2 dans l'un des sous-réseaux.

L'IPAM publie des métriques relatives à l'utilisation des adresses IP dans les sous-réseaux. Vous pouvez définir des alarmes CloudWatch sur la métrique SubnetIPUsage, ce qui vous permet de prendre des mesures lorsque les seuils d'utilisation des adresses IP sont dépassés. Si, par exemple, un CIDR /24 (256 adresses IP) est attribué à un sous-réseau et que vous souhaitez être averti lorsque 80 % des adresses IP ont été utilisées, vous pouvez configurer une alarme CloudWatch pour vous avertir lorsque ce seuil est atteint. Pour plus d'informations sur la création d'une alarme pour l'utilisation de l'adresse IP du sous-réseau, consultez Astuce rapide pour créer des alarmes.

Étape 5 : nettoyage

Suivez ces étapes pour supprimer les ressources que vous avez créées à l'aide de ce didacticiel.

Nettoyer les ressources.

1. À l'aide du compte administrateur IPAM, ouvrez la console IPAM à l'adresse suivante : https://console.aws.amazon.com/ipam/.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez la portée privée.
4. Choisissez le groupe de planification des ressources, puis Action > Supprimer.
5. Sélectionnez Supprimer en cascade. Le groupe de planification des ressources et les groupes de sous-réseaux seront supprimés. Cela ne supprimera pas les sous-réseaux eux-mêmes. Ils conserveront les CIDR qui leur ont été provisionnés même si les CIDR ne proviendront plus d'un groupe IPAM.
6. Choisissez Supprimer.
7. Supprimer les sous-réseaux.
8. Supprimer le VPC.

Le nettoyage est terminé.

Gestion des identités et des accès dans IPAM

AWS utilise les informations d'identification de sécurité pour identifier et vous accorder l'accès à vos ressources AWS. Vous pouvez utiliser les fonctions de AWS Identity and Access Management (IAM) pour permettre à d'autres utilisateurs, services et applications d'utiliser vos ressources AWS pleinement ou de façon limitée, sans partager vos autorisations de sécurité.

Cette section décrit les rôles liés aux services AWS créés spécifiquement pour IPAM et les stratégies gérées attachées aux rôles liés au service IPAM. Pour plus d'informations sur les rôles et les stratégies AWS IAM, consultez Termes et concepts relatifs aux rôles dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur la gestion des identités et des accès pour VPC, consultez Gestion des identités et des accès pour Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

Table des matières

- Rôles liés à un service pour IPAM
- Stratégies gérées AWS pour IPAM
- Exemple de stratégie

Rôles liés à un service pour IPAM

Les rôles liés à un service dans AWS Identity and Access Management (IAM) permettent aux services AWS d'appeler d'autres services AWS en votre nom. Pour plus d'informations sur l'utilisation des rôles liés à un service, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur IAM.

Pour l'instant, il n'y a qu'un rôle lié à un service IPAM : AWSServiceRoleForIPAM.

Autorisations accordées au rôle lié à un service

IPAM utilise le service lié à un rôle AWSServiceRoleForIPAM pour appeler les actions dans la stratégie gérée attachée AWSIPAMServiceRolePolicy. Pour plus d'informations sur les actions autorisées dans cette stratégie, consultez Stratégies gérées AWS pour IPAM.

Une stratégie de confiance IAM est également attachée au rôle lié à un service, laquelle permet au service `ipam.amazonaws.com` d'assumer le rôle lié à un service.

Création du rôle lié à un service

IPAM surveille l'utilisation des adresses IP dans un ou plusieurs comptes en endossant le rôle lié au service dans un compte, en découvrant les ressources et leurs CIDR, et en intégrant ces ressources à IPAM.

Le rôle lié à un service est créé de l'une des deux manières suivantes :

- Lors de votre intégration à AWS Organisations

  Si vous Intégrer l'IPAM aux comptes d'une organisation AWS en utilisant la console IPAM ou utilisant la commande de AWS CLI `enable-ipam-organization-admin-account`, le service lié à un rôle AWSServiceRoleForIPAM est créé automatiquement dans chacun de vos comptes membres AWS Organizations. Par conséquent, les ressources de tous les comptes membres sont détectables par IPAM.

  > **Important**
  >
  > Pour qu'IPAM crée le rôle lié au service en votre nom :
  >
  > - Le compte de gestion AWS Organizations qui permet l'intégration d'IPAM à AWS Organizations doit être associé à une politique IAM qui autorise les actions suivantes :
  >   - `ec2:EnableIpamOrganizationAdminAccount`
  >   - `organizations:EnableAwsServiceAccess`
  >   - `organizations:RegisterDelegatedAdministrator`
  >   - `iam:CreateServiceLinkedRole`
  > - Le compte IPAM doit être associé à une politique IAM qui autorise l'action `iam:CreateServiceLinkedRole`.

- Lorsque vous créez un IPAM à l'aide d'un seul compte AWS

  Si vous Utilisation d'IPAM avec un seul compte, le rôle lié au service AWSServiceRoleForIPAM est automatiquement créé lorsque vous créez un IPAM en tant que compte.

  > **Important**
  >
  > Si vous utilisez IPAM avec un seul compte AWS, avant de créer un IPAM, vous devez vous assurer que le compte AWS que vous utilisez est associé à une politique IAM qui autorise l'action `iam:CreateServiceLinkedRole`. Lorsque vous créez l'IPAM, vous créez

automatiquement le rôle lié au service AWSServiceRoleForIPAM. Pour plus d'informations sur la gestion des politiques IAM, consultez Modification des politiques IAM dans le Guide de l'utilisateur IAM.

La modification du rôle lié à un service

Vous ne pouvez pas modifier le rôle lié au service AWSServiceRoleForIPAM.

La suppression du rôle lié à un service

Si vous n'avez plus besoin d'utiliser IPAM, nous vous recommandons de supprimer le rôle lié au service AWSServiceRoleForIPAM.

> **Note**
>
> Vous pouvez supprimer le rôle lié à un service après que vous avez supprimé toutes les ressources IPAM de votre compte AWS. Ainsi, vous ne pouvez pas involontairement supprimer la capacité de contrôle d'IPAM.

Suivez les étapes suivantes pour supprimer le rôle lié à un service par l'intermédiaire de l'AWS CLI :

1. Supprimez vos ressources IPAM à l'aide de deprovision-ipam-pool-cidr et delete-ipam. Pour plus d'informations, consultez Pour désapprovisionner un CIDR de groupe et Suppression d'un IPAM.
2. Désactivez le compte IPAM à l'aide de disable-ipam-organization-admin-account.
3. Désactivez le service IPAM à l'aide de disable-aws-service-access en utilisant l'option `--service-principal ipam.amazonaws.com`.
4. Supprimez le rôle lié à un service : delete-service-linked-role. Lorsque vous supprimez le rôle lié à un service, la stratégie gérée par IPAM est également supprimée. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Stratégies gérées AWS pour IPAM

Si vous utilisez l'IPAM avec un seul compte AWS et que vous créez un IPAM, la politique gérée AWSIPAMServiceRolePolicy est automatiquement créée dans votre compte IAM et attachée au rôle lié au service AWSServiceRoleForIPAM.

Si vous activez l'intégration IPAM avec AWS Organizations, la politique gérée AWSIPAMServiceRolePolicy est automatiquement créée dans votre compte IAM et dans chacun de vos comptes membres AWS Organizations, et la politique gérée est attachée au rôle lié au service AWSServiceRoleForIPAM.

Cette stratégie gérée permet à IPAM d'effectuer les opérations suivantes :

- Contrôler les CIDR associés aux ressources réseau chez tous les membres de votre organisation AWS.
- Stocker les métriques associées à IPAM dans Amazon CloudWatch, telles que l'espace d'adressage IP disponible dans vos groupes IPAM et le nombre de CIDR de ressource conformes aux règles d'allocation.

L'exemple suivant affiche les détails de la stratégie gérée créée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IPAMDiscoveryDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:ListByoipCidrs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
```

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

La première instruction de l'exemple précédent permet à IPAM de surveiller les CIDR utilisés par votre compte AWS unique ou par les membres de votre AWS Organization.

La deuxième instruction de l'exemple précédent utilise la clé de condition `cloudwatch:PutMetricData` pour permettre à IPAM de stocker des métriques IPAM dans votre espace de noms Amazon CloudWatch `AWS/IPAM`. Ces métriques sont utilisées par la console de gestion AWS pour afficher les données relatives aux allocations dans vos groupes et portées IPAM. Pour plus d'informations, consultez Contrôle de l'utilisation des CIDR à l'aide du tableau de bord IPAM.

Mises à jour de la stratégie gérée AWS

Consultez les détails des mises à jour des stratégies gérées AWS pour IPAM depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
AWSIPAMServiceRolePolicy	Action ajoutée à la politique gérée AWSIPAMSe rviceRolePolicy (`ec2:GetIp amDiscoveredPublic Addresses`) pour	13 novembre 2023

Modification	Description	Date
	permettre à IPAM d'obtenir des adresses IP publiques lors de la découverte de ressources.	
AWSIPAMServiceRolePolicy	Actions ajoutées à la politique gérée AWSIPAMServiceRolePolicy (`ec2:DescribeAccountAttributes`, `ec2:DescribeNetworkInterfaces`, `ec2:DescribeSecurityGroups`, `ec2:DescribeSecurityGroupRules`, `ec2:DescribeVpnConnections`, `globalaccelerator:ListAccelerators` et `globalaccelerator:ListByoipCidrs`) pour permettre à IPAM d'obtenir des adresses IP publiques lors de la découverte de ressources.	1er novembre 2023

Modification	Description	Date
AWSIPAMServiceRolePolicy	Deux actions (`ec2:GetIpamDiscoveredAccounts` et `ec2:GetIpamDiscoveredResourceCidrs`) ont été ajoutées à la politique gérée AWSIPAMServiceRolePolicy afin de permettre à IPAM d'obtenir les CIDR des ressources et comptes AWS surveillés lors de la découverte de ressources.	25 janvier 2023
IPAM a commencé à suivre les modifications	IPAM a commencé à suivre les modifications pour ses stratégies gérées AWS.	2 décembre 2021

Exemple de stratégie

L'exemple de politique présenté dans cette section contient toutes les actions AWS Identity and Access Management (IAM) pertinentes pour une utilisation complète d'IPAM. Selon la façon dont vous utilisez IPAM, il se peut que vous n'ayez pas besoin d'inclure toutes les actions IAM. Pour profiter pleinement de la console IPAM, vous devrez peut-être inclure des actions IAM supplémentaires pour des services tels qu'AWS Organizations, AWS Resource Access Manager (RAM) et Amazon CloudWatch.

```
{
"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"
                }
```

```
            }
        }
    ]
}
```

Quotas pour votre IPAM

Cette section répertorie les quotas liés à IPAM. La console Service Quotas fournit également des informations sur les quotas IPAM. Vous pouvez utiliser la console Service Quotas pour afficher les quotas par défaut et demander des augmentations de quota pour les quotas ajustables. Pour de plus amples informations, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Nom	Par défaut	Ajustable
Longueur du masque réseau de bloc CIDR IPv6 fourni par Amazon	/52	Oui. Contactez le centre de support AWS comme décrit dans la section Quotas de service AWS (langue française non garantie) de la Références générales AWS.
Blocs CIDR IPv6 fournis par Amazon par groupe régional	1	Oui. Contactez le centre de support AWS comme décrit dans la section Quotas de service AWS (langue française non garantie) de la Références générales AWS.
Numéros de systèmes autonomes (ASN) que vous pouvez apporter à l'IPAM	5	Oui. Contactez le centre de support AWS comme décrit dans la section Quotas

Nom	Par défaut	Ajustable
		de service AWS (langue française non garantie) de la Références générales AWS.
CIDR par groupe	50	Oui
Administrateurs IPAM par organisation	1	Non
IPAM par Région	1	Non
Profondeur de groupe (nombre de groupes dans les groupes)	10	Oui
Groupes par portée	50	Oui
Associations de découvertes de ressources par IPAM	5	Oui
Découvertes de ressources par région	1	Non
Métriques d'utilisation des ressources	50	Oui. Contactez le centre de support AWS comme décrit dans la section Quotas de service AWS (langue française non garantie) de la Références générales AWS.

Nom	Par défaut	Ajustable
Portées par IPAM	5	Oui. Lorsque vous créez un IPAM, des portées par défaut (une privée et une publique) sont créées pour vous. Si vous souhaitez créer des portées supplémentaires, celles-ci seront privées. Vous ne pouvez pas créer d'autres portées publiques.

Tarification d'IPAM

Cette section explique comment afficher les informations relatives à la tarification et à vos coûts IPAM actuels.

Afficher les informations sur la tarification

L'IPAM est proposé en deux niveaux : le niveau gratuit et le niveau avancé. Pour plus d'informations sur les fonctionnalités disponibles dans chaque niveau et les coûts associés aux niveaux, consultez l'onglet IPAM sur la page de tarification d'Amazon VPC.

Consultez vos coûts et votre utilisation actuels à l'aide de AWS Cost Explorer

Lorsque vous utilisez le niveau avancé IPAM, vous payez un tarif horaire par adresse IP active gérée par IPAM. Si vous souhaitez afficher et analyser vos coûts et votre utilisation de l'IPAM, vous pouvez utiliser l' AWS Cost Explorer.

1. Ouvrez la AWS Cost Management console à l'adresse https://console.aws.amazon.com/cost-management/home.
2. Lancez l'explorateur de coûts.
3. Filtrez l'utilisation de l'IPAM en choisissant Type d'utilisation et en saisissant **`IPAddressManager`**.
4. Cochez une ou plusieurs cases. Chacune d'entre elles représente une AWS région différente.
5. Cliquez sur Apply.

Si, par exemple, vous sélectionnez AddressManagerUSE1-IP -IP-Hours (Hrs) et que us-east-1 est votre région d'origine IPAM, vous verrez le nombre d'heures IP actives facturées par IPAM dans toutes les régions ainsi que le coût. Si, par exemple, l'utilisation en heures est de 18, cela signifie que vous pouvez avoir 1 adresse IP active pendant 18 heures, 3 adresses IP dans 3 régions différentes, chacune active pendant 6 heures, ou toute combinaison de ces adresses pour un total de 18 heures.

Pour plus d'informations AWS Cost Explorer, consultez la section Analyse de vos coûts AWS Cost Explorer dans le guide de AWS Cost Management l'utilisateur.

Informations connexes

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

- Amazon VPC IP Address Manager Best Practices (Bonnes pratiques du gestionnaire d'adresses IP Amazon VPC) :AWS blog sur les bonnes pratiques pour planifier et créer un schéma d'adresses évolutif avec un gestionnaire d'adresses IP Amazon VPC.
- Network Address Management and Auditing at Scale with Amazon VPC IP Address Manager (Gestion et audit des adresses réseau à grande échelle avec le gestionnaire d'adresses IP Amazon VPC) :AWS blog qui présente le gestionnaire d'adresses IP Amazon VPC et explique comment utiliser le service dans la console AWS.
- Configurer un accès précis à vos ressources partagées en utilisant AWS Resource Access Manager : un blog AWS qui explique comment partager un groupe IPAM avec les comptes d'une unité d'organisation AWS Organizations.

Historique de document pour IPAM

Le tableau suivant décrit les versions d'IPAM.

Fonction	Description	Date de parution
Niveaux gratuits et avancés de l'IPAM	Vous pouvez désormais choisir entre le niveau gratuit et le niveau avancé pour votre IPAM.	17 novembre 2023
Informations sur les adresses IP publiques	Auparavant, vous ne pouviez consulter les Public IP Insights que dans une seule région. Vous pouvez désormais consulter les Public IP Insights dans toutes les régions. En outre, vous pouvez désormais consulter les informations sur les adresses IP publiques dans Amazon CloudWatch.	17 novembre 2023
Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau	Vous pouvez désormais utiliser l'IPAM pour planifier l'espace IP du sous-réseau dans un VPC et surveiller les métriques liées aux adresses IP au niveau du sous-réseau et du VPC.	17 novembre 2023
Apportez votre propre ASN (BYOASN)	Vous pouvez désormais apporter votre numéro de système autonome (ASN) à AWS.	17 novembre 2023
Mises à jour de politique gérée par AWS : mise à jour d'une politique existante	La politique AWSIPAMServiceRolePolicy existante a été mise à jour.	17 novembre 2023
Mises à jour de politique gérée par AWS : mise à	La politique AWSIPAMServiceRolePolicy existante a été mise à jour.	1er novembre 2023

Fonction	Description	Date de parution
jour d'une politique existante		
Métriques d'utilisation des ressources	IPAM publie désormais des métriques d'utilisation IP pour les ressources qu'il surveille sur Amazon CloudWatch.	2 août 2023
Informations sur les adresses IP publiques	Les informations sur les adresses IP publiques affichent toutes les adresses IPv4 publiques utilisées par les services de cette région dans votre compte. Vous pouvez utiliser ces informations pour identifier l'utilisation des adresses IPv4 publiques et consulter des recommandations pour publier les adresses IP Elastic non utilisées.	28 juillet 2023
Mises à jour de politique gérée par AWS : mise à jour d'une politique existante	La politique AWSIPAMServiceRolePolicy existante a été mise à jour.	25 janvier 2023
Intégration d'IPAM à des comptes extérieurs à votre organisation	Vous pouvez désormais gérer les adresses IP extérieures à votre organisation à partir d'un seul compte IPAM et partager des groupes IPAM avec les comptes d'autres AWS Organizations.	25 janvier 2023
Bloc CIDR contigu IPv6 fourni par Amazon pour groupes IPAM	Lorsque vous créez un groupe IPAM dans la portée publique, vous pouvez désormais provisionner un bloc CIDR contigu IPv6 fourni par Amazon pour le groupe. Pour de plus amples informations, veuillez consulter Création de groupes IPv6.	25 janvier 2023

Fonction	Description	Date de parution
Première version	Cette version présente Amazon VPC IP Address Manager.	2 décembre 2021

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.