



IP Address Manager

# Amazon Virtual Private Cloud



## Amazon Virtual Private Cloud: IP Address Manager

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

# Table of Contents

Qu'est-ce qu'IPAM ? .....	1
Fonctionnement d'IPAM .....	2
Démarrage avec IPAM .....	4
Accès à IPAM .....	4
Configuration des options d'intégration pour votre IPAM .....	5
Intégration d'IPAM aux comptes d'une organisation AWS .....	6
Intégration d'IPAM à des comptes extérieurs à votre organisation .....	9
Utilisation d'IPAM avec un seul compte .....	11
Création d'un IPAM .....	12
Planification de l'approvisionnement des adresses IP .....	15
Exemples de plans de groupes IPAM .....	17
Création de groupes IPv4 .....	19
Création de groupes IPv6 .....	29
Allocation de CIDR .....	38
Création d'un VPC qui utilise un CIDR de groupe IPAM .....	39
Allocation manuelle d'un CIDR à un groupe pour réserver de l'espace d'adresse IP .....	40
Gestion de l'espace d'adressage IP dans IPAM .....	42
Automatisation des mises à jour des listes de préfixes avec IPAM .....	43
La solution au problème .....	43
Fonctionnement .....	43
Contexte d'utilisation .....	44
Prérequis .....	44
Étapes de configuration .....	44
Modifier l'état de contrôle des CIDR VPC .....	50
Création de portées supplémentaires .....	51
Suppression d'un IPAM .....	53
Suppression d'un groupe .....	55
Suppression d'une portée .....	56
Pour désapprovisionner un CIDR de groupe .....	57
Modifier un groupe IPAM .....	58
Activation de la répartition des coûts .....	59
Intégrer le VPC IPAM à l'infrastructure Infoblox .....	61
Vue d'ensemble du processus d'intégration .....	61
Quand utiliser cette intégration .....	61

Conditions préalables .....	44
Rôle IAM pour Infoblox .....	62
Configurer l'intégration d'Infoblox dans le VPC IPAM .....	62
Étapes suivantes .....	64
Activer le provisionnement de CIDR GUA IPv6 privés .....	64
Renforcez l'utilisation d'IPAM pour la création de VPC avec SCPs .....	66
Appliquer l'IPAM lors de la création VPCs .....	66
Appliquer un pool IPAM lors de la création VPCs .....	67
Appliquer l'IPAM pour tous sauf pour une liste donnée OUs .....	68
Exclure les unités organisationnelles d'IPAM .....	69
Comment fonctionnent les exclusions UO .....	69
Ajouter ou supprimer des exclusions d'UO .....	71
Modifier un niveau IPAM .....	77
Modifiez les régions d'exploitation IPAM .....	79
Approvisionnement de CIDR à un groupe .....	80
Déplacez des CIDR VPC entre les portées .....	82
Définition de la stratégie IPv4 d'allocation .....	83
Libération d'une allocation .....	89
Partage d'un groupe IPAM à l'aide d'AWS RAM .....	91
Utilisation des découvertes de ressources .....	93
Créer une découverte de ressources .....	94
Afficher les détails d'une découverte de ressources .....	96
Partage d'une découverte de ressources .....	98
Associer une découverte de ressources à un IPAM .....	101
Dissocier une découverte de ressources .....	102
Supprimer une découverte de ressources .....	103
Suivi de l'utilisation des adresses IP dans IPAM .....	104
Contrôle de l'utilisation des CIDR à l'aide du tableau de bord IPAM .....	104
Contrôle de l'utilisation du CIDR par ressource .....	108
Surveiller l'IPAM avec Amazon CloudWatch .....	112
Gestion des alarmes .....	113
Métriques relatives aux groupes et périmètres .....	115
Métriques d'utilisation des ressources .....	119
Afficher l'historique des adresses IP .....	124
Affichage de Public IP Insights .....	128
Didacticiels .....	134

Prise en main de l'IPAM à l'aide de l'interface de ligne de commande AWS .....	134
Prérequis .....	44
Création d'un IPAM .....	135
Obtention de l'ID de portée IPAM .....	135
Création d'un groupe IPv4 de niveau supérieur .....	136
Création d'un groupe IPv4 régional .....	137
Création d'un groupe IPv4 de développement .....	138
Création d'un VPC utilisant un CIDR de groupe IPAM .....	139
Vérification de l'allocation du groupe IPAM .....	139
Résolution des problèmes .....	139
Nettoyage des ressources .....	140
Étapes suivantes .....	141
Créer un IPAM et des groupes à l'aide de la console .....	142
Prérequis .....	44
Comment AWS Organizations s'intègre à IPAM .....	143
Étape 1 : délégation d'un administrateur IPAM .....	144
Étape 2 : création d'un IPAM .....	146
Étape 3 : Création d'un groupe IPAM de niveau supérieur .....	148
Étape 4 : création de groupes IPAM régionaux .....	153
Étape 5 : création d'un groupe de développement de pré-production .....	157
Étape 6 : partage du groupe IPAM .....	161
Étape 7 : création d'un VPC avec un CIDR alloué à partir d'un groupe IPAM .....	166
Étape 8 : nettoyage .....	170
Créer un IPAM et des groupes en utilisant la AWS CLI .....	172
Étape 1 : activation d'IPAM dans votre organisation .....	173
Étape 2 : création d'un IPAM .....	173
Étape 3 : création d'un groupe d'adresses IPv4 .....	175
Étape 4 : approvisionnement d'un CIDR au groupe de niveau supérieur .....	177
Étape 5. Création d'un groupe régional avec un CIDR provenant du groupe de niveau supérieur .....	178
Étape 6 : approvisionnement d'un CIDR au groupe régional .....	180
Étape 7. Création d'un partage RAM pour activer les attributions IP entre les comptes .....	182
Étape 8. Création d'un VPC .....	183
Étape 9. Nettoyage .....	184
Afficher l'historique des adresses IP à l'aide de la AWS CLI .....	184
Présentation .....	185

Scénarios .....	185
Apporter votre ASN à l'IPAM .....	193
Conditions préalables à l'onboarding de votre ASN .....	194
Étapes du didacticiel .....	195
Apporter vos adresses IP à IPAM .....	199
Vérification du contrôle du domaine .....	200
BYOIP avec console AWS et CLI .....	207
BYOIP avec CLI AWS uniquement .....	235
Utilisez votre propre adresse IP pour CloudFront utiliser IPAM .....	284
Transfert d'un CIDR IPv4 BYOIP vers IPAM .....	288
Étape 1 : Création de profils d'AWS CLI nommés et de rôles IAM .....	289
Étape 2 : obtention de l'ID de portée publique de votre IPAM .....	289
Étape 3 : création d'un groupe IPAM .....	290
Étape 4 : partager le groupe IPAM en utilisant AWS RAM .....	292
Étape 5 : transfert d'un CIDR IPV4 BYOIP existant vers IPAM .....	295
Étape 6 : affichage du CIDR dans IPAM .....	297
Étape 7 : nettoyage .....	298
Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau .....	301
Étape 1 : Création d'un VPC .....	302
Étape 2 : créer un groupe de planification des ressources .....	303
Étape 3 : créer des groupes de sous-réseaux .....	304
Étape 4 : créer des sous-réseaux .....	305
Étape 5 : nettoyage .....	306
Allouer des adresses IP Elastic séquentielles à partir d'un groupe IPAM .....	306
Étape 1 : création d'un IPAM .....	308
Étape 2 : création d'un groupe IPAM et provisionnement d'un CIDR .....	310
Étape 3 : allocation d'une adresse IP Elastic à partir du groupe .....	314
Étape 4 : associer l'adresse IP élastique à une EC2 instance .....	316
Étape 5 : suivre et surveiller l'utilisation du groupe .....	316
Nettoyage .....	318
Gestion des identités et des accès dans IPAM .....	320
Rôles liés à un service pour IPAM .....	320
Autorisations de rôles liés à un service .....	321
Création du rôle lié à un service .....	321
Modifier le rôle lié à un service .....	322
La suppression du rôle lié à un service .....	322

Stratégies gérées pour IPAM .....	323
Mises à jour de la politique AWS gérée .....	325
Exemple de stratégie .....	327
Quotas .....	330
Tarification .....	335
Afficher les informations sur la tarification .....	335
Consultez vos coûts et votre utilisation actuels à l'aide de AWS Cost Explorer .....	335
Informations connexes .....	337
Historique de document .....	338
.....	cccxlii

# 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

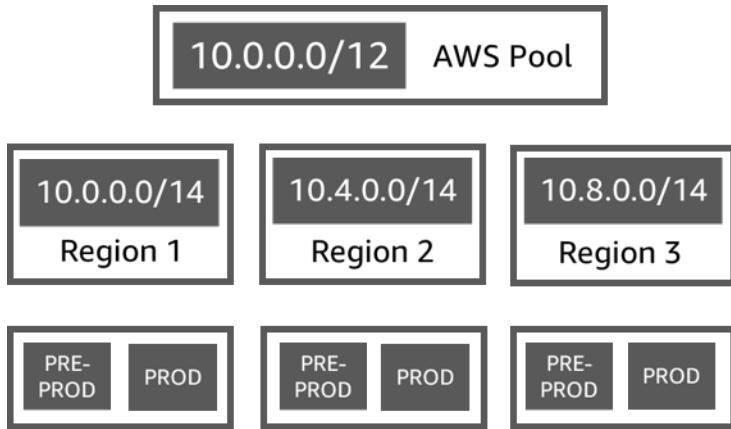
Ce guide comprend les sections suivantes :

- [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. Lorsque vous créez un IPAM, un périmètre public par défaut et un périmètre privé par défaut sont automatiquement créés pour vous. Chaque portée représente l'espace IP d'un réseau unique. Le périmètre privé est destiné à toutes les adresses IP qui ne peuvent pas être publiées sur Internet. Le périmètre public est généralement destiné à toutes les adresses IP qui peuvent être publiées sur Internet à partir d'AWS. Notez que lorsque vous [fournissez des adresses BYOIPv6 à un groupe IPAM](#), vous pouvez configurer les adresses pour qu'elles ne soient pas publiées publiquement, même si elles se situent dans le périmètre public. 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 surveiller l'espace IPv6 public et privé. Pour plus d'informations sur les adresses IPv6 publiques et privées, voir [Adresses IPv6](#) dans le Guide de l'utilisateur Amazon VPC.

Pour commencer et créer un IPAM, consultez [Démarrage avec IPAM](#).

# Démarrage avec IPAM

Suivez les étapes de cette section pour démarrer avec IPAM. Cette section est destinée à vous aider à démarrer rapidement avec IPAM, mais vous constaterez peut-être que les étapes décrites dans cette section ne répondent pas à vos besoins. Pour plus d'informations sur les différentes manières d'utiliser IPAM, reportez-vous aux sections [Planification de l'approvisionnement des adresses IP](#) et [Didacticiels pour Amazon VPC IP Address Manager \(IPAM\)](#).

Dans cette section, 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.

## Tâches

- [Accès à IPAM](#)
- [Configuration des options d'intégration pour votre IPAM](#)
- [Création d'un IPAM](#)
- [Planification de l'approvisionnement des adresses IP](#)
- [Allouer des CIDR à partir d'un groupe IPAM](#)

## 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/>.
- AWS Command Line Interface (AWS CLI) : fournit des commandes pour un vaste éventail de services AWS, dont Amazon VPC. L'AWS CLI est prise en charge sur Windows, macOS et Linux. Pour obtenir la 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 relative à l'exécution d'un processus dans la console, nous incluons des liens vers la documentation de référence sur les commandes de l'AWS CLI, de sorte que vous puissiez effectuer les mêmes tâches en utilisant 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 options d'intégration pour votre IPAM](#).

## Configuration des options d'intégration pour votre IPAM

Cette section décrit les options qui s'offrent à vous pour intégrer IPAM aux organisations AWS ou à d'autres comptes AWS, ou pour l'utiliser avec un seul compte AWS.

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 [Intégration d'IPAM aux comptes d'une organisation AWS](#) (français non garanti).
- Après l'intégration à AWS Organizations, veuillez consulter la section [Intégration d'IPAM à des comptes extérieurs à votre organisation](#) afin d'intégrer 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

- [Intégration d'IPAM aux comptes d'une organisation AWS](#)
- [Intégration d'IPAM à des comptes extérieurs à votre organisation](#)
- [Utilisation d'IPAM avec un seul compte](#)

## Intégration d'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 à AWS Organizations et la délégation d'un administrateur IPAM présentent les avantages suivants :

- Partagez vos groupes IPAM avec votre organisation : lorsque vous délégez un compte IPAM, IPAM active d'autres comptes membres AWS Organizations pour allouer des CIDR à partir de groupes 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 délégez un compte IPAM, vous autorisez IPAM à contrôler l'utilisation de l'IP sur tous vos comptes. Ainsi, IPAM importe automatiquement les CIDR utilisés par les VPC existants sur d'autres comptes membres AWS Organizations dans IPAM.

Si vous ne délégez pas de compte membre AWS Organizations comme compte IPAM, IPAM ne contrôlera les ressources que dans le compte AWS que vous utilisez pour créer l'IPAM.

### Note

Lors de l'intégration à AWS Organizations :

- Vous devez activer l'intégration avec AWS Organizations à l'aide d'IPAM dans AWS CloudWatch Metrics à l'aide de l'interface de ligne de commande [enable-ipam-organization-admin-account](#) AWS. Cela garantit que le AWS Service Role For IPAM rôle lié à un service est créé. Si vous activez l'accès approuvé avec AWS Organizations en utilisant le AWS CloudWatch Metrics.

Organizations ou la commande de l'interface de ligne de commande [register-delegated-administrator](#) AWS, AWS*ServiceRoleForIPAM* le rôle lié au service n'est pas créé et vous ne pouvez ni gérer ni surveiller les ressources au sein de votre organisation.

- Le compte IPAM doit être un compte membre des organisations AWS. Vous ne pouvez pas utiliser le compte de gestion AWS Organizations comme compte IPAM. Pour vérifier si votre IPAM est déjà intégré aux organisations AWS, suivez les étapes ci-dessous et consultez les détails de l'intégration dans les paramètres de l'organisation.
- 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 posséder un compte dans AWS Organizations et 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 utiliser 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 service *AWS*ServiceRoleForIPAM**.
- L'utilisateur associé au compte de gestion AWS Organizations doit être utiliser un rôle IAM qui a les actions de politique IAM suivantes attachées :
  - `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 organisations AWS peut utiliser un rôle IAM auquel sont attachées les actions de politique IAM suivantes pour dresser la liste de 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 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. L'option Déléguer n'est disponible que si vous êtes connecté à la console en tant que compte de gestion AWS Organizations. Choisissez Delegate (Déléguer).
5. Saisissez l'ID de compte AWS d'un compte IPAM. L'administrateur IPAM doit être un compte membre AWS Organizations.
6. Sélectionnez Enregistrer les modifications.

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes de l'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 l'AWS CLI, utilisez la commande suivante : [enable-ipam-organization-admin-account](#)

Lorsque vous délégez 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 gestion AWS Organizations qui a délégué l'administrateur IPAM est maintenant terminé. 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 [Intégration d'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](#).

[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 [Intégration d'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 [Intégration d'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 [Création d'une découverte de ressources à intégrer à un autre IPAM](#) et [Partage d'une découverte de ressources avec un autre compte AWS](#)) (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 [Intégration d'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 Gestion des identités et des accès AWS (IAM).

Les rôles liés à un service sont un type de rôle IAM qui permet à des services AWS d'accéder à d'autres services AWS en votre nom. Ils simplifient le processus de gestion des autorisations en créant et en gérant automatiquement les autorisations nécessaires pour que des services AWS spécifiques puissent effectuer les actions requises, rationalisant ainsi la configuration et l'administration de ces services.

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 l'IPAM aux AWS Organizations, IPAM a besoin de votre autorisation pour répliquer les informations relatives à l'utilisation des ressources et des adresses IP entre les comptes (des comptes membres au compte membre délégué de l'IPAM) et entre AWS les régions (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 AWS régions dans lesquelles l'IPAM est autorisé à gérer l'adresse IP. CIDRs Ces AWS régions sont appelées régions opérationnelles. L'IPAM découvre et surveille les ressources uniquement dans les AWS régions que vous sélectionnez comme régions opérationnelles. IPAM ne stocke aucune donnée en dehors des Régions d'exploitation que vous sélectionnez.

L'exemple de hiérarchie suivant montre l'impact des AWS régions que vous attribuez lors de la création de l'IPAM sur les régions qui seront disponibles pour les pools que vous créerez ultérieurement.

- IPAM opérant dans les AWS régions 1 et AWS 2
  - 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 <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans la console AWS de gestion, choisissez la AWS région 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 Régions opérationnelles, sélectionnez les AWS régions dans lesquelles cet IPAM peut gérer et découvrir des ressources. La AWS région dans laquelle vous créez votre IPAM est sélectionnée comme l'une des régions opérationnelles par défaut. Par exemple, si vous créez cet IPAM dans une AWS région us-east-1 mais que vous souhaitez créer ultérieurement des pools IPAM régionaux qui le fournissent CIDRs us-west-2, sélectionnez us-west-2 ici. VPCs 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. Choisissez si vous souhaitez activer le IPv6 GUA privé CIDRs. Pour plus d'informations sur cette option, consultez [Activer le provisionnement de CIDR GUA IPv6 privés](#).
8. Choisissez si vous souhaitez activer le Mode de mesure. Pour plus d'informations sur cette option, consultez [Activation de la répartition des coûts](#).
9. Sélectionnez Create IPAM (Créer un IPAM).

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes de l'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, modifier et afficher les informations relatives à votre IPAM :

1. Créez l'IPAM : [create-ipam](#)

2. Affichez l'IPAM que vous avez créé : [describe-ipams](#)
3. Consultez les étendues 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 les sélectionnant IPAMs dans le volet 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 groupe est différent pour les groupes situés dans des périmètres publics et privés. Cette section décrit les étapes de création d'un groupe régional dans le périmètre privé. Pour les tutoriels BYOIP et BYOASN, consultez [Didacticiels](#).

### Important

Pour utiliser des groupes IPAM sur des comptes AWS, vous devez intégrer IPAM à AWS Organizations. Sinon, certaines fonctions risquent de ne pas fonctionner correctement. Pour de plus amples informations, consultez [Intégration d'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 groupes pour des Régions AWS 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 Région 1 AWS et Région 2 AWS
  - Portée privée
    - Groupe de niveau supérieur
    - Groupe régional dans Région 1 AWS
      - 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 [Allouer des CIDR à partir d'un groupe IPAM](#).

### Table des matières

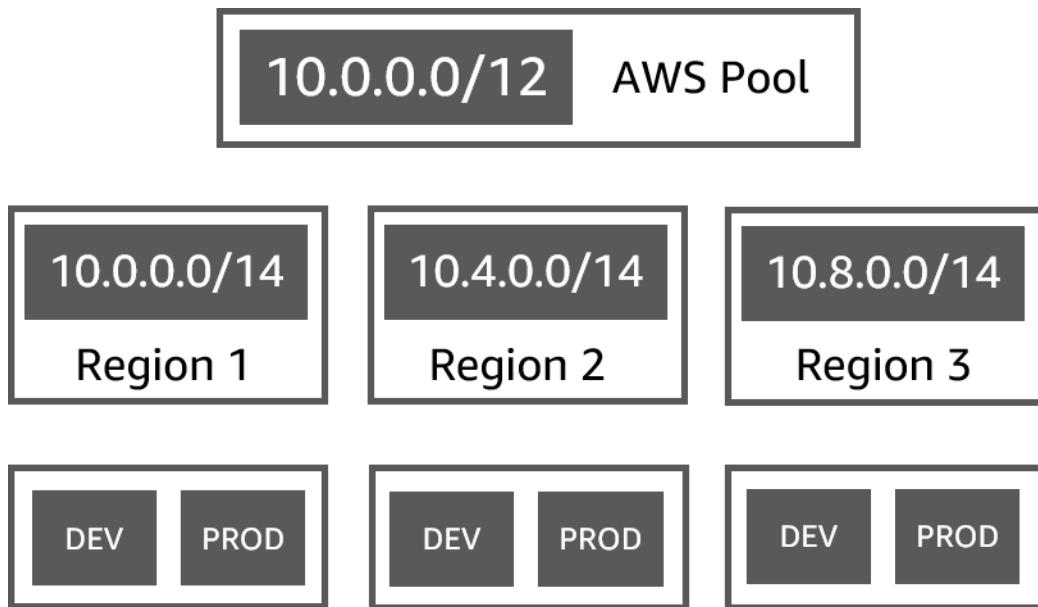
- [Exemples de plans de groupes IPAM](#)
- [Création de groupes IPv4](#)
- [Créez des groupes d'adresses IPv6 dans votre IPAM](#)

## 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.

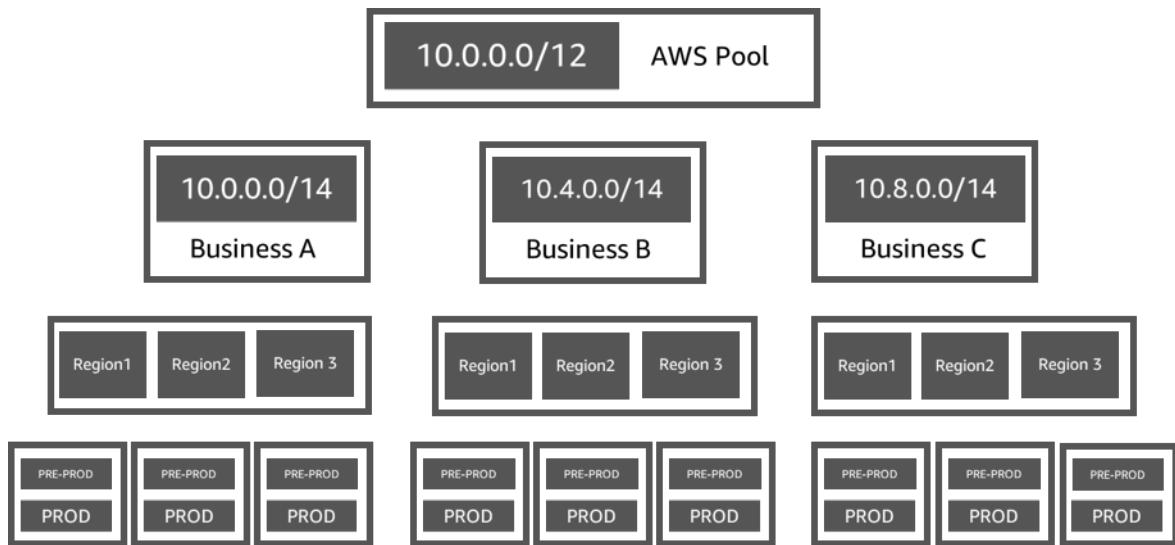
### IPv4 piscines dans plusieurs AWS régions

L'exemple suivant montre une hiérarchie de pool IPAM pour plusieurs AWS régions au sein d'un pool de niveau supérieur. Chaque pool AWS régional comprend deux pools de développement IPAM, un pool pour les ressources de développement et un pool pour les ressources de production.



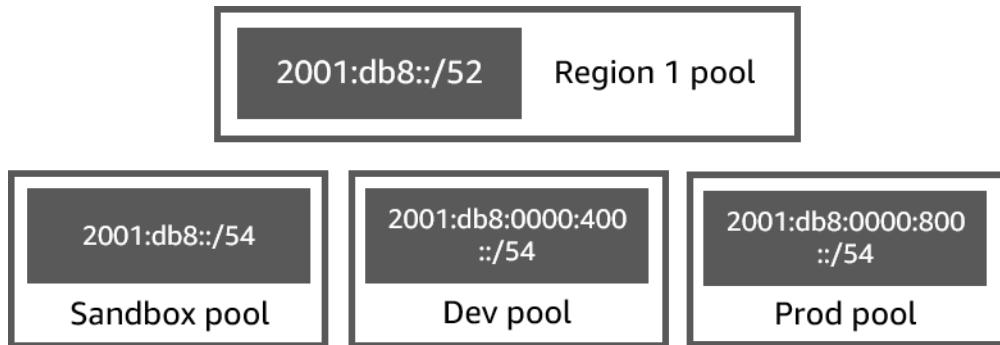
### IPv4 pools pour plusieurs secteurs d'activité

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



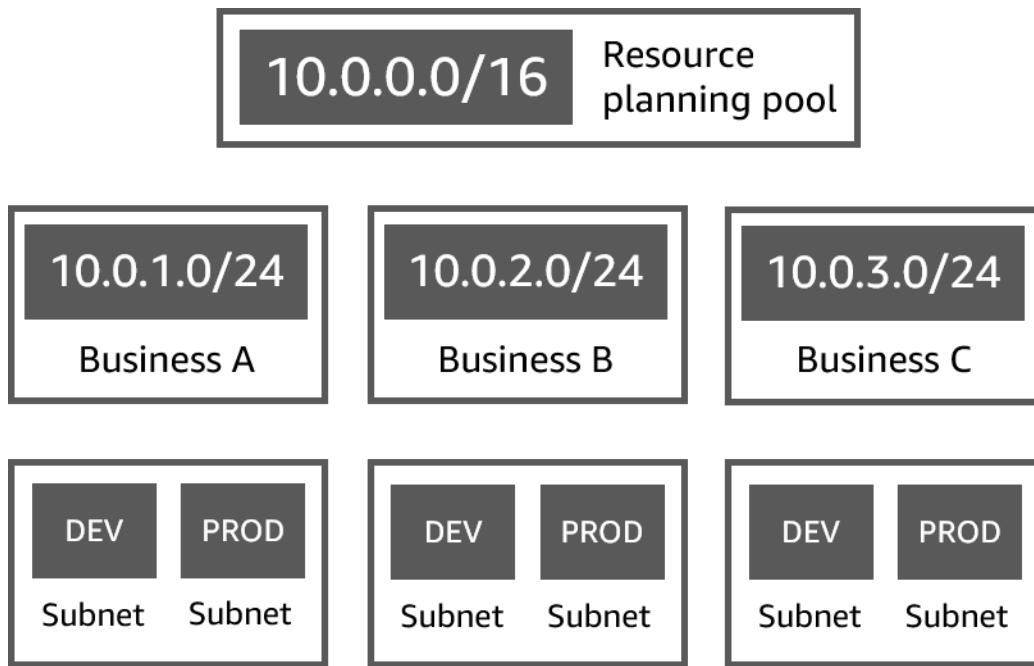
## IPv6 piscines dans une AWS région

L'exemple suivant montre une hiérarchie de IPv6 pool IPAM pour plusieurs secteurs d'activité au sein d'un pool 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, consultez [Partage 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, la création d'une ressource à l'aide d'un CIDR supérieur à /24 à partir de ce groupe enfreint une règle d'allocation concernant le groupe et la création échoue. Les ressources existantes dont le CIDR est supérieur à /24 sont signalées comme non conformes.

### **⚠️ 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, consultez [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. Sous Address family (Famille d'adresses), choisissez IPv4.
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, consultez [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.

Remarques :

- 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.

 Note

Les règles d'allocation s'appliquent uniquement aux [ressources gérées](#) au sein de ce groupe. Les règles ne s'appliquent pas aux ressources de groupes au sein d'un groupe.

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 sur les commandes 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 [Allouer des CIDR à partir d'un groupe IPAM](#).

### Note

Le processus de création de groupe est différent pour les groupes situés dans des périmètres publics et privés. Cette section décrit les étapes de création d'un groupe régional dans le périmètre privé. Pour les tutoriels 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 Région 1 AWS et Région 2 AWS
  - Portée privée
  - Groupe de niveau supérieur (10.0.0.0/8)
    - Groupe régional dans région AWS 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. Si vous créez ce groupe dans un périmètre public, vous verrez une option pour la famille d'adresses. Choisissez IPv4.
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. 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.

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.

 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. Si vous créez ce groupe dans un périmètre public, vous verrez une option pour le 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. (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.
12. 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.
13. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
14. Lorsque vous avez fini de configurer votre groupe, choisissez Create pool (Créer un groupe).
15. Consultez [Création d'un groupe IPv4 de développement](#).

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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 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 [Allouer des CIDR à partir d'un groupe IPAM](#).

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, sélectionnez 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. (En option) Sélectionnez 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 [Allouer des CIDR à partir d'un groupe IPAM](#).

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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.

## Créez des groupes d'adresses IPv6 dans votre IPAM

AWS offre une connectivité IPv6 à plusieurs de ses services, notamment EC2, VPC et S3, ce qui vous permet de profiter de l'espace d'adressage accru ainsi que des fonctionnalités de sécurité améliorées d'IPv6. IPv6 a été conçu pour résoudre cette limitation fondamentale de l'IPv4. En passant à un espace d'adressage de 128 bits, IPv6 offre un grand nombre d'adresses IP uniques. Cette extension massive des adresses permet la prolifération continue des technologies connectées, qu'il s'agisse de smartphones, d'appareils IoT ou d'infrastructures cloud.

Vous pouvez par ailleurs utiliser l'IPAM pour vous assurer d'utiliser des CIDR IPv6 contigus dans le cadre de la création de VPC. Les CIDR contigus sont alloués de manière séquentielle. Ils vous permettent de simplifier vos règles de sécurité et de mise en réseau. Les CIDR IPv6 peuvent être

regroupés au sein d'une seule entrée dans des structures de réseau et de sécurité telles que des listes de contrôle d'accès, des tables de routage, des groupes de sécurité et des pare-feu.

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.

### Note

L'adressage IPv6 public et privé est disponible dans AWS. AWS prend en compte les adresses IP publiques à partir desquelles les annonces sont publiées sur Internet depuis AWS, tandis que les adresses IP privées ne sont pas et ne peuvent pas être annoncées sur Internet à partir d'AWS. Si vous souhaitez que vos réseaux privés prennent en charge le protocole IPv6 et que vous n'avez pas l'intention d'acheminer le trafic de ces adresses vers Internet, créez votre groupe IPv6 dans un périmètre privé. Pour plus d'informations sur les adresses IPv6 publiques et privées, voir [Adresses IPv6](#) dans le Guide de l'utilisateur Amazon VPC.

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
    - 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. Ils montrent que le groupe de développement au sein du groupe régional est approvisionné par une partie du groupe régional CIDR.

## Table des matières

- [Création d'un groupe d'adresses IPv6 régionales dans votre IPAM](#)
- [Création d'un groupe IPv6 de développement dans votre IPAM](#)

## Création d'un groupe d'adresses IPv6 régionales dans votre IPAM

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
    - 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](#).

### Note

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, consultez [Partage 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.

### Note

- Cette section explique comment créer un groupe régional IPv6 avec une plage d'adresses IPv6 fournie par AWS ou avec une plage IPv6 privée. Si vous souhaitez intégrer vos propres plages d'adresses IP IPv4 ou IPv6 publiques à AWS (BYOIP), certaines conditions sont requises. Pour de plus amples informations, consultez [Didacticiel : apporter vos adresses IP à IPAM](#).
- Si vous créez un groupe IPv6 dans un périmètre privé, vous pouvez utiliser un GUA ou une plage ULA IPv6 privée. Pour utiliser une plage GUA privée, vous devez d'abord avoir activé l'option sur votre IPAM (voir [Activer le provisionnement de CIDR GUA IPv6 privés](#)).

## 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, sélectionnez Pools (Groupes).
3. Sélectionnez Create pool (Créer un groupe).
4. Sous Portée IPAM, sélectionnez le périmètre public ou privé. Si vous souhaitez que vos réseaux privés prennent en charge le protocole IPv6 et que vous n'avez pas l'intention d'acheminer le trafic de ces adresses vers Internet, choisissez un périmètre privé. 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.

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. Si vous créez ce groupe dans le périmètre public, tous les CIDR de ce groupe pourront être publiés publiquement.
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. Si vous souhaitez provisionner un bloc CIDR IPv6 fourni par Amazon à un groupe, il doit être provisionné dans un groupe avec des paramètres régionaux (région AWS) sélectionnés. 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 choisies pour l'IPAM lors de sa création. Vous pouvez ajouter des régions d'exploitation à tout moment.

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.

**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. (Facultatif) Si vous créez un groupe IPv6 dans le périmètre public, 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. (Facultatif) Si vous créez un groupe IPv6 dans un périmètre public, sous l'option Source IP publique, choisissez Propriété d'Amazon pour 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, consultez [Didacticiel : apporter vos adresses IP à IPAM](#).
12. (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. Pour provisionner un CIDR, effectuez l'une des actions suivantes :
  - Si vous créez un groupe IPv6 dans un périmètre public avec une source IP publique appartenant à Amazon, pour provisionner un CIDR, sous CIDR à provisionner, choisissez Ajouter un CIDR appartenant à Amazon, puis la taille du masque réseau du CIDR (entre /40 et /52). 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. 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 (français non garanti) [Quotas pour votre IPAM](#).
  - Si vous créez un groupe IPv6 dans un périmètre privé, vous pouvez utiliser un GUA ou une plage ULA IPv6 privée :
    - Pour plus de détails sur l'adressage IPv6 privé, voir [Adresses IPv6 privées](#) dans le Guide de l'utilisateur Amazon VPC.

- Pour utiliser une plage ULA IPv6 privée, sous CIDR à provisionner, choisissez Ajouter une adresse CIDR ULA par masque réseau puis choisissez une taille de masque réseau ou choisissez Input private IPv6 CIDR et entrez une plage ULA. L'espace IPv6 ULA valide est tout ce qui est inférieur à fd00::/8 qui ne chevauche pas la plage réservée Amazon fd00::/16.
- Pour utiliser une plage GUA IPv6 privée, vous devez d'abord avoir activé l'option sur votre IPAM (voir [Activer le provisionnement de CIDR GUA IPv6 privés](#)). Une fois que vous avez activé les CIDR GUA IPv6 privés, entrez un GUA IPv6 dans Input private IPv6 CIDR.

13. 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.

14. (En option) Sélectionnez Tags (Étiquettes) pour le groupe.
15. Sélectionnez Create pool (Créer un groupe).
16. Consultez [Création d'un groupe IPv6 de développement dans votre IPAM](#).

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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. Si vous souhaitez activer le provisionnement des CIDR GUA IPv6 privés, modifiez l'IPAM avec [modify-ipam](#) et incluez l'option enable-private-gua. Pour de plus amples informations, consultez [Activer le provisionnement de CIDR GUA IPv6 privés](#).
2. Créez un groupe avec : [create-ipam-pool](#).
3. Attribuer un CIDR au groupe : [provision-ipam-pool-cidr](#).
4. Modifiez le groupe après l'avoir créé pour modifier les règles d'allocation : [modify-ipam-pool](#).

## Création d'un groupe IPv6 de développement dans votre IPAM

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 [Allouer des CIDR à partir d'un groupe IPAM](#).

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
    - 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, sélectionnez Pools (Groupes).
3. Sélectionnez Create pool (Créer un groupe).
4. Sous Portée IPAM, sélectionnez un périmètre. 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, 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. (En option) Sélectionnez 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 d'adresses IPv6 régionales dans votre IPAM](#) 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 [Allouer des CIDR à partir d'un groupe IPAM](#).

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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.

## Allouer des CIDR à partir d'un groupe IPAM

L'une des fonctionnalités importantes d'IPAM est sa capacité d'allouer et de gérer l'espace d'adressage IP. Lorsque vous créez un VPC, vous devez spécifier un bloc d'adresse IP CIDR, qui définit la plage d'adresses IP disponibles pour ce VPC. IPAM simplifie ce processus en fournissant une vue globale de l'ensemble de votre inventaire d'adresses IP, ce qui vous aide à attribuer et à réutiliser de manière stratégique des prefixes IP sur plusieurs VPC.

Cette allocation d'espace d'adressage est cruciale pour garantir l'absence de chevauchement des plages d'adresses IP, ce qui pourrait entraîner des conflits de routage et des problèmes de connectivité. IPAM vous permet également de réserver de l'espace d'adresse IP pour une future extension du VPC, évitant ainsi de devoir procéder plus tard à une renumérotation complexe.

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

Avec Amazon Virtual Private Cloud (Amazon VPC), vous pouvez lancer des ressources AWS dans un réseau virtuel logiquement isolé que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Un cloud privé virtuel (VPC) est un réseau virtuel dédié à votre compte AWS. Il est logiquement isolé des autres réseaux virtuels dans le cloud AWS. Vous pouvez spécifier une plage d'adresses IP pour le VPC, ajouter des sous-réseaux, ajouter des passerelles et associer des groupes de sécurité.

Suivez les étapes décrites dans la section [Create a VPC](#) du Guide d'utilisation d'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 sur 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, sélectionnez 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 sur les commandes 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. Notez que cette section est un regroupement de procédures toutes liées à l'utilisation d'IPAM. Les procédures sont classées par ordre alphabétique.

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

- [Automatisation des mises à jour des listes de préfixes avec IPAM](#)
- [Modifiez l'état de contrôle des CIDR VPC](#)
- [Création de portées supplémentaires](#)
- [Suppression d'un IPAM](#)
- [Suppression d'un groupe](#)
- [Suppression d'une portée](#)
- [Pour désapprovisionner un CIDR de groupe](#)
- [Modifier un groupe IPAM](#)
- [Activation de la répartition des coûts](#)
- [Intégrer le VPC IPAM à l'infrastructure Infoblox](#)
- [Activer le provisionnement de CIDR GUA IPv6 privés](#)
- [Renforcez l'utilisation d'IPAM pour la création de VPC avec SCPs](#)
- [Exclure les unités organisationnelles d'IPAM](#)
- [Modifier un niveau IPAM](#)
- [Modifiez les régions d'exploitation IPAM](#)
- [Approvisionnement de CIDR à un groupe](#)
- [Déplacez des CIDR VPC entre les portées](#)
- [Définir une stratégie IPv4 d'allocation publique avec les politiques de l'IPAM](#)
- [Libération d'une allocation](#)
- [Partage d'un groupe IPAM à l'aide d'AWS RAM](#)

- [Utilisation des découvertes de ressources](#)

## Automatisation des mises à jour des listes de préfixes avec IPAM

Une [liste de préfixes gérée](#) est un ensemble de blocs CIDR que vous pouvez référencer dans des règles de groupe de sécurité et des tables de routage au lieu de spécifier des adresses IP individuelles. Par exemple, au lieu de créer des règles de groupe de sécurité distinctes pour `10.1.0.0/16`, `10.2.0.0/16`, et `10.3.0.0/16`, vous pouvez créer une liste de préfixes contenant les trois CIDR et référencer cette dernière dans une seule règle.

Deux types de listes de préfixes existent :

- Listes de préfixes gérées par le client : plages d'adresses IP que vous définissez et gérez
- Listes de préfixes gérées par AWS : plages d'adresses IP associées à des services AWS (tels que S3 ou CloudFront)

Cette fonctionnalité IPAM automatise la gestion des listes de préfixes gérées par le client, en faisant en sorte que vos entrées CIDR demeurent synchronisées avec les modifications apportées au réseau.

### La solution au problème

Sans automatisation, les équipes réseau passent beaucoup de temps à mettre à jour manuellement les listes de préfixes lorsque l'infrastructure évolue et à maintenir des listes de préfixes cohérentes entre les environnements et les régions.

L'IPAM résout ce problème en vous permettant de créer des règles qui renseignent automatiquement les listes de préfixes. Vous pouvez utiliser deux approches : référencer les CIDR à partir de vos groupes IPAM ou créer des règles basées sur vos ressources AWS réelles, telles que « inclure tous les VPC balisés avec env=prod », « inclure tous les sous-réseaux dans us-east-1 » ou « inclure toutes les adresses IP Elastic détenues par le compte 123456789 ». Lorsque vous ajoutez ou supprimez ces ressources, l'IPAM met automatiquement à jour la liste de préfixes avec leurs CIDR.

### Fonctionnement

Créez des règles qui indiquent à l'IPAM les adresses IP à inclure dans une liste de préfixes. Par exemple, « inclure tous les CIDR VPC balisés avec env=prod ». Lorsque vous ajoutez ou supprimez des VPC de production, l'IPAM met automatiquement à jour la liste de préfixes.

## Contexte d'utilisation

- Groupes de sécurité : créez une règle « inclure tous les VPC balisés avec env=prod » pour que lors de l'ajout de nouveaux VPC de production, ces derniers soient automatiquement autorisés dans les règles de vos groupes de sécurité.
- Multi-région : déployez les mêmes règles IPAM dans plusieurs régions pour conserver des listes de préfixes identiques sans copier manuellement les entrées CIDR.
- Infrastructure dynamique : lorsque vous créez/supprimez des VPC ou des sous-réseaux, leurs CIDR sont automatiquement ajoutés/supprimés des listes de préfixes sans mise à jour manuelle.

## Prérequis

Avant de commencer, assurez-vous de ce qui suit :

- Vous disposez d'un [IPAM](#) pour lequel le [Niveau avancé](#) est activé.
- Vous disposez d'une [liste de préfixes gérée par le client](#) (ou vous allez en créer une lors de la configuration).
- Vous disposez des [Autorisations IAM](#) dans le cadre des opérations de liste de préfixes IPAM et EC2.

## Étapes de configuration

### Étape 1 : création d'un résolveur de liste de préfixes IPAM

Définissez les CIDR à inclure dans votre liste de préfixes en créant un résolveur de liste de préfixes IPAM.

#### AWS Management Console

Pour créer un résolveur de liste de préfixes IPAM

1. Ouvrez la [console IPAM](#).
2. Dans le panneau de navigation, sélectionnez Résolveurs de listes de préfixes.
3. Sélectionnez Créer un résolveur de liste de préfixes.
4. À l'étape 1 : configurer les détails du résolveur, choisissez les éléments suivants :
  - IPAM : instance IPAM

- Famille d'adresses : IPv4 ou IPv6
  - Balise Nom – facultatif : nom descriptif
  - Description – facultatif : description
  - Balises : balises de ressource
5. Choisissez Suivant.
6. À l'étape 2 : configurer les règles, sélectionnez Ajouter une règle. Vous pouvez ajouter jusqu'à 99 règles.

 **Important**

Vous pouvez créer un résolveur de liste de préfixes sans aucune règle de sélection de CIDR, cependant le résolveur générera des versions vides (ne contenant aucun CIDR) jusqu'à ce que vous ajoutiez des règles.

7. Choisissez l'un des types de règles suivants :

- CIDR statique : liste fixe de CIDR qui ne changent pas (comme une liste manuelle répliquée entre les régions)
- CIDR du groupe IPAM : CIDR provenant de groupes IPAM spécifiques (comme tous les CIDR de votre groupe de production IPAM)

Si vous choisissez cette option, choisissez les éléments suivants :

- Portée IPAM : sélectionnez la portée IPAM pour rechercher des ressources
- Conditions:
  - Propriété
    - ID du groupe IPAM : sélectionnez un groupe IPAM contenant les ressources
    - CIDR (comme, 10.24.34.0/23)
  - Opération : égal à/non égal à
  - Valeur : valeur à laquelle répondre à la condition
- CIDR de ressource de portée : CIDR provenant de ressources AWS telles que des VPC, des sous-réseaux, des EIP dans une portée IPAM

Si vous choisissez cette option, choisissez les éléments suivants :

- Portée IPAM : sélectionnez la portée IPAM pour rechercher des ressources
- Type de ressource : sélectionnez une ressource, comme un VPC ou un sous-réseau

- Conditions:
  - Propriété:
    - ID de ressource : ID unique d'une ressource (comme vpc-1234567890abcdef0)
    - Propriétaire de la ressource (comme 111122223333)
    - Région de la ressource (comme us-east-1)
    - Balise de ressource (comme clé : nom, valeur : dev-vpc-1)
    - CIDR (comme 10.24.34.0/23)
  - Opération : égal à/non égal à
  - Valeur : valeur à laquelle répondre à la condition

8. Choisissez Suivant.
9. Choisissez Valider et créer.

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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 résolveur de liste de préfixes IPAM :

- Utilisez la commande [create-ipam-prefix-list-resolver](#) et enregistrez l'ID du résolveur renvoyé pour l'étape 2.

## Étape 2 : création d'une cible de résolveur pour se connecter à une liste de préfixes

Reliez votre résolveur à une liste de préfixes existante en créant une cible de résolveur. Utilisez l'ID du résolveur renvoyé à l'étape 1.

## AWS Management Console

Pour créer une cible de résolveur de liste de préfixes IPAM

1. Dans la console IPAM, sélectionnez Résolveurs de listes de préfixes.
2. Choisissez le résolveur que vous avez créé à l'étape 1.
3. Sur la page des détails du résolveur, sélectionnez l'onglet Cibles.

4. Sélectionnez **Créer une cible**.
5. Configurez la cible :
  - **Région** : sélectionnez la région dans laquelle se trouve la liste de préfixes gérée existante ou dans laquelle vous prévoyez d'en créer une.
  - **Liste de préfixes** : choisissez une liste de préfixes gérée existante ou créez-en une nouvelle.
6. Sous **Version souhaitée**, sélectionnez l'une des options suivantes :
  - **Toujours suivre la dernière version** : choisissez cette option pour les mises à jour automatiques lorsque vous souhaitez que vos listes de préfixes restent à jour avec les modifications de l'infrastructure sans intervention manuelle.
  - **Suivre une version spécifique** : choisissez cette option pour des raisons de stabilité lorsque vous avez besoin de mises à jour prévisibles et contrôlées et que vous souhaitez approuver manuellement les modifications apportées à vos listes de préfixes.
7. Sélectionnez **Créer une cible**.

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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 cible de résolveur de liste de préfixes IPAM :

- Utilisez la commande [create-ipam-prefix-list-resolver-target](#) avec l'ID du résolveur issu de l'étape 1 et l'ID de votre liste de préfixes existante.

L'IPAM met désormais automatiquement à jour votre liste de préfixes en fonction de vos règles. La liste des préfixes sera renseignée avec les CIDR correspondant à vos critères.

## Étape 3 : surveillance des versions et de la synchronisation

À la suite de la création d'un résolveur de liste de préfixes et d'une cible, le résolveur de liste de préfixes génère des versions de CIDR en fonction de vos règles, puis la cible synchronise ces CIDR à partir du résolveur avec une liste de préfixes gérée spécifique. Chaque version est un instantané

des CIDR qui correspondaient à vos règles à ce moment-là. Le numéro de version augmente chaque fois que la liste CIDR change en raison de modifications de l'infrastructure.

Exemple de version :

État initial (version 1)

Environnement de production :

- vpc-prod-web (10.1.0.0/16) – balisé avec env=prod
- vpc-prod-db (10.2.0.0/16) – balisé avec env=prod

Règle du résolveur : inclure tous les VPC balisés avec env=prod

CIDR version 1 : 10.1.0.0/16, 10.2.0.0/16

Modification de l'infrastructure (version 2)

Nouveau VPC ajouté :

- vpc-prod-api (10.3.0.0/16) – balisé avec env=prod

L'IPAM détecte automatiquement la modification et crée une nouvelle version.

CIDR version 2 : 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16

Cette section explique comment surveiller la création de versions à l'aide de la console AWS ou de l'interface de ligne de commande AWS et la réussite de la synchronisation avec l'interface de ligne de commande AWS.

Nous vous encourageons également à configurer des alarmes CloudWatch sur les métriques de défaillance, car vous devrez peut-être réévaluer et ajuster les règles de sélection des CIDR afin de respecter les limites de version et de taille de liste de préfixes. Pour obtenir la liste des métriques CloudWatch relatives aux listes de préfixes IPAM, consultez la section [Métriques de résolveur de listes de préfixes IPAM](#).

AWS Management Console

Pour afficher les versions créées et surveiller la synchronisation des cibles

1. Dans la console IPAM, sélectionnez Résolveurs de listes de préfixes.

2. Choisissez le résolveur que vous avez créé à l'étape 1.
3. Sur la page des détails du résolveur, sélectionnez l'onglet Versions. Vous y verrez toutes les versions créées par le résolveur ainsi que tous les CIDR contenus dans la version.
4. Sur la page de détails du résolveur, sélectionnez l'onglet Surveillance. Cette vue présente les [Métriques de résolveur de listes de préfixes IPAM](#) sous forme de graphique :
  - Réussite de la création de la version du résolveur de listes de préfixes
  - Échec de la création de la version du résolveur de listes de préfixes
5. Dans l'onglet Surveillance, vous pouvez également configurer une alarme CloudWatch en choisissant Créer une alarme en cas de création de version du résolveur de liste de préfixes. Vous êtes redirigé vers la console CloudWatch avec l'alarme partiellement configurée pour la métrique. Pour plus d'informations sur la finalisation de la création de l'alarme, consultez la section [Create a CloudWatch alarm based on a static threshold](#) dans le Guide d'utilisation d'Amazon CloudWatch..

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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 surveiller les versions et la synchronisation :

1. Utilisez la commande [get-ipam-prefix-list-resolver-version-entries](#) pour afficher la dernière version créée par le résolveur.
2. Utilisez la commande [describe-ipam-prefix-list-resolver-targets](#) pour surveiller l'état de synchronisation de la cible du résolveur.

La commande de surveillance affiche les éléments suivants :

- state : état de synchronisation actuel (create-complete, modify-complete, etc.)
- lastSyncedVersion : dernière version synchronisée avec succès
- desiredVersion : version cible avec laquelle effectuer la synchronisation
- stateMessage : détails de l'erreur en cas d'échec de la synchronisation

## Étape 4 : (facultatif) activation et désactivation de la synchronisation de la liste de préfixes IPAM

Si une liste de préfixes gérée a été configurée comme cible de liste de préfixes IPAM et que vous souhaitez apporter des modifications à la liste de préfixes sans avoir besoin d'autorisations pour accéder à la cible du résolveur de liste de préfixes IPAM, vous pouvez [modifier la liste de préfixes gérée](#) et désactiver la synchronisation avec le résolveur de liste de préfixes IPAM. Si vous désactivez cette fonctionnalité, les CIDR de la liste de préfixes ne seront pas automatiquement mis à jour et vous pourrez les modifier. Si vous activez cette fonctionnalité, les CIDR de la liste de préfixes seront automatiquement mis à jour en fonction des règles de sélection des CIDR du résolveur associé.

## 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, consultez [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, consultez [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 CIDR 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](#)

## 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 ou IPv6 privés, les CIDR de ressource sont importés dans le périmètre privé par défaut et n'apparaissent dans aucun périmètre privé 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 sur les commandes 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](#)

## Suppression d'un IPAM

Vous souhaiterez peut-être supprimer un IPAM s'il n'est plus nécessaire, si vous devez restructurer la gestion de votre adresse IP ou si vous souhaitez repartir à zéro avec une nouvelle configuration IPAM. La suppression d'un IPAM peut contribuer à simplifier la gestion de votre adresse IP et à l'adapter à l'évolution des exigences commerciales ou opérationnelles.

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](#).

### Note

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 plus d'informations, consultez [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 sur les commandes 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](#).

## Suppression d'un groupe

Un groupe IPAM dans AWS représente une plage définie d'adresses IP qui peuvent être allouées et gérées au sein d'un environnement ou d'une organisation AWS spécifique. Les groupes sont utilisés pour organiser l'espace d'adresses IP, permettre la gestion automatique des adresses IP et appliquer les politiques de gouvernance des adresses IP dans l'ensemble de votre infrastructure cloud.

Il peut être utile de supprimer un groupe IPAM afin de supprimer l'espace d'adresses IP inutilisé ou superflu et de le récupérer à d'autres fins. 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.

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

### 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 sur les commandes 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](#).

## Suppression d'une portée

Vous souhaiterez peut-être supprimer un périmètre IPAM s'il ne répond plus à son objectif, par exemple lorsque vous restructurez votre réseau, consolidez des régions ou ajustez votre allocation d'adresses IP. La suppression des périmètres inutilisés peut aider à rationaliser votre configuration IPAM et à optimiser la gestion de vos adresses IP au sein de AWS.

### Note

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 sur les commandes 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](#).

## Pour désapprovisionner un CIDR de groupe

Il peut être utile de déprovisionner un groupe CIDR afin de libérer de l'espace d'adresses IP, de simplifier la gestion des adresses IP, de se préparer à des changements de réseau ou de se conformer à des exigences de conformité. Le déprovisionnement d'un groupe CIDR permet de mieux contrôler et d'optimiser les allocations d'adresses IP au sein d'IPAM, tout en garantissant que l'espace IP inutilisé est récupéré et rendu disponible pour une utilisation future. Vous ne pouvez pas désactiver le CIDR s'il y a des allocations dans le groupe. Pour supprimer des allocations, consultez [the section called “Libération d'une allocation”](#).

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.

### 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 sur les commandes 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](#).

## Modifier un groupe IPAM

Vous pouvez modifier un groupe de façon à ce qu'il exécute l'une des opérations suivantes :

- Modifiez les règles d'allocation pour le groupe. Pour plus d'informations sur les règles d'allocations, consultez [Création d'un groupe IPv4 de niveau supérieur](#).
- Modifiez le nom, la description ou d'autres métadonnées du groupe pour améliorer l'organisation et la visibilité au sein d'IPAM.
- Modifiez les options du groupe, telles que l'importation automatique des ressources découvertes, afin d'optimiser la gestion automatique des adresses IP d'IPAM.

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

## 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](#)

## Activation de la répartition des coûts

Lorsque vous activez la répartition des coûts, vous répartissez les [frais des adresses IP actives](#) entre les comptes utilisant les adresses IP plutôt qu'auprès du propriétaire de l'IPAM. Cette fonction s'avère utile pour les grandes entreprises dans lesquelles l'administrateur IPAM délégue gère les adresses IP de manière centralisée à l'aide de l'IPAM et où chaque compte est responsable de sa propre utilisation, éliminant ainsi le besoin de calculs de facturation manuels.

L'option de répartition des coûts est disponible lorsque vous [créez un IPAM ou que vous modifiez un IPAM](#) sous Mode de mesure. Cette option offre les choix suivants :

- Propriétaire de l'IPAM (valeur par défaut) : le compte AWS propriétaire de l'IPAM est facturé pour toutes les adresses IP actives gérées dans l'IPAM.
- Propriétaire de la ressource : le compte AWS propriétaire de l'adresse IP est facturé pour l'adresse IP active.

## Prérequis

- Votre IPAM doit être [intégré à AWS Organizations](#).
- L'IPAM doit avoir été créé par l'administrateur IPAM délégué de votre organisation AWS.
- La région d'origine de l'IPAM doit être une région activée par défaut. Il ne peut pas s'agir d'une [région d'adhésion](#).

## Fonctionnement de la facturation des frais

- Même si vous pouvez répartir les frais des adresses IP au sein d'une organisation, tous les frais IPAM sont consolidés sur le compte payeur de l'organisation par le biais de la [facturation consolidée d'AWS Organizations](#).
- Lorsque la répartition des coûts est activée, les comptes membres de l'organisation peuvent toujours consulter leur utilisation individuelle de l'IPAM et leurs frais dans leurs factures de compte.
- Lorsque la répartition des coûts est activée, l'ARN de l'IPAM apparaît sur les factures des comptes individuels, ce qui permet aux propriétaires de ressources de suivre leur utilisation des adresses IP actives dans l'IPAM. Si vous utilisez les [Exportations de données AWS](#), les frais IPAM apparaissent avec l'ARN de l'IPAM associé dans les factures des comptes consolidés et individuels.
- Seuls les comptes au sein de l'organisation de l'administrateur délégué peuvent recevoir des frais pour les ressources qu'ils possèdent. Les coûts des adresses IP en dehors de l'organisation sont facturés au propriétaire de l'IPAM.

## Restrictions temporelles

- Vous avez 24 heures pour vous désinscrire après avoir activé la répartition des coûts. À l'issue de ce délai de 24 heures, vous ne pourrez pas modifier le paramétrage pendant 7 jours. À l'issue de cette période de 7 jours, vous pourrez désactiver la répartition des coûts.

# Intégrer le VPC IPAM à l'infrastructure Infoblox

L'intégration entre Amazon VPC IPAM et Infoblox connecte votre gestionnaire d'adresses IP AWS VPC (IPAM) à Infoblox, ce qui vous permet de AWS gérer les adresses IP via vos flux de travail Infoblox existants tout en bénéficiant de fonctionnalités cloud natives. AWS

Cette intégration permet de relever un défi courant dans les entreprises : éviter la duplication des systèmes de gestion IP. Au lieu d'apprendre de nouveaux outils et de gérer des processus distincts pour les réseaux locaux AWS et pour les réseaux locaux, vous pouvez désigner Infoblox comme autorité de gestion pour les étendues IPAM des VPC et continuer à utiliser votre interface Infoblox habituelle pour toutes les opérations relatives aux adresses IP.

## Vue d'ensemble du processus d'intégration

Les étapes suivantes fournissent une vue d'ensemble du processus d'intégration complet :

1. Configurer l'étendue IPAM (décrite dans ce document) : l'administrateur délégué IPAM d'Amazon VPC crée une nouvelle étendue ou modifie une étendue existante pour utiliser Infoblox comme autorité externe.
2. Configurer Infoblox (décrit en dehors de ce document) : voir. [Étapes suivantes](#)
3. Créer un pool de haut niveau : l'administrateur délégué IPAM d'Amazon VPC crée un pool dans le périmètre lié à Infoblox. Le pool démarre sans qu'aucun CIDR ne soit attribué.
4. Fournir un CIDR auprès d'une autorité externe : l'administrateur délégué Amazon VPC IPAM fournit un CIDR pour le pool. Vous pouvez demander n'importe quel CIDR disponible (Infoblox choisit parmi la plage autorisée) ou demander un CIDR spécifique (Infoblox accepte ou rejette en fonction de la disponibilité). L'IPAM se coordonne automatiquement avec Infoblox pour obtenir et fournir le CIDR approuvé.
5. Poursuivez les opérations IPAM standard : créez des pools enfants et VPCs à partir du CIDR alloué à l'aide des procédures IPAM standard d'Amazon VPC.

## Quand utiliser cette intégration

Utilisez cette intégration si vous utilisez ou prévoyez d'utiliser Infoblox pour la gestion du réseau sur site et que vous souhaitez étendre vos pratiques de gestion IP existantes AWS sans avoir à gérer des systèmes distincts.

## Conditions préalables

Avant de configurer cette intégration, assurez-vous d'avoir :

- Niveau avancé VPC IPAM : activé dans votre compte AWS Pour plus d'informations, consultez [VPC IPAM Advanced Tier](#).
- Autorisations IAM requises : répertoriées ci-dessous
- Identifiant de ressource Infoblox : fourni par votre administrateur Infoblox

## Rôle IAM pour Infoblox

Créez un rôle IAM que le directeur d'Infoblox devra assumer, ou utilisez un rôle existant. Le rôle a besoin des autorisations suivantes :

- `ec2:DescribeIpamPools`
- `ec2:DescribeIpams`
- `ec2:DescribeIpamScopes`
- `ec2:GetIpamPoolAllocations`
- `ec2:GetIpamPoolCidrs`
- `ec2:GetIpamResourceCidrs`

Pour savoir comment ajouter ces autorisations à un rôle ou à une politique IAM, consultez la section [Ajouter et supprimer des autorisations d'identité IAM](#) dans le guide de l'utilisateur IAM.

 Note

Infoblox peut avoir besoin d'autorisations pour la découverte d'un VPC IPAM en plus de ces autorisations requises pour activer cette intégration.

## Configurer l'intégration d'Infoblox dans le VPC IPAM

Vous pouvez activer l'intégration d'Infoblox lorsque vous créez ou modifiez des étendues dans la console VPC AWS IPAM ou AWS CLI

**⚠️ Important**

L'intégration d'Infoblox n'est disponible que pour les étendues privées, et non pour les étendues publiques.

## Création d'un nouveau scope grâce à l'intégration d'Infoblox

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez IPAM, puis Scopes.
3. Choisissez Create scope (Créer une portée).
4. Pour les paramètres de portée, procédez comme suit :
  - L'identifiant IPAM est automatiquement renseigné.
  - (Facultatif) Dans le champ Name tag, entrez le nom de l'étendue.
  - (Facultatif) Dans Description, entrez une description de l'étendue.
5. Pour Scope Authority, choisissez Infoblox IPAM.
6. Pour l'identifiant de ressource Infoblox, entrez l'identifiant de ressource Infoblox au format.  
`<version>.identity.account.<entity_realm>.<entity_id>`
7. Vérifiez que vous disposez des autorisations IAM requises, comme indiqué dans la zone d'information.
8. Choisissez Create scope (Créer une portée).

La AWS CLI commande correspondante est [create-ipam-scope](#).

## Modification des étendues existantes

Pour modifier l'autorité d'étendue d'Amazon VPC IPAM à Infoblox IPAM pour une étendue existante, modifiez les paramètres de portée et suivez les mêmes étapes de configuration que dans la procédure précédente.

La AWS CLI commande correspondante est [modify-ipam-scope](#).

## Étapes suivantes

Ceci complète la configuration IPAM d'Amazon VPC nécessaire à l'intégration. Après avoir configuré l'autorité de portée, vous pouvez créer un pool IPAM de niveau supérieur au sein de l'étendue. Pour de plus amples informations, veuillez consulter [Création d'un groupe IPv4 de niveau supérieur](#).

L'intégration nécessite également la configuration d'un pool source Infoblox, la vérification de l'état des tâches de découverte, la configuration de l'étendue privée à gérer par Infoblox, l'activation de la gestion d'Infoblox pour Amazon VPC IPAM et la création de pools soit à partir de l'intégration Infoblox, soit directement à partir du portail Infoblox.

Pour plus d'informations sur le côté Infoblox de l'intégration, consultez le guide de l'utilisateur de l'intégration AWS IPAM dans la documentation d'Infoblox.

## Activer le provisionnement de CIDR GUA IPv6 privés

Si vous souhaitez que vos réseaux privés prennent en charge le protocole IPv6 et que vous n'avez pas l'intention d'acheminer le trafic de ces adresses vers Internet, vous pouvez fournir une plage ULA ou GUA IPv6 privée à un groupe IPAM dans un périmètre privé.

Pour plus de détails sur l'adressage IPv6 privé, voir [Adresses IPv6 privées](#) dans le Guide de l'utilisateur Amazon VPC.

Il existe deux types d'adresses IPv6 privées :

- Plages IPv6 ULA : adresses IPv6 telles que définies dans [RFC4193](#). Ces plages d'adresses commencent toujours par « fc » ou « fd », ce qui les rend facilement identifiables. L'espace IPv6 ULA valide est tout ce qui est inférieur à fd00::/8 qui ne chevauche pas la plage réservée Amazon fd00::/16.
- Plages IPv6 GUA : adresses IPv6 telles que définies dans [RFC3587](#). L'option d'utilisation des plages IPv6 GUA en tant qu'adresses IPv6 privées est désactivée par défaut et doit être activée avant de pouvoir l'utiliser.

Pour utiliser une plage d'adresses ULA IPv6, vous choisissez l'option IPv6 lorsque vous attribuez un CIDR à un groupe IPAM et que vous entrez la plage d'adresses ULA IPv6. Toutefois, pour utiliser vos propres plages GUA IPv6 comme adresses IPv6 privées, vous devez d'abord suivre les étapes décrites dans cette section. L'option est désactivée par défaut.

### Note

- Lorsque vous utilisez des plages IPv6 GUA privées, nous vous demandons d'utiliser des plages IPv6 GUA dont vous êtes propriétaire.
- IPAM détecte les ressources avec des adresses IPv6 ULA et GUA et surveille les groupes pour détecter tout chevauchement d'espaces d'adressage IPv6 ULA et GUA.
- Si vous souhaitez vous connecter à Internet à partir d'une ressource dotée d'une adresse IPv6 privée, vous pouvez le faire, mais vous devez pour cela acheminer le trafic via une ressource d'un autre sous-réseau doté d'une adresse IPv6 publique.
- Si une plage IPv6 GUA privée est attribuée à un VPC, vous ne pouvez pas utiliser l'espace IPv6 GUA public qui chevauche l'espace IPv6 GUA privé du même VPC.
- La communication entre les ressources dotées de plages d'adresses IPv6 ULA et GUA privées est prise en charge (par exemple via Direct Connect, l'appairage de VPC, la passerelle de transit ou les connexions VPN).
- Une plage IPv6 GUA privée ne peut pas être convertie en une plage IPv6 GUA annoncée publiquement.

## AWS Management Console

### Activation du provisionnement de CIDR GUA IPv6 privés

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 votre IPAM et choisissez Actions > Modifier.
4. Sous CIDR GUA IPv6 privés, choisissez Activer le provisionnement de l'espace CIDR GUA dans des groupes IPAM IPv6 privés.
5. Sélectionnez Enregistrer les modifications.

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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 activer le provisionnement de CIDR GUA IPv6 privés :

1. Affichez les IPAM actuels avec [describe-ipams](#)
2. Modifiez l'IPAM avec [modify-ipam](#) et incluez l'option à enable-private-gua.

Une fois que vous avez activé l'option permettant de provisionner des CIDR GUA IPv6 privés, vous pouvez fournir un CIDR GUA IPv6 privé à un groupe. Pour plus d'informations, consultez [Approvisionnement de CIDR à un groupe](#).

## Renforcez l'utilisation d'IPAM pour la création de VPC avec SCPs

### Note

Cette section ne s'applique à vous que si vous avez activé l'intégration d'IPAM à

AWS Organizations Pour de plus amples informations, veuillez consulter [Intégration d'IPAM aux comptes d'une organisation AWS](#).

Cette section décrit comment créer une politique de contrôle des services AWS Organizations qui oblige les membres de votre organisation à utiliser IPAM lorsqu'ils créent un VPC. Les politiques de contrôle des services (SCPs) sont un type de politique d'organisation qui vous permet de gérer les autorisations au sein de votre organisation. Pour plus d'informations, consultez [Politiques de contrôle de service](#) du Guide de l'utilisateur AWS Organizations .

## Appliquer l'IPAM lors de la création VPCs

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

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

1. Suivez les étapes décrites dans la section [Create a service control policy](#) du Guide d'utilisation d'AWS Organizations et saisissez le texte suivant dans l'éditeur JSON :

JSON

```
{
```

```

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

```

- Associez la stratégie à une ou plusieurs unités organisationnelles de votre organisation. Pour plus d'informations, consultez les sections sur [l'attachement](#) et le [détachement de politiques](#) dans le Guide d'utilisation d'AWS Organizations .

## Appliquer un pool IPAM lors de la création VPCs

Suivez les étapes décrites dans cette section pour obliger les membres de votre organisation à utiliser un pool IPAM spécifique lors de la création VPCs.

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

- Suivez les étapes décrites dans la section [Create a service control policy](#) du Guide d'utilisation d'AWS Organizations et saisissez le texte suivant dans l'éditeur JSON :

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. Remplacez la valeur de l'ipam-pool-0123456789abcdefgexemple par l'ID de IPv4 pool auquel vous souhaitez limiter les utilisateurs.
3. Associez la stratégie à une ou plusieurs unités organisationnelles de votre organisation. Pour plus d'informations, consultez les sections sur l'[attachement](#) et le [détachement de politiques](#) dans le Guide d'utilisation d'AWS Organizations .

## Appliquer l'IPAM pour tous sauf pour une liste donnée OUs

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

Pour créer un SCP et appliquer l'IPAM pour tous sauf une liste donnée de OUs

1. Suivez les étapes décrites dans la section [Create a service control policy](#) du Guide d'utilisation d'AWS Organizations et saisissez le texte suivant dans l'éditeur JSON :

JSON

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

```
  } ]  
}
```

2. Supprimez les valeurs d'exemple (commeo-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/) et ajoutez AWS les chemins d'entités Organizations OUs dont vous souhaitez avoir la possibilité (mais pas obligatoire) d'utiliser IPAM. Pour plus d'informations sur le chemin de l'entité, consultez [Understand the AWS Organizations entity path](#) et [aws : PrincipalOrgPaths](#) dans le guide de l'utilisateur IAM.
3. Attachez la politique à la racine de votre organisation. Pour plus d'informations, consultez les sections sur l'[attachement](#) et le [détachement de politiques](#) dans le Guide d'utilisation d'AWS Organizations .

## Exclure les unités organisationnelles d'IPAM

Si votre IPAM est intégré à AWS Organizations, vous pouvez exclure une [unité organisationnelle \(UO\)](#) de la gestion par IPAM. Si vous excluez une UO, l'IPAM ne gérera pas les adresses IP des comptes de cette UO. Cette fonctionnalité vous donne une plus grande flexibilité dans la façon dont vous utilisez IPAM.

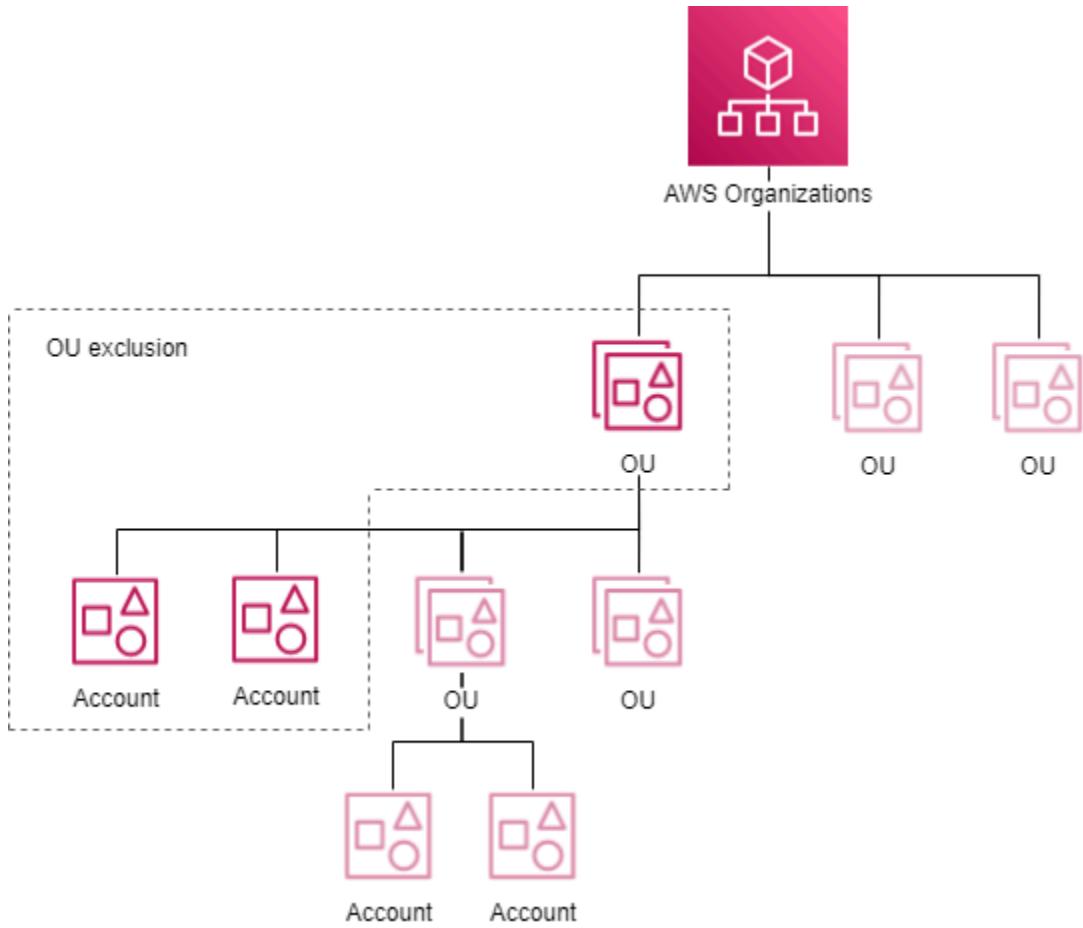
Vous pouvez utiliser les exclusions d'UO comme suit :

- Activer IPAM pour des secteurs spécifiques de votre entreprise : si vous avez plusieurs unités commerciales ou filiales dans les organisations AWS , vous pouvez désormais utiliser IPAM uniquement pour celles qui en ont besoin.
- Séparer vos comptes d'environnement de test (sandbox) : vous pouvez exclure vos comptes d'environnement de test (sandbox) d'IPAM, en vous concentrant uniquement sur les comptes réellement importants pour la gestion de votre IP.

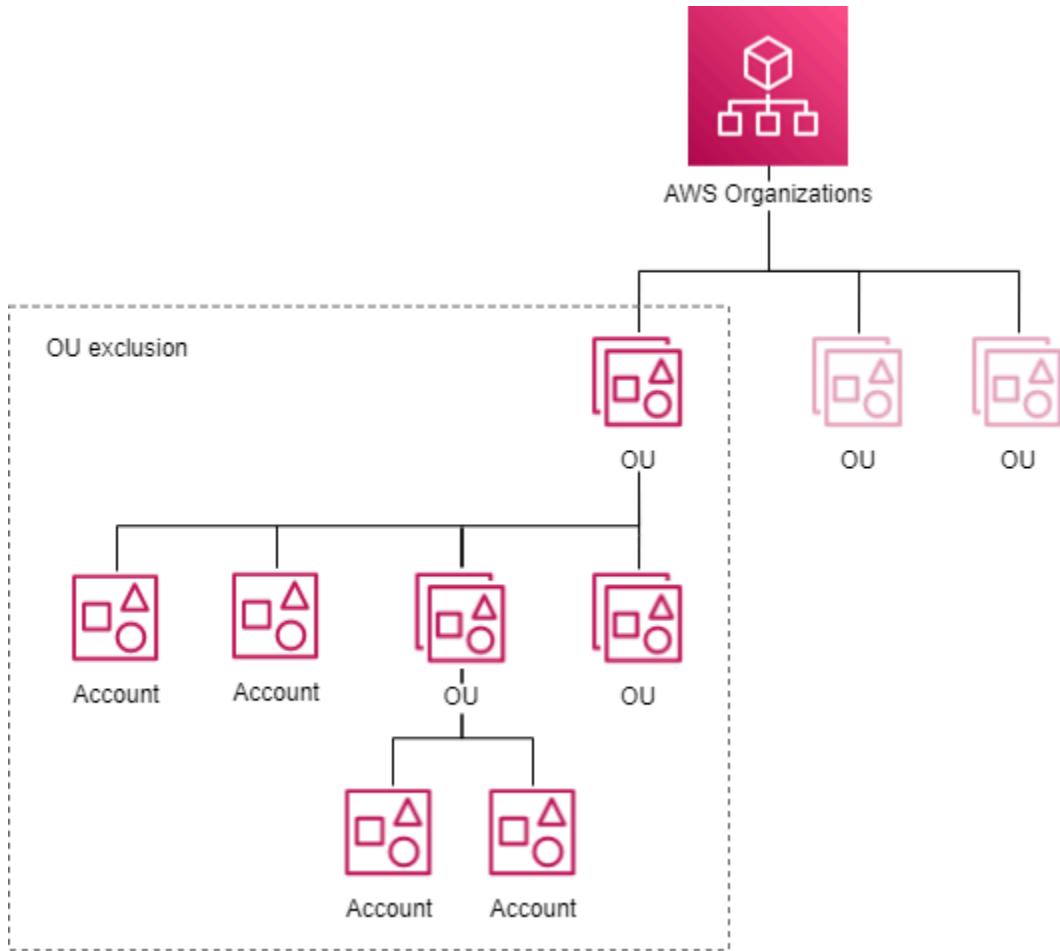
## Comment fonctionnent les exclusions UO

Les diagrammes de cette section illustrent deux cas d'utilisation permettant d'ajouter des exclusions UO dans l'IPAM.

Le premier diagramme montre l'impact de l'ajout d'une exclusion d'unité organisationnelle (UO) sur une UO parent uniquement. Par conséquent, IPAM ne gérera pas les adresses IP des comptes de l'UO parent. IPAM gérera les adresses IP des comptes de l'autre en OUs dehors de l'exclusion.



Le deuxième diagramme montre l'impact de l'ajout d'une exclusion d'unité organisationnelle (OU) sur une OU parent et sur tous les enfants OUs. Par conséquent, IPAM ne gérera pas les adresses IP des comptes de l'unité d'organisation parent ou des comptes d'un enfant OUs. L'IPAM gérera les adresses IP des comptes situés en OUs dehors de l'exclusion.



## Ajouter ou supprimer des exclusions d'OU

Suivez les étapes de cette section pour ajouter ou supprimer des exclusions d'OU.

### i Note

- Le compte administrateur IPAM délégué n'est pas exclu même s'il se trouve au sein d'une OU exclue.
- Votre IPAM doit être intégré AWS Organizations pour ajouter une exclusion d'unité d'organisation. L'Organisation doit y OUs participer.
- Vous devez être l'administrateur IPAM délégué pour afficher, ajouter ou supprimer des exclusions d'OU.
- IPAM met du temps à découvrir les unités organisationnelles récemment créées.

- Il existe un quota par défaut pour le nombre d'exclusions que vous pouvez ajouter par découverte de ressources. Pour plus d'informations, consultez la section Exclusions d'unités organisationnelles par découverte de ressources dans [Quotas pour votre IPAM](#).
- Si vous [partagez une découverte de ressources avec un autre compte](#), ce compte peut voir les exclusions de l'unité organisationnelle qui y figurent, qui contiennent des informations telles que l'identifiant de l'organisation, l'identifiant racine et l'unité organisationnelle IDs de l'organisation du propriétaire de la découverte des ressources.

## AWS Management Console

### Ajout ou suppression des exclusions d'UO

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans le volet de navigation, sélectionnez Découvertes de ressources.
3. Sélectionnez votre découverte de ressources par défaut.
4. Choisissez Modifier.
5. Sous Exclusions des unités organisationnelles, procédez comme suit :
  - Pour ajouter une exclusion d'UO :
    - Si vous souhaitez exclure l'UO et tous ses enfants OUs :
      - Trouvez l'UO dans le tableau et cochez la case. Tous les enfants OUs sont automatiquement sélectionnés.
    - Si vous souhaitez exclure uniquement les comptes de l'UO parent :
      - Trouvez l'UO dans le tableau et cochez la case. Tous les enfants OUs sont automatiquement sélectionnés. Désélectionnez tous les enfants OUs.
    - Vous pouvez également utiliser la colonne Actions pour sélectionner uniquement une unité d'organisation parent ou un parent et un enfant OUs :
      - Sélectionnez tous les enfants OUs : incluez n'importe quel enfant OUs dans l'exclusion. À la suite du choix d'une UO, celle-ci est ajoutée à l'écran. Chaque UO contient l'ID et le [chemin d'entité](#) de l'exclusion de l'UO.
      - Sélectionner uniquement cette UO : incluez uniquement cette UO dans l'exclusion. À la suite du choix d'une UO, celle-ci est ajoutée à l'écran. Chaque UO contient l'ID et le [chemin d'entité](#) de l'exclusion de l'UO.

- Copier le chemin de l'entité UO : copiez le chemin de l'entité d'organisation à utiliser selon les besoins.
- Si vous connaissez déjà le chemin de l'entité AWS Organizations ou si vous souhaitez le créer :
  - Choisissez Exclusion de l'UO d'entrée et entrez le [chemin d'entité](#) de l'exclusion de l'UO. Créez le chemin pour la ou les UO à l'aide d' AWS Organizations IDs séparées par un/. Incluez tous les enfants OUs en terminant le chemin par/\*.
  - Exemple 1
    - Chemin d'accès à une UO enfant : o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscffff/ou-jkl0-awsdddd/
    - Dans cet exemple, o-a1b2c3d4e5 est l'ID de l'organisation, r-f6g7h8i9j0example est l'ID racine, ou-ghi0-awscffff est l'ID d'une UO et ou-jkl0-awsdddd est l'ID d'une UO enfant.
    - IPAM ne gérera pas les adresses IP des comptes de l'UO enfant.
  - Exemple 2
    - Parcours où tous les enfants OUs participeront à l'exclusion : o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscffff/\*
    - Dans cet exemple, IPAM ne gérera pas les adresses IP des comptes de l'unité d'organisation (ou-ghi0-awscffff) ni des comptes des comptes des enfants de l'unité d'organisation. OUs
- Pour supprimer une exclusion d'UO :
  - Choisissez le X à côté d'une UO déjà ajoutée. L'ID d'unité d'organisation situé /\* après indique qu'il s'agit d'une unité d'organisation parent et que OUs les enfants font partie de l'exclusion de l'unité d'organisation.

## 6. Sélectionnez Enregistrer les modifications.

### Command line

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

1. Consultez les détails de la découverte des ressources pour obtenir l'ID de la découverte des ressources par défaut pour l'étape suivante avec [describe-ipam-resource-discoveries](#).

Entrée :

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

Sortie :

```
{  
  "IpamResourceDiscoveries": [  
    {  
      "OwnerId": "111122223333",  
      "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",  
      "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-  
      resource-discovery/ipam-res-disco-1234567890abcdef0",  
      "IpamResourceDiscoveryRegion": "us-east-1",  
      "OperatingRegions": [  
        {  
          "RegionName": "us-east-1"  
        },  
        {  
          "RegionName": "us-west-1"  
        },  
        {  
          "RegionName": "us-west-2"  
        }  
      ],  
    }  
  ]  
}
```

```
        "IsDefault": true,  
  
        "State": "modify-complete",  
  
        "Tags": []  
  
    }  
  
]  
  
}
```

2. Ajoutez ou supprimez une exclusion d'unité organisationnelle dans une découverte de ressources avec [modify-ipam-resource-discovery](#) les `--remove-organizational-unit-exclusions` options `--add-organizational-unit-exclusions` ou. Vous devez saisir le chemin d'une entité AWS Organizations. Créez le chemin pour la ou les UO à l'aide d' AWS Organizations IDs séparées par un/. Incluez tous les enfants OUs en terminant le chemin par/\*. Vous ne pouvez pas inclure le même chemin d'entité plusieurs fois dans les paramètres d'ajout ou de suppression.

- Exemple 1

- Chemin d'accès à une UO enfant : `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscccc/ou-jkl0-awsdddd/`
- Dans cet exemple, `o-a1b2c3d4e5` est l'ID de l'organisation, `r-f6g7h8i9j0example` est l'ID racine, `ou-ghi0-awscccc` est l'ID d'une UO et `ou-jkl0-awsdddd` est l'ID d'une UO enfant.
- IPAM ne générera pas les adresses IP des comptes de l'UO enfant.

- Exemple 2

- Parcours où tous les enfants OUs participeront à l'exclusion : `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscccc/*`
- Dans cet exemple, IPAM ne générera pas les adresses IP des comptes de l'unité d'organisation (`ou-ghi0-awscccc`) ni des comptes des comptes des enfants de l'unité d'organisation. OUs

### Note

L'ensemble d'exclusions qui en résulte ne doit pas générer de « chevauchement », c'est-à-dire que deux exclusions d'UO ou plus ne doivent pas exclure la même UO. Exemple de chemins d'entités ne se chevauchant pas :

- Chemin 1 = « o-1/r-1/ou-1/ »
- Chemin 2 = « o-1/r-1/ou-1/ou-2/ »

Ces chemins ne se chevauchent pas du fait que le chemin 1 exclut uniquement les comptes présents sous « ou-1 » et que le chemin 2 exclut uniquement les comptes présents sous « ou-2 ».

Exemple de chemins d'entités se chevauchant :

- Chemin 1 = « o-1/r-1/ou-1/\* »
- Chemin 2 = « o-1/r-1/ou-1/ou-2/ »

Ces chemins se chevauchent du fait que le chemin 1 représente à la fois « o-1/r-1/ou-1/ » et « o-1/r-1/ou-1/ou-2/ », et que « o-1/r-1/ou-1/ou-2/ » est en situation de chevauchement avec le chemin 2.

Entrée :

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

Sortie :

```
{
  "IpamResourceDiscovery": {
```

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

## Modifier un niveau IPAM

L'IPAM propose deux niveaux : le niveau gratuit et le niveau avancé. Le passage au niveau avancé du Gestionnaire d'adresses IP d'Amazon VPC permet un contrôle plus granulaire de la gestion des adresses IP. Cela peut être bénéfique à mesure que la complexité de votre réseau augmente, ce qui vous permet de mieux optimiser et gérer votre espace d'adresses IP. Pour plus d'informations sur les fonctionnalités disponibles dans chaque niveau gratuit et les coûts associés au niveau avancé, consultez l'onglet IPAM sur la [page de tarification d'Amazon VPC](#).

### Note

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 <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans le panneau de navigation, sélectionnez IPAMs.
3. Dans le panneau de contenu, sélectionnez votre IPAM.
4. Sélectionnez Actions > Edit (Modifier).

### Note

Si vous utilisez le niveau gratuit, vous verrez s'afficher la mention Votre nombre total d'adresses IP actives dans l'IPAM est estimé à....

Nombre total d'adresses IP actives dans votre IPAM qui vous seraient facturées si vous passiez du niveau gratuit au niveau avancé. Une adresse IP active est définie comme une adresse IP ou un préfixe associé à une interface réseau élastique (ENI) attachée à une ressource telle qu'une EC2 instance.

- Cette métrique est uniquement disponible pour les clients de l'offre gratuite.
- Si votre IPAM est [intégré à AWS Organizations](#), le nombre d'adresses IP actives couvre tous les comptes de l'organisation.
- Vous ne pouvez pas consulter la répartition du nombre d'adresses IP actives par type d'IP (public/private) or class (IPv4/IPv6).
- L'IPAM ne compte IPs que s'il est ENIs détenu par des comptes surveillés. Le décompte peut être inexact pour les sous-réseaux partagés. Les adresses IP sont exclues si le propriétaire du sous-réseau ou le propriétaire de l'ENI n'est pas couvert par IPAM.

5. Choisissez le niveau IPAM que vous souhaitez utiliser pour l'IPAM.
6. Sélectionnez Enregistrer les modifications.

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes de l'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 afficher et modifier un niveau IPAM :

1. Afficher le cours IPAMs : [describe-ipams](#)
2. Modifiez le niveau IPAM : [modify-ipam](#)
3. Afficher votre mise à jour IPAMs : [describe-ipams](#)

## Modifiez 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.

L'ajout d'une région d'exploitation à un IPAM vous permet de gérer l'espace d'adresses IP dans plusieurs régions AWS. Cela peut améliorer l'utilisation des adresses IP, permettre la segmentation régionale et prendre en charge une infrastructure distribuée géographiquement. L'extension du périmètre régional de l'IPAM offre une flexibilité et un contrôle accrus sur la gestion globale de votre adresse IP.

### 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. Sélectionnez Enregistrer les modifications.

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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](#)

## 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, sélectionnez 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. Effectuez l'une des actions suivantes :
  - Si vous fournissez un CIDR à un groupe dans le périmètre public, saisissez le masque de réseau.
  - Si vous fournissez un CIDR à un groupe IPv4 dans le périmètre privé, saisissez le CIDR.
  - Si vous fournissez un CIDR à un groupe IPv6 dans le périmètre privé, notez ce qui suit :
    - Pour plus de détails sur l'adressage IPv6 privé, voir [Adresses IPv6 privées](#) dans le Guide de l'utilisateur Amazon VPC.
    - Pour utiliser une plage ULA IPv6 privée, sous CIDR à provisionner, choisissez Ajouter une adresse CIDR ULA par masque réseau puis choisissez une taille de masque réseau ou choisissez Input private IPv6 CIDR et entrez une plage ULA. Les plages valides pour les IPv6 ULA privées sont comprises entre /9 et /60, et commencent par fd80::/9.
    - Pour utiliser une plage GUA IPv6 privée, vous devez d'abord avoir activé l'option sur votre IPAM (voir [Activer le provisionnement de CIDR GUA IPv6 privés](#)). Une fois que vous avez activé les CIDR GUA IPv6 privés, entrez un GUA IPv6 dans Input private IPv6 CIDR.

 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. Choisissez Provisionner.
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 sur les commandes 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 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](#)

## Déplacez des CIDR VPC entre les portées

Le déplacement des CIDR entre les périmètres vous permet d'optimiser l'allocation des adresses IP, de les organiser par région, de séparer les préoccupations, de renforcer la conformité et de vous adapter aux changements d'infrastructure. Cette flexibilité permet de gérer efficacement votre espace d'adresses IP à mesure que vos charges de travail évoluent.

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](#)

## Définir une stratégie IPv4 d'allocation publique avec les politiques de l'IPAM

Une politique IPAM est un ensemble de règles qui définissent la manière dont les IPv4 adresses publiques des pools IPAM sont allouées aux AWS ressources. Chaque règle associe un AWS service à des pools IPAM que le service utilisera pour obtenir des adresses IP. Une même politique peut comporter plusieurs règles et être appliquée à plusieurs AWS régions. Si le pool IPAM est à court d'adresses, les services se rabattent sur les adresses IP fournies par Amazon. Une politique peut être appliquée à un AWS compte individuel ou à une entité au sein d' AWS Organizations. Si vous [apportez votre propre adresse IP \(BYOIP\)](#), cela permet de réduire vos dépenses AWS publiques IPv4 .

## Quand utiliser les politiques IPAM

Utilisez les politiques IPAM pour :

- Réduisez les IPv4 coûts publics en utilisant des adresses BYOIP
- Contrôlez de manière centralisée les pools IP utilisés par vos AWS ressources
- Garantissez une allocation IP cohérente au sein de votre organisation

## Fonctionnement

Lorsque vous créez une AWS ressource qui a besoin d'une adresse IP publique dans un compte avec des politiques IPAM appliquées :

- L'IPAM vérifie l'ordre de vos règles de politique.
- Si une règle correspond au type de ressource, IPAM alloue une adresse IP à partir du pool spécifié.
- Si le pool est vide et que le débordement est activé, Amazon fournit une adresse IP.
- Si aucune règle ne correspond, le comportement par défaut s'applique.

## Services et ressources pris en charge

Vous pouvez créer des politiques IPAM pour définir comment les IPv4 adresses publiques des pools IPAM sont allouées aux AWS services et ressources suivants :

- Adresses IP élastiques (EIPs)
- Passerelles NAT régionales

### Important

En EIPs effet, si vous choisissez un pool IPAM spécifique lorsque vous leur attribuez une IPv4 adresse publique, cela remplacera la politique IPAM.

## Conditions préalables

- Un [IPAM](#) dans le compte d'administrateur délégué avec le [niveau avancé activé](#)
- Un [pool IPAM public](#) avec des adresses IPv4
- [Autorisations IAM](#) pour l'IPAM et les opérations EC2

## Terminologie

### Politique IPAM

Une politique IPAM est un ensemble de règles qui définissent la manière dont les IPv4 adresses publiques des pools IPAM sont allouées aux AWS ressources. Chaque règle associe un AWS service à des pools IPAM que le service utilisera pour obtenir des adresses IP. Une même politique peut comporter plusieurs règles et être appliquée à plusieurs AWS régions. Si le pool IPAM est à court d'adresses, les services se rabattent sur les adresses IP fournies par Amazon. Une politique peut être appliquée à un AWS compte individuel ou à une entité au sein d' AWS Organizations. Une politique peut être appliquée à un AWS compte individuel ou à une entité au sein d' AWS Organizations.

### Règles d'allocation

Configurations facultatives au sein d'une politique IPAM qui mappent AWS des types de ressources à des pools IPAM spécifiques. Si aucune règle n'est définie, les types de ressources utilisent par défaut les adresses IP fournies par Amazon.

### Cible

AWS Compte individuel ou entité au sein d'une AWS organisation auquel une politique IPAM peut être appliquée.

## Étape 1 : créer une politique IPAM

### À l'aide de AWS la console :

Procédez comme suit pour créer une politique IPAM à l'aide de la AWS console :

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans le volet de navigation de gauche, choisissez Politiques.
3. Choisissez Créer une politique.
4. Entrez un nom pour votre police (facultatif).
5. Sélectionnez l'IPAM à associer à cette politique.
6. (Facultatif) Ajoutez des balises.
7. Choisissez Create Policy (Créer une politique).

### À l'aide de la AWS CLI :

Utilisez la commande [create-ipam-policy](#).

## Étape 2 : Ajouter des règles d'allocation

Après avoir créé la politique, vous devez ajouter des règles d'allocation qui définissent le mode d'allocation des adresses IP :

À l'aide de AWS la console :

Procédez comme suit pour ajouter des règles d'allocation à l'aide de la AWS console :

1. Dans le volet de navigation de gauche, choisissez Politiques.
2. Choisissez la politique que vous avez créée à l'étape précédente.
3. Sur la page des détails de votre politique, choisissez l'onglet Règles d'allocation.
4. Choisissez Créer des règles de répartition.
5. Configurez la configuration du service :
  - Lieu : Choisissez la AWS région (us-east-1) ou la zone locale dans laquelle vous souhaitez que cette politique s'applique.
  - Type de ressource : sélectionnez le type de AWS service ou de ressource pour cette politique (adresses IP élastiques).
6. Configuration des règles :
  - Pool IPAM : sélectionnez le pool IPAM qui fournira les adresses IP.
  - Vérifiez les détails du pool (paramètres régionaux, source IP publique, espace disponible et plages d'adresses CIDR disponibles).
7. (Facultatif) Choisissez Ajouter une nouvelle règle pour créer des règles supplémentaires.
8. Choisissez Créer une règle d'allocation.

À l'aide de la AWS CLI :

Utilisez la commande [modify-ipam-policy-allocation-rules](#).

## Étape 3 : activer la politique

Spécifiez les comptes qui doivent utiliser cette politique.

À l'aide de AWS la console :

Procédez comme suit pour activer la politique à l'aide de la AWS console :

1. Sur la page des détails de votre politique, choisissez l'onglet Cibles.
2. Choisissez Gérer les objectifs de politique.
3. Effectuez l'une des actions suivantes :
  - Pour utiliser un seul compte (IPAM n'est pas intégré à AWS Organizations), choisissez Enable pour votre compte.
  - Pour l'intégration d'IPAM à AWS Organizations (lorsque vous êtes l'administrateur délégué) :
    - Dans la section Structure organisationnelle, sélectionnez les comptes ou les unités organisationnelles auxquels vous souhaitez appliquer cette politique.
    - Cochez la case Activé pour chaque cible.
    - Choisissez Save Changes (Enregistrer les modifications).
    - Important : l'activation de cette stratégie remplacera toutes les politiques IPAM actives sur les comptes ou unités organisationnelles sélectionnés.

À l'aide de la AWS CLI :

Utilisez la [enable-ipam-policy](#) commande en fonction de votre configuration :

Pour l'utilisation d'un seul compte (IPAM non intégré à AWS Organizations) :

```
aws ec2 enable-ipam-policy \
--ipam-policy-id ipam-policy-12345678
```

Pour l'intégration d'IPAM à AWS Organizations (lorsque vous êtes l'administrateur délégué) :

```
aws ec2 enable-ipam-policy \
--ipam-policy-id ipam-policy-12345678 \
--organization-target-id 123456789012
```

**⚠️ Important**

L'activation de cette stratégie remplacera toutes les politiques IPAM actives sur les comptes ou unités organisationnelles sélectionnés.

## Étape 4 : (Facultatif) Application à l'échelle de l'organisation

Si vous avez activé cette politique IPAM sur une entité AWS Organizations, utilisez des politiques déclaratives pour ajouter une gestion et une gouvernance centralisées à vos politiques IPAM.

Ce que cela ajoute :

L'application de la loi à l'échelle de l'organisation offre les avantages suivants :

- Gestion centralisée des politiques sur tous les comptes de l'organisation
- Application automatique sans configuration par compte
- Contrôles de gouvernance pour empêcher les changements de politique au niveau du compte

Prérequis :

Avant de mettre en place une mise en œuvre à l'échelle de l'organisation, assurez-vous de disposer des éléments suivants :

- AWS Organizations dont toutes les fonctionnalités sont activées
- IPAM dans le compte de gestion de l'organisation ou le compte administrateur délégué
- Autorisations appropriées pour les Organizations et l'IPAM

Pour obtenir des instructions détaillées sur la configuration de l'application des politiques déclaratives à l'échelle de l'organisation, voir [Getting started with declarative policies dans le Guide de l'utilisateur](#) des AWS Organizations.

## Étape 5 : Testez votre politique

Activez une nouvelle ressource du type que vous avez configuré (comme un EIP) dans l'un des comptes cibles. La ressource utilisera automatiquement une adresse IP de votre pool IPAM.

### Important

En EIPs effet, si vous choisissez un pool IPAM spécifique lorsque vous leur attribuez une IPv4 adresse publique, cela remplacera la politique IPAM.

## Étape 6 : Surveiller l'utilisation

Vérifiez votre [pool IPAM](#) dans la console pour voir les adresses IP allouées à vos ressources.

## Libération d'une allocation

Si vous envisagez de supprimer un groupe, vous devrez peut-être libérer une allocation de groupe. Une allocation est une affectation CIDR d'un groupe IPAM vers un autre groupe de ressources ou IPAM.

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 [ReleaselpamPoolAllocation](#).
- Pour libérer une allocation dans une étendue privée, vous devez ignorer ou supprimer le CIDR de la ressource. Pour plus d'informations, consultez [Modifiez l'état de contrôle des CIDR VPC](#). Après un certain temps, Amazon VPC IPAM libérera automatiquement l'allocation en votre nom.

### 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 IPv4 CIDR public à IPAM en utilisant uniquement la CLI AWS](#) ou Cleanup (Nettoyage) dans [Apportez votre propre CIDR IPv6 sur IPAM en utilisant uniquement la AWSCLI](#). 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. Si vous utilisez IPAM au niveau avancé, il faut quelques minutes pour que le CIDR devienne disponible pour les allocations futures. Si vous utilisez IPAM dans le cadre de l'offre gratuite, il faudra jusqu'à 48 heures 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.
  - sous-réseau : allocation de sous-réseau.
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 sur les commandes 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 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 [Allouer des CIDR à partir d'un groupe IPAM](#). Pour supprimer le groupe après avoir libéré des allocations, vous devez d'abord [Pour désapprovisionner un CIDR de groupe](#).

## 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 plus d'informations, consultez [Intégration d'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 avec AWS Organizations utilisant RAM. Pour de plus amples informations, veuillez consulter [Activer le partage des ressources dans AWS Organizations](#) dans le Guide de l'utilisateur RAM AWS.
- 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.

- Bien que vous puissiez partager des groupes IPAM avec n'importe quel compte AWS en dehors d'une organisation AWS, IPAM ne surveillera les adresses IP des comptes en dehors de l'organisation que si le propriétaire du compte a suivi le processus de partage de la découverte des ressources avec l'administrateur délégué d'IPAM, comme décrit dans la section [Intégration d'IPAM à des comptes extérieurs à votre organisation](#).

## 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, sélectionnez 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 procédez au partage, et sélectionnez Create (Créer).

## Command line

La ou les commandes de cette section renvoient vers la documentation de référence sur les commandes de l'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 la section [Create a VPC](#) dans le Guide d'utilisation d'Amazon VPC.

## 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 de la découverte de ressources. Cela permet à IPAM de maintenir un inventaire à jour de l'utilisation des adresses IP dans l'ensemble de vos charges de travail, facilitant ainsi la gestion et la planification des adresses IP.

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.

Notez que cette section regroupe des procédures qui sont toutes liées à l'utilisation des découvertes de ressources.

## Table des matières

- [Création d'une découverte de ressources à intégrer à un autre IPAM](#)
- [Afficher les détails d'une découverte de ressources](#)
- [Partage d'une découverte de ressources avec un autre compte AWS](#)
- [Associer une découverte de ressources à un IPAM](#)
- [Dissocier une découverte de ressources](#)
- [Supprimer une découverte de ressources](#)

## Création d'une découverte de ressources à intégrer à un autre IPAM

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 Créez 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 sur les commandes 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

L'affichage des détails d'une découverte de ressources dans IPAM AWS peut fournir des informations précieuses, telles que :

- Identifier les ressources AWS spécifiques qui ont été importées ainsi que leurs allocations d'adresses IP associées.
- Surveillance de l'état et de la progression du processus de découverte de ressources.
- Résolution des problèmes ou des divergences entre IPAM et les ressources découvertes.
- Analyse de l'utilisation des adresses IP et des tendances.

Ces informations peuvent vous aider à optimiser la gestion de vos adresses IP, et à garantir l'alignement entre IPAM et vos déploiements de ressources réels.

## 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.
  - Allocation de l'adresse IP : pourcentage d'espace d'adressage IP utilisé. Afin de convertir la décimale en pourcentage, multipliez-la par 100. Remarques :
    - 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.
- Crée 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 sur les commandes de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Affichage des détails d'une découverte de ressources : [describe-ipam-resource-discovery](#)

## Partage d'une découverte de ressources avec un autre compte AWS

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
- En cas de partage d'une découverte de ressources avec un autre compte, ce compte peut voir les [exclusions d'UO](#), qui contiennent des informations telles que l'ID de l'organisation, l'ID racine et les ID des UO de l'organisation du propriétaire de la découverte 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.

#### 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 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 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 plus d'informations, consultez [Associer une découverte de ressources à un IPAM](#).

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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 Associer.

### Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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

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

## Command line

Les commandes de cette section renvoient vers la documentation de référence sur les commandes 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 sur les commandes 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](#)

# Suivi de l'utilisation des adresses IP dans IPAM

Le Gestionnaire d'adresses IP d'Amazon VPC propose des fonctionnalités de suivi de l'utilisation des adresses IP qui peuvent profiter à tous ceux qui gèrent des environnements réseau complexes. IPAM fournit une visibilité sur l'allocation, l'utilisation et les tendances de consommation des adresses IP dans l'ensemble d'AWS. Cela vous permet d'identifier les adresses IP inutilisées ou utilisées de manière inefficace, d'optimiser l'espace d'adressage et de prévenir l'épuisement potentiel des adresses IP.

IPAM suit l'utilisation des adresses IP au niveau du CIDR, du périmètre et d'IPAM, en fournissant des rapports et des analytiques détaillés. Cela est utile pour les déploiements à grande échelle, les configurations multicomptes et l'évolution des exigences du réseau.

En tirant parti du suivi de l'utilisation d'IPAM, vous pouvez prendre des décisions éclairées, améliorer la gestion des adresses IP et garantir une utilisation efficace des ressources IP.

## Note

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.

## 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

Le tableau de bord IPAM du Gestionnaire d'adresses IP d'Amazon VPC vous permet de surveiller l'utilisation du CIDR pour plusieurs scénarios clés :

- Identifier l'espace d'adresse IP inutilisé ou sous-utilisé : le tableau de bord fournit une visibilité sur l'utilisation des CIDR, ce qui vous permet d'identifier les CIDR ayant une capacité disponible qui peut être récupérée ou réallouée.
- Optimiser la gestion des adresses IP : en suivant de près l'utilisation du CIDR, vous pouvez prendre des décisions éclairées concernant l'extension, la contraction ou la réattribution des blocs d'adresses IP afin de répondre à l'évolution des exigences commerciales et en matière d'infrastructure.
- Prévenir l'épuisement des adresses IP : la surveillance de l'utilisation du CIDR vous aide à anticiper le moment où vous pourriez avoir besoin d'acquérir de l'espace d'adresse IP supplémentaire, ce qui vous permet de planifier de manière proactive et d'éviter les interruptions de service dues à l'épuisement des adresses IP.
- Garantir la conformité et la gouvernance : le tableau de bord IPAM peut vous aider à démontrer les modèles d'utilisation des adresses IP afin de répondre aux exigences réglementaires ou aux politiques internes en matière de gestion des adresses IP.
- Résoudre les problèmes de réseau : des données d'utilisation détaillées du CIDR peuvent aider à identifier les causes profondes des problèmes de connectivité réseau ou des conflits de ressources.

En surveillant de près l'utilisation du CIDR via le tableau de bord IPAM, vous pouvez améliorer l'efficacité, la résilience et la conformité de la gestion de vos adresses IP dans AWS.

## 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, consultez [Métriques d'utilisation des ressources IPAM](#).
- 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, consultez [Métriques d'utilisation des ressources IPAM](#).
- 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

La vue Ressources du Gestionnaire d'adresses IP d'Amazon VPC fournit une vue d'ensemble centralisée de l'utilisation des adresses IP dans l'ensemble de vos ressources AWS. Cela vous permet d'identifier rapidement les ressources consommant des adresses IP, de suivre les tendances en matière d'allocation d'adresses et d'optimiser la gestion de vos adresses IP afin de l'aligner sur l'évolution de votre infrastructure et de vos besoins commerciaux.

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 pour d'autres, il les contrôle uniquement. Il est donc important de comprendre la différence entre les deux 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 :
  - Adresses IP élastiques

- Groupes IPv4 publics

 Note

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.

- VPC
- 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 :
  - Adresses IP élastiques
  - Groupes IPv4 publics
  - VPC
  - Sous-réseaux VPC

## 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, choisissez Resources (Ressources).
3. Dans le menu déroulant IP situé en haut du volet de contenu, choisissez le protocole d'adresse IP que vous souhaitez utiliser : IPv4 ou IPv6.
4. Dans le menu déroulant des périmètres se trouvant dans la partie supérieure du panneau de contenu, sélectionnez le périmètre que vous souhaitez utiliser. Pour plus d'informations sur les portées, consultez [Fonctionnement d'IPAM](#).
5. 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.

6. 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.
  - IP allouées : 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.
7. 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 sur les commandes 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.

L'intégration d'IPAM à CloudWatch améliore votre capacité à surveiller, analyser et optimiser la gestion de vos adresses IP au sein de AWS.

Cas d'utilisation :

- Suivi des tendances d'utilisation des adresses IP : CloudWatch peut surveiller l'utilisation du groupe CIDR, l'allocation du périmètre et d'autres indicateurs IPAM, vous aidant ainsi à identifier de manière proactive les risques potentiels d'épuisement des adresses IP.
- Configuration d'alertes basées sur l'utilisation : Vous pouvez configurer les alarmes CloudWatch pour qu'elles vous avertissent lorsque l'utilisation des CIDR atteint des seuils prédéterminés, ce qui permet une intervention et une optimisation opportunes.
- Surveillance des événements IPAM : CloudWatch peut capturer et analyser les événements liés à IPAM, tels que les allocations CIDR, les désallocations et les modifications du périmètre, offrant ainsi une visibilité sur les activités de gestion des adresses IP.
- Génération de tableaux de bord personnalisés : en combinant les données IPAM avec d'autres indicateurs AWS, vous pouvez créer des tableaux de bord complets pour visualiser et analyser votre paysage d'adresses IP ainsi que les indicateurs de performance et d'infrastructure associés.

## Table des matières

- [Gestion des alarmes depuis la console IPAM](#)
- [Métriques IPAM](#)
- [Métriques d'utilisation des ressources IPAM](#)

## Gestion des alarmes depuis la console IPAM

Vous pouvez créer et gérer les alarmes Amazon CloudWatch directement depuis la console IPAM. Les alarmes associées aux [Métriques IPAM](#) ou aux [Métriques d'utilisation des ressources IPAM](#) à l'état INSUFFICIENT\_DATA ou ALARME apparaîtront sous forme de barres d'avertissement en haut de la console et sous forme d'indicateurs visuels dans le menu de navigation de gauche à côté de Surveillance.

Pour gérer les alarmes dans le cadre de ressources spécifiques, sélectionnez Ressources, puis choisissez un VPC, un sous-réseau ou un groupe. Lorsque la page des détails de la ressource s'ouvre, sélectionnez l'onglet Alarmes.

L'onglet Alarmes affiche toutes les alarmes CloudWatch associées à la ressource sélectionnée. Cet onglet permet de consulter les détails des alarmes, de surveiller les états actuels et d'accéder aux options de configuration des alarmes. L'onglet affiche les alarmes issues de l'espace de noms AWS/IPAM qui sont pertinentes pour la ressource que vous consultez.

La capture d'écran suivante illustre l'interface de gestion des alarmes de la console IPAM :

Alarm name	State	Metric	Resource ID	Time last updated	Actions enabled
nowalarm	ALARM	SubnetIPUsage	subnet-0	7/23/2025, 1:32:05 PM	Yes

L'onglet **Alarmes** fournit un résumé détaillé des alarmes CloudWatch dans l'espace de noms Amazon CloudWatch AWS/IPAM au sein de la région d'origine de votre IPAM :

- Nom de l'alarme : nom défini par l'utilisateur pour l'alarme CloudWatch.
- État : état actuel de l'alarme CloudWatch :
  - ALARME : la métrique est en dehors du seuil défini.
  - OK : la métrique se situe dans les limites du seuil défini.
  - INSUFFICIENT\_DATA : données insuffisantes pour déterminer l'état de l'alarme.
- Métrique : métrique CloudWatch spécifique surveillée par l'alarme.
- ID de ressource : identificateur unique de la ressource AWS surveillée par l'alarme.
- Heure de la dernière mise à jour : date et heure auxquelles l'état de l'alarme a été modifié ou évalué pour la dernière fois.
- Actions activées : indique si les actions CloudWatch sont activées pour l'alarme :
  - Oui : l'alarme peut déclencher des actions configurées lorsque les conditions sont remplies.
  - Non : l'alarme surveille mais n'exécute aucune action.

Par ailleurs, si vous consultez les graphiques d'utilisation dans l'onglet **Surveillance** d'un VPC, d'un sous-réseau ou d'un groupe, vous pourrez sélectionner l'option de création d'alarme dans le cadre de l'utilisation de la ressource. Vous serez ensuite redirigé vers la console CloudWatch, avec les détails de la ressource et des métriques préremplis. À partir de là, vous pourrez configurer un seuil d'alarme, afin d'être averti lorsque l'utilisation atteint un pourcentage spécifique, par exemple.

## Métriques IPAM

IPAM publie des données concernant vos groupes et périmètres 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 IPAM

L'espace de noms AWS/IPAM inclut les métriques IPAM suivantes.

Nom des métriques	Description
TotalActivelpCount	<p>Nombre total d'adresses IP actives dans votre IPAM qui vous seraient facturées si vous passiez du niveau gratuit au niveau avancé. Une adresse IP active est définie comme une adresse IP ou un préfixe associé à une interface réseau Elastic (ENI) qui est attachée à une ressource telle qu'une instance EC2.</p> <ul style="list-style-type: none"><li>• Cette métrique est uniquement disponible pour les clients de l'offre gratuite.</li><li>• Si votre IPAM est <a href="#">intégré à AWS Organizations</a>, le nombre d'adresses IP actives couvre tous les comptes de l'organisation.</li><li>• Vous ne pouvez pas afficher la répartition du nombre d'adresses IP actives par type d'IP (public/privé) ou par classe (IPv4/IPv6).</li><li>• IPAM ne compte que les adresses IP des ENI appartenant à des comptes surveillés. Le décompte peut être inexact pour les sous-réseaux partagés. Les adresses IP sont exclues si le propriétaire du sous-réseau ou le propriétaire de l'ENI n'est pas couvert par IPAM.</li></ul>

## Métriques de groupes IPAM

L'espace de noms AWS/IPAM comprend les métriques de groupe suivantes pour 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 <a href="#">Création d'un groupe IPv4 de niveau supérieur</a> .
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 <a href="#">Création d'un groupe IPv4 de niveau supérieur</a> .
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

L'espace de noms AWS/IPAM comprend les métriques de périmètre suivantes pour 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.

## Métriques IP publiques IPAM

L'espace de noms AWS/IPAM comprend les métriques IP publiques suivantes pour IPAM.

Nom des métriques	Description
AmazonOwnedContigIPs	Le nombre d'adresses IP au sein des CIDR qui sont fournies à des groupes IPv4 publics contigus fournis par Amazon et appartenant à l'IPAM.
AllocatedAmazonOwnedContigIPs	Nombre d'adresses IP allouées à partir d'un bloc CIDR de groupe IPv4 public contigu fourni par Amazon.
UnallocatedAmazonOwnedContigIPs	Nombre d'adresses IP dans le bloc CIDR du groupe IPv4 public contigu fourni par Amazon et appartenant à l'IPAM.
AssociatedAmazonOwnedContigIPs	Nombre d'adresses IP Elastic allouées à partir d'un bloc CIDR de groupe IPv4 public contigu fourni par Amazon et associé à une interface réseau Elastic.
UnassociatedAmazonOwnedContigIPs	Nombre d'adresses IP Elastic qui ont été allouées à partir d'un bloc CIDR de groupe IPv4 public contigu fourni par Amazon et qui ne sont pas associées à une interface réseau Elastic.

## Métriques de résolveur de listes de préfixes IPAM

Nous vous encourageons à configurer des alarmes CloudWatch sur les métriques de défaillance, car vous devrez peut-être réévaluer et ajuster les [règles du résolveur de liste de préfixes](#) afin de respecter les limites de version et de taille de liste de préfixes.

Nom des métriques	Description
IpamPrefixListResolverSyncFailure	Le résolveur de liste de préfixes n'a pas pu être synchronisé avec la cible. Cela peut se produire si un quota comme « entrées CIDR par version du résolveur de liste de préfixes » est dépassé, si la liste de préfixes cible est introuvable ou si la synchronisation est désactivée sur la liste de préfixes gérée cible.
IpamPrefixListResolverSyncSuccess	Le résolveur de liste de préfixes a été correctement synchronisé avec la cible.
IpamPrefixListResolverVersionCreationSuccess	La création de la version a réussi.
IpamPrefixListResolverVersionCreationFailure	La création de la version a échoué. Cela peut se produire si vous avez atteint le quota « entrées CIDR par version du résolveur de liste de préfixes ».

## Dimensions métriques

Pour filtrer ces métriques IPAM, utilisez les dimensions suivantes.

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

Dimension	Description
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

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.
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.
BringYourOwnIPs	Le nombre d'adresses IPv4 publiques que vous avez transférées 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-réseau par défaut ou dans un sous-réseau configuré pour attribuer automatiquement une adresse IPv4 publique.
ServiceManagedBringYourOwnIPs	Le nombre d'adresses IPv4 publiques que vous avez transférées 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.
UnassociatedAmazonOwnedElasticIPs	Le nombre d'adresses IP Elastic détenues par Amazon que vous n'avez pas associées aux ressources dans votre compte AWS.
UnassociatedBringYourOwnIPs	Le nombre d'adresses IPv4 publiques que vous avez transférées vers AWS en utilisant Fourniture de vos propres adresses

Nom des métriques	Description
	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 compte AWS 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 vous [Intégration d'IPAM à des comptes extérieurs à votre organisation](#), le propriétaire de l'IPAM peut 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 renvoient vers la documentation de référence sur les commandes de l'AWS CLI. La documentation fournit des descriptions détaillées des options que vous pouvez utiliser lorsque vous exécutez les commandes.

- Consulter l'historique d'un CIDR : [get-ipam-address-history](#)

Pour voir des exemples de la façon dont vous pouvez utiliser l'AWS CLI pour 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

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

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

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 facture toutes les adresses IPv4 publiques, y compris les adresses IPv4 publiques associées aux instances en cours d'exécution ainsi que 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 Elastic (EIP) : adresses IPv4 publiques statiques fournies par Amazon que vous pouvez associer à une instance EC2, à une interface réseau Elastic 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 comprises dans la plage d'adresses IPv4 que vous avez redirigées vers AWS en utilisant [Fourniture de vos propres adresses IP \(BYOIP, Bring your own IP addresses\)](#).
- Adresses IPv4 gérées par le service : adresses IPv4 publiques automatiquement provisionnées sur des ressources AWS et gérées par un service AWS. Par exemple, les adresses IPv4 publiques sur Amazon ECS, Amazon RDS ou Amazon WorkSpaces.

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 détenues par Amazon : adresses IP Elastic que vous avez provisionnées ou attribuées à des ressources dans 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 transférées vers AWS en utilisant [Fourniture de vos propres adresses IP \(BYOIP\)](#).
  - IP gérées par le service : adresses IPv4 publiques provisionnées et gérées par un service AWS.

- BYOIP géré par un service : adresses IPv4 publiques amenées vers AWS et gérées par un service AWS.
- EIP contigüs appartenant à Amazon : adresses IP Elastic allouées à partir d'un groupe IPAM IPv4 public contigu fourni par Amazon.
- Utilisation d'EIP : le nombre d'adresses IP Elastic organisées selon leur utilisation.
  - EIP associées détenues par Amazon : adresses IP Elastic que vous avez provisionnées dans votre compte AWS et que vous avez associées à une instance EC2, à une interface réseau ou à une ressource AWS.
  - BYOIP associée : adresses IPv4 publiques que vous avez transférées vers AWS en utilisant la BYOIP et que vous avez associées à une interface réseau.
  - EIP non associées détenues par Amazon : adresses IP Elastic que vous avez provisionnées dans votre compte AWS mais que vous n'avez pas associées à une interface réseau.
  - BYOIP non associée : adresses IPv4 publiques que vous avez transférées vers AWS en utilisant la BYOIP mais que vous n'avez pas associées à une interface réseau.
  - EIP contigüs associées appartenant à Amazon : adresses IP Elastic allouées à partir d'un groupe IPAM IPv4 public contigu fourni par Amazon et associées à une ressource.
  - EIP contigüs non associées appartenant à Amazon : adresses IP Elastic allouées à partir d'un groupe IPAM IPv4 public contigu fourni par Amazon et non associées à une ressource.
- Utilisation des adresses IP IPv4 contigüs appartenant à Amazon : tableau qui indique l'utilisation des adresses IPv4 publiques contigüs au fil du temps et les groupes IPAM IPv4 associés appartenant à Amazon.
- Adresses IP publiques : un tableau des adresses IPv4 publiques et de leurs attributs.
  - Adresse IP : l'adresse IPv4 publique.
  - Associée : si l'adresse est associée ou non à une instance EC2, à une interface réseau ou à une ressource AWS.
    - Associée : l'adresse IPv4 publique est associée à une instance EC2, à une interface réseau ou à une ressource AWS.
    - Non associée : l'adresse IPv4 publique n'est associée à aucune ressource et est inactive dans votre compte AWS.
  - 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 transférée vers AWS en utilisant BYOIP.

- IP publique EC2 : l'adresse IPv4 publique a été attribuée automatiquement à une instance EC2.
- Service géré BYOIP : l'adresse IPv4 publique a été transférée vers AWS en utilisant Apportez votre propre adresse IP (BYOIP).
- IP gérée par le service : l'adresse IPv4 publique a été provisionnée et est gérée par un service AWS.
- 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](#).
  - Database Migration Service : une instance de réplication AWS Database Migration Service (DMS).
  - Redshift : un cluster Amazon Redshift.
  - RDS : une instance Amazon Relational Database Service (RDS).
  - Équilibrer de charge (EC2) : un Application Load Balancer ou un Network Load Balancer.
  - Passerelle NAT (VPC) : une passerelle NAT publique Amazon VPC.
  - VPN Site-to-Site : une 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 de bordure réseau : si l'adresse IP est publiée, il s'agit de la Région AWS à partir de laquelle l'adresse IP est publiée.

- 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 n'êtes pas autorisé à 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.
- Balises : les paires de clés et de valeurs qui jouent le rôle de métadonnées pour organiser vos ressources AWS.

## Command line

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

# 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

- [Prise en main de l'IPAM à l'aide de l'interface de ligne de commande AWS](#)
- [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](#)
- [Allouer des adresses IP Elastic séquentielles à partir d'un groupe IPAM](#)

## Prise en main de l'IPAM à l'aide de l'interface de ligne de commande AWS

Ce tutoriel vous guide tout au long du processus de configuration et d'utilisation du Gestionnaire d'adresses IP (IPAM) d'Amazon VPC à l'aide de l'interface de ligne de commande AWS avec un seul compte AWS. À la fin de ce tutoriel, vous aurez créé un IPAM et une hiérarchie de groupes d'adresses IP et aurez alloué un CIDR à un VPC.

## Prérequis

Avant de commencer ce tutoriel, assurez-vous de ce qui suit :

- Vous disposez d'un compte AWS autorisé à créer et à gérer des ressources IPAM.
- Vous disposez de l'interface de ligne de commande AWS, installée et configurée avec les informations d'identification appropriées. Pour plus d'informations sur l'installation de l'interface de ligne de commande AWS, consultez la section [Installing or updating the latest version of the](#)

[AWS CLI](#). Pour plus d'informations sur la configuration de l'interface de ligne de commande AWS, consultez la section [Configuration basics](#).

- Vous avez une compréhension de base de l'adressage IP et de la notation CIDR.
- Vous avez une connaissance de base des concepts Amazon VPC.
- Durée du tutoriel : environ 30 minutes.

## Création d'un IPAM

La première étape consiste à créer un IPAM avec des régions d'exploitation. Un IPAM vous permet de planifier, suivre et surveiller les adresses IP dans le cadre de vos charges de travail AWS.

Créez un IPAM avec les régions d'exploitation us-east-1 et us-west-2 :

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

Cette commande crée un IPAM et permet à ce dernier de gérer les adresses IP dans les régions spécifiées. Les régions d'exploitation sont les régions AWS au sein desquelles l'IPAM est autorisé à gérer des CIDR d'adresses IP.

Vérifiez que votre IPAM a été créé :

```
aws ec2 describe-ipams
```

Notez l'ID de l'IPAM indiqué dans la sortie obtenue, car vous en aurez besoin pour les étapes suivantes.

Attendez que l'IPAM soit entièrement créé et disponible (environ 20 secondes) :

```
sleep 20
```

## Obtention de l'ID de portée IPAM

Lorsque vous créez un IPAM, AWS crée automatiquement une portée privée et une portée publique. Dans le cadre de ce tutoriel, nous utiliserons la portée privée.

Récupérez les détails de l'IPAM et extrayez l'ID de portée privée :

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

Remplacez `ipam-0abcd1234` par l'ID de l'IPAM réel.

Dans la sortie obtenue, identifiez et notez l'ID de portée privée indiqué dans le champ `PrivateDefaultScopeId`. Elle doit ressembler à ceci : `ipam-scope-0abcd1234`.

## Création d'un groupe IPv4 de niveau supérieur

Créons à présent un groupe de niveau supérieur dans la portée privée. Ce groupe servira de parent à tous les autres groupes de notre hiérarchie.

Créez un groupe IPv4 de niveau supérieur :

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

Remplacez `ipam-scope-0abcd1234` par l'ID de portée privée réel.

Attendez que le groupe soit entièrement créé et disponible :

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

Remplacez `ipam-pool-0abcd1234` par l'ID de groupe de niveau supérieur réel. L'état doit être `create-complete` avant de poursuivre.

Une fois le groupe disponible, provisionnez-le avec un bloc CIDR :

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

Attendez que le CIDR soit entièrement provisionné :

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

L'état doit être provisioned avant de poursuivre.

## Création d'un groupe IPv4 régional

Créez ensuite un groupe régional au sein du groupe de niveau supérieur. Ce groupe sera spécifique à une région AWS particulière.

Créez un groupe IPv4 régional :

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

Remplacez `ipam-scope-0abcd1234` par l'ID de portée privée réel et `ipam-pool-0abcd1234` par l'ID de groupe de niveau supérieur.

Attendez que le groupe régional soit entièrement créé et disponible :

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

Remplacez `ipam-pool-1abcd1234` par l'ID de groupe régional réel. L'état doit être `create-complete` avant de poursuivre.

Une fois le groupe disponible, provisionnez-le avec un bloc CIDR :

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

Attendez que le CIDR soit entièrement provisionné :

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

L'état doit être provisioned avant de poursuivre.

## Création d'un groupe IPv4 de développement

Créez à présent un groupe de développement au sein du groupe régional. Ce groupe sera utilisé dans le cadre d'environnements de développement.

Créez un groupe IPv4 de développement :

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

Remplacez `ipam-scope-0abcd1234` par l'ID de portée privée réel et `ipam-pool-1abcd1234` par l'ID de groupe régional.

Remarque : il est important d'inclure le paramètre `--locale` correspondant aux paramètres régionaux du groupe parent.

Attendez que le groupe de développement soit entièrement créé et disponible :

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

Remplacez `ipam-pool-2abcd1234` par l'ID de groupe de développement réel. L'état doit être `create-complete` avant de poursuivre.

Une fois le groupe disponible, provisionnez-le avec un bloc CIDR :

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

Attendez que le CIDR soit entièrement provisionné :

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

L'état doit être `provisioned` avant de poursuivre.

## Création d'un VPC utilisant un CIDR de groupe IPAM

Créez enfin un VPC qui utilise un CIDR à partir de votre groupe IPAM. Cet exemple montre comment l'IPAM peut être utilisé pour allouer de l'espace d'adressage IP aux ressources AWS.

Créez un VPC utilisant un CIDR de groupe IPAM :

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

Remplacez `ipam-pool-2abcd1234` par l'ID de groupe de développement réel.

Le paramètre `--ipv4-netmask-length 26` indique que vous souhaitez qu'un bloc CIDR /26 (64 adresses IP) soit alloué à partir du groupe. Cette longueur de masque réseau est choisie pour s'assurer qu'elle est inférieure au bloc CIDR du groupe (/24).

Vérifiez que votre VPC a été créé :

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

## Vérification de l'allocation du groupe IPAM

Vérifiez que le CIDR a été alloué à partir de votre groupe IPAM :

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

Remplacez `ipam-pool-2abcd1234` par l'ID de groupe de développement réel.

Cette commande affiche toutes les allocations effectuées à partir du groupe IPAM spécifié, y compris le VPC que vous venez de créer.

## Résolution des problèmes

Voici quelques problèmes courants que vous pouvez rencontrer dans le cadre de l'utilisation de l'IPAM :

- Erreurs d'autorisation : assurez-vous que l'utilisateur ou le rôle IAM dispose des autorisations nécessaires pour créer et gérer des ressources IPAM. Vous aurez peut-être besoin des autorisations `ec2:CreateIpam`, `ec2:CreateIpamPool` et d'autres autorisations connexes.
- Limite de ressource dépassée : par défaut, vous ne pouvez créer qu'un seul IPAM par compte. Si vous possédez déjà un IPAM, vous devrez le supprimer avant d'en créer un nouveau ou d'utiliser celui qui existe.
- Échecs d'allocation de CIDR : lorsque vous provisionnez des CIDR dans des groupes, assurez-vous que le CIDR que vous essayez de provisionner ne génère pas de chevauchement avec les allocations existantes dans d'autres groupes.
- Expiration des demandes d'API : si vous rencontrez des erreurs de type « `RequestExpired` », cela peut être dû à la latence du réseau ou à des problèmes de synchronisation temporelle. Essayez à nouveau d'exécuter la commande.
- Erreurs d'état incorrect : si vous recevez des erreurs de type « `IncorrectState` », cela peut être dû au fait que vous essayez d'effectuer une opération sur une ressource dont l'état n'est pas correct. Attendez que la ressource soit entièrement créée ou provisionnée avant de poursuivre.
- Erreurs de taille d'allocation : si vous recevez des erreurs de type « `InvalidParameterValue` » concernant la taille d'allocation, assurez-vous que la longueur du masque réseau que vous demandez est adaptée à la taille du groupe. Par exemple, vous ne pouvez pas allouer un CIDR /25 à partir d'un groupe /24.
- Violations de dépendance : lors du nettoyage des ressources, vous pouvez rencontrer des erreurs de type « `DependencyViolation` ». Cela est dû au fait que les ressources présentent des dépendances les unes par rapport aux autres. Assurez-vous de supprimer les ressources dans l'ordre inverse de leur création et de déprovisionner les CIDR avant de supprimer les groupes.

## Nettoyage des ressources

Lorsque vous avez terminé ce tutoriel, nettoyez les ressources créées pour éviter des frais inutiles.

### 1. Supprimer le VPC

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

### 2. Déprovisionnez le CIDR à partir du groupe de développement :

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

### 3. Supprimez le groupe de développement :

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

### 4. Déprovisionnez le CIDR à partir du groupe régional :

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

### 5. Supprimez le groupe régional :

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

### 6. Déprovisionnez le CIDR à partir du groupe de niveau supérieur :

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

### 7. Supprimez le groupe de niveau supérieur :

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

### 8. Supprimez l'IPAM :

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

Remplacez tous les ID par les ID de ressource réels.

#### Note

Vous devrez peut-être attendre entre ces opérations que les ressources soient entièrement supprimées avant de passer à l'étape suivante. Si vous rencontrez des violations de dépendance, attendez quelques secondes et réessayez.

## Étapes suivantes

Maintenant que vous avez appris à créer et à utiliser l'IPAM avec l'interface de ligne de commande AWS, vous souhaiterez peut-être explorer des fonctionnalités plus avancées :

- [Planification de l'approvisionnement des adresses IP](#) – Découvrez comment planifier efficacement votre espace d'adressage IP
- [Contrôle de l'utilisation du CIDR par ressource](#) – Découvrez comment surveiller l'utilisation des adresses IP
- [Partage d'un groupe IPAM à l'aide d'AWS RAM](#) – Découvrez comment partager des groupes IPAM entre des comptes AWS
- [Intégration d'IPAM aux comptes d'une organisation AWS](#) – Découvrez comment utiliser l'IPAM au sein de votre organisation

## 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.

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. [Learn more](#)

**Organization**

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

**Actions**

**Organizational structure**

**Account created/joined date**

Account	Created/Joined Date
example-member-account-1 848560618819   example-member-account-1@amazon.com	Joined 2022/12/28
example-member-account-2 848560618819   example-member-account-2@amazon.com	Joined 2022/12/28
example-management-account 855210303341   example-management-account@amazon.com	Joined 2022/12/28

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

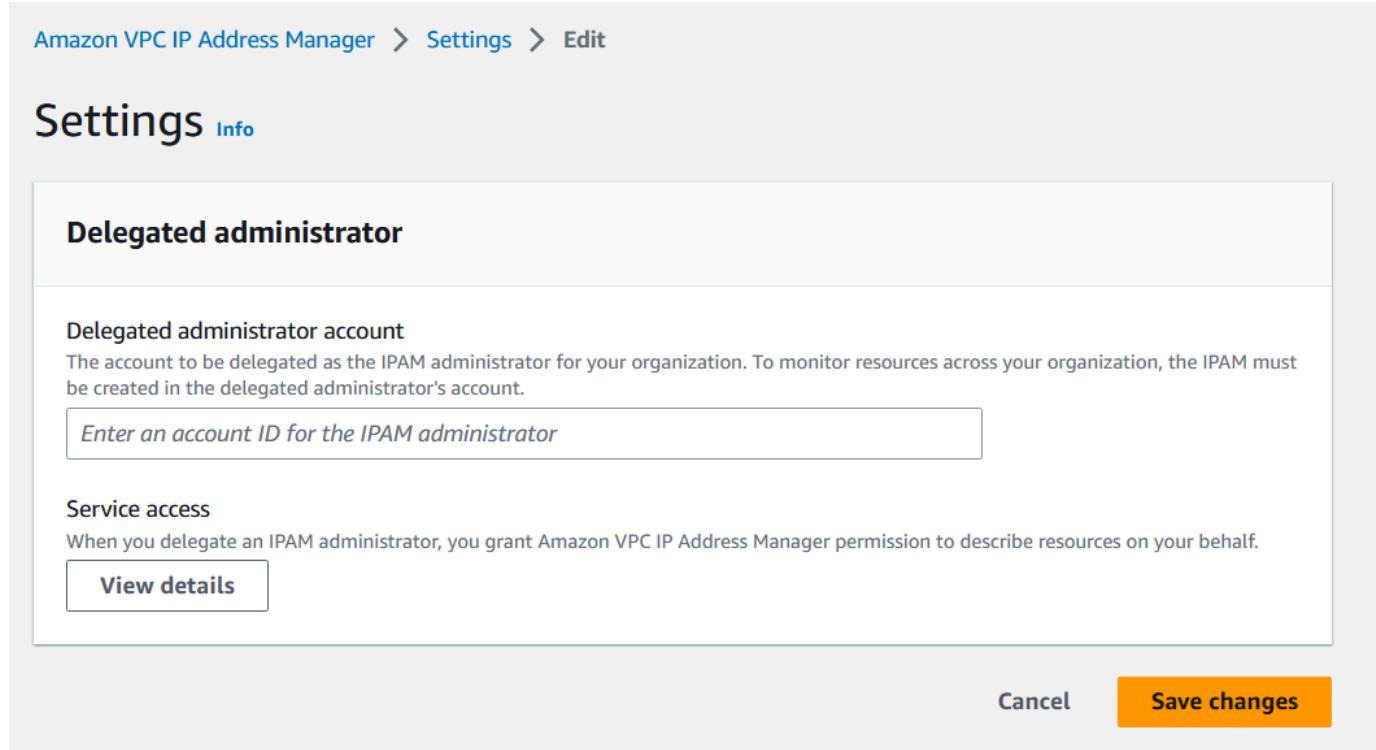
Au cours de cette étape, vous allez déléguer un compte membre AWS Organizations en tant qu'administrateur IPAM. Lorsque vous délégez un administrateur IPAM, [un rôle lié au service](#) est automatiquement créé dans chacun de vos comptes membres AWS Organizations. IPAM contrôle l'utilisation des adresses 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 Gestion des identités et des accès AWS (IAM) requises. Pour plus d'informations, consultez [Intégration d'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 AWS Management Console, sélectionnez la région AWS dans laquelle vous souhaitez utiliser l'IPAM.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation).
4. Choisissez 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.



The screenshot shows the 'Settings' page in the Amazon VPC IP Address Manager. The 'Delegated administrator' section is highlighted. It contains a text input field for entering an account ID for the IPAM administrator, a 'Service access' section with a 'View details' button, and a 'Cancel' and 'Save changes' button at the bottom.

Amazon VPC IP Address Manager > Settings > Edit

## Settings Info

### Delegated administrator

Delegated administrator account

The account to be delegated as the IPAM administrator for your organization. To monitor resources across your organization, the IPAM must be created in the delegated administrator's account.

Enter an account ID for the IPAM administrator

Service access

When you delegate an IPAM administrator, you grant Amazon VPC IP Address Manager permission to describe resources on your behalf.

[View details](#)

Cancel [Save changes](#)

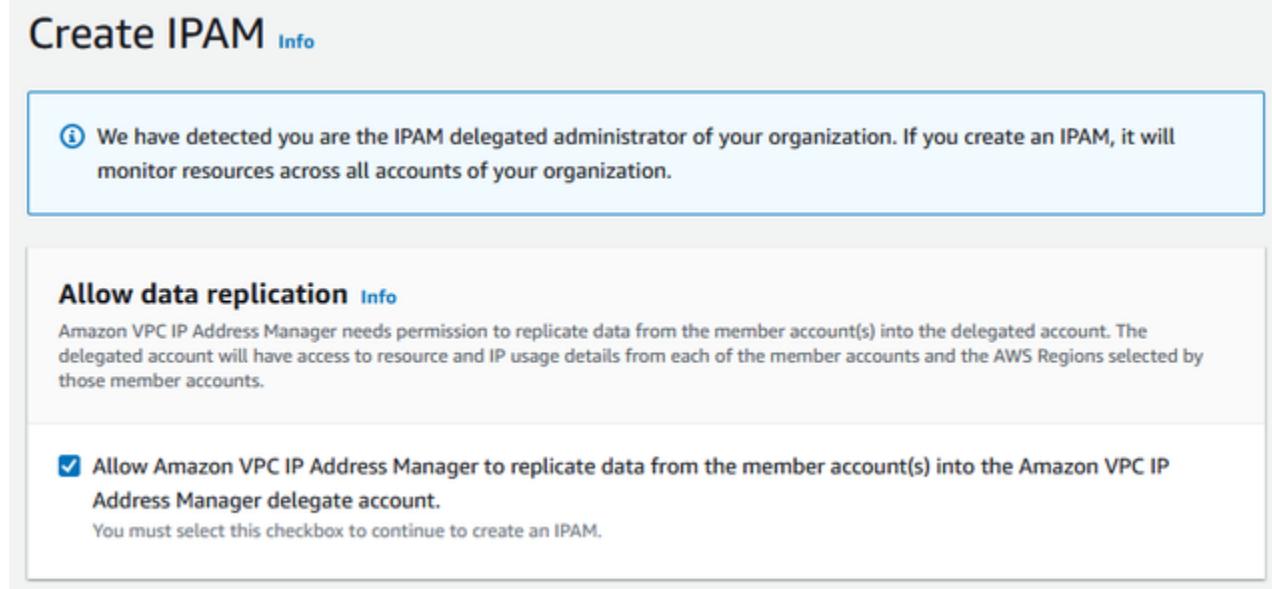
6. Sélectionnez Enregistrer les modifications. Les informations relatives à l'administrateur délégué sont renseignées avec les détails liés au compte membre.

## 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 plus d'informations, consultez [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.

### IPAM settings Info

#### Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

#### Description - *optional*

Write a brief description for the IPAM.

#### Operating Regions

Select Regions in which the IPAM will discover resources and manage IPs. The current region will always be set as an operating region.

 X X X

#### Default resources will be created

On IPAM creation, the following IPAM resources will also be created:

- A default private scope. Resources using private IP space will be imported into the private scope.
- A default public scope. Resources using public IP space will be imported into the public scope.
- A default resource discovery, which controls the resources that IPAM will discover.

## 6. Sélectionnez Create IPAM (Créer un IPAM).

Successfully created IPAM ipam-005f921c17ebd5107

Amazon VPC IP Address Manager > IPAMs > ipam-005f921c17ebd5107

## DemolIPAM (ipam-005f921c17ebd5107) [Info](#)

[Edit](#) [Delete](#)

IPAM details			
IPAM ID <a href="#">ipam-005f921c17ebd5107</a>	Description -	Owner ID <a href="#">320805250157</a>	Region <a href="#">us-east-1</a>
IPAM ARN <a href="#">arn:aws:ec2::320805250157:ipam/ipam-005f921c17ebd5107</a>	Default public scope <a href="#">ipam-scope-0d3539a30b57dcdd1</a>	Default private scope <a href="#">ipam-scope-0a158dde35c51107b</a>	Scope count 2
State <a href="#">Create-complete</a>	Default resource discovery <a href="#">ipam-res-disco-0f4ef577a9f37a162</a>		

[Operating Regions](#) [Associated discoveries](#) [Tags](#)

### Operating Regions (3) [Info](#)

Filter Regions

Region

US East (N. Virginia) - us-east-1
US West (N. California) - us-west-1
US West (Oregon) - us-west-2

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

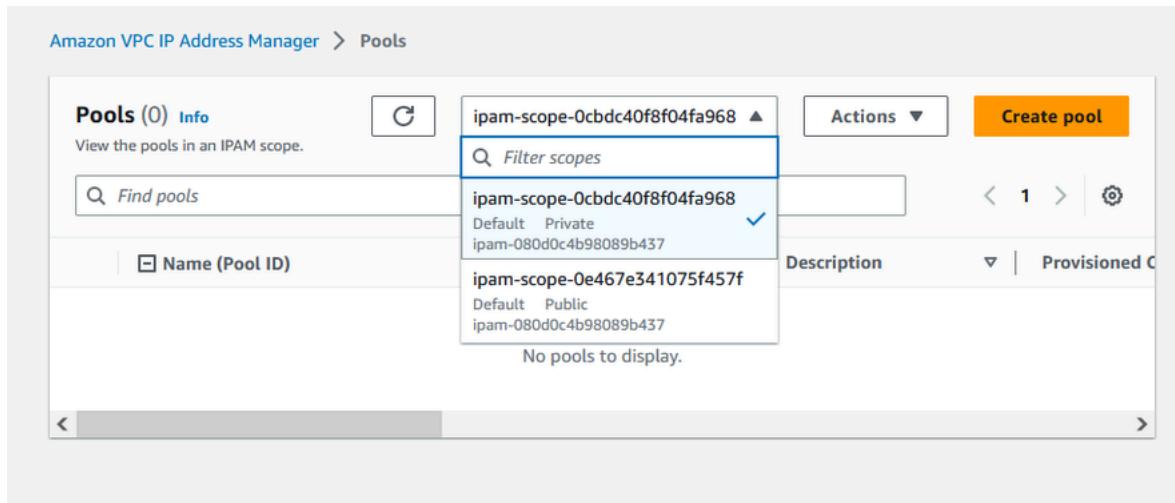
Dans ce didacticiel, vous créez une hiérarchie de groupes en commençant par le groupe IPAM de niveau supérieur. Dans les étapes suivantes, vous créerez une paire de groupes régionaux et un groupe de développement de pré-production dans l'un des groupes régionaux.

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, sélectionnez Pools (Groupes).
3. Choisissez la portée privée.



The screenshot shows the 'Pools' section of the IP Address Manager. A dropdown menu is open, showing 'ipam-scope-0cbcdc40f8f04fa968' as the selected scope. Below the dropdown, a table lists two scopes: 'ipam-scope-0cbcdc40f8f04fa968' (Default Private) and 'ipam-scope-0e467e341075f457f' (Default Public). A message at the bottom of the table says 'No pools to display.'

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. Sous Address family (Famille d'adresses), choisissez IPv4.
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.

Amazon VPC IP Address Manager > Pools > Create

## Create pool in ipam-scope-0cbdc40f8f04fa968

### Pool settings

Name (IPAM ID)	Name (Scope ID)
DemolPAM (ipam-080d0c4b98089b437)	ipam-scope-0cbdc40f8f04fa968

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify. Tags are not visible to other accounts even if a pool is shared.

Global pool

**Description - optional**  
Write a brief description for the pool.

My pool for VPCs

### Pool hierarchy Info

**Source pool**  
To provision a CIDR into this pool, it must be available in the source pool. If no source pool is selected, then the space must be available in the scope.

No source pool

**Address family**  
Select the address family for this pool.

IPv4  
 IPv6

Pools in the private scope must have address family IPv4.

**Locale**  
Select a locale for this pool to reside.

None

A locale can only be selected if there is no source pool, or if the source pool's locale is None.

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

**CIDRs to provision** Info

CIDRs to be provisioned must either be available in the source pool's space, or in the scope's space if no source pool.

**CIDR**

Enter a CIDR to be provisioned.

65K IPs

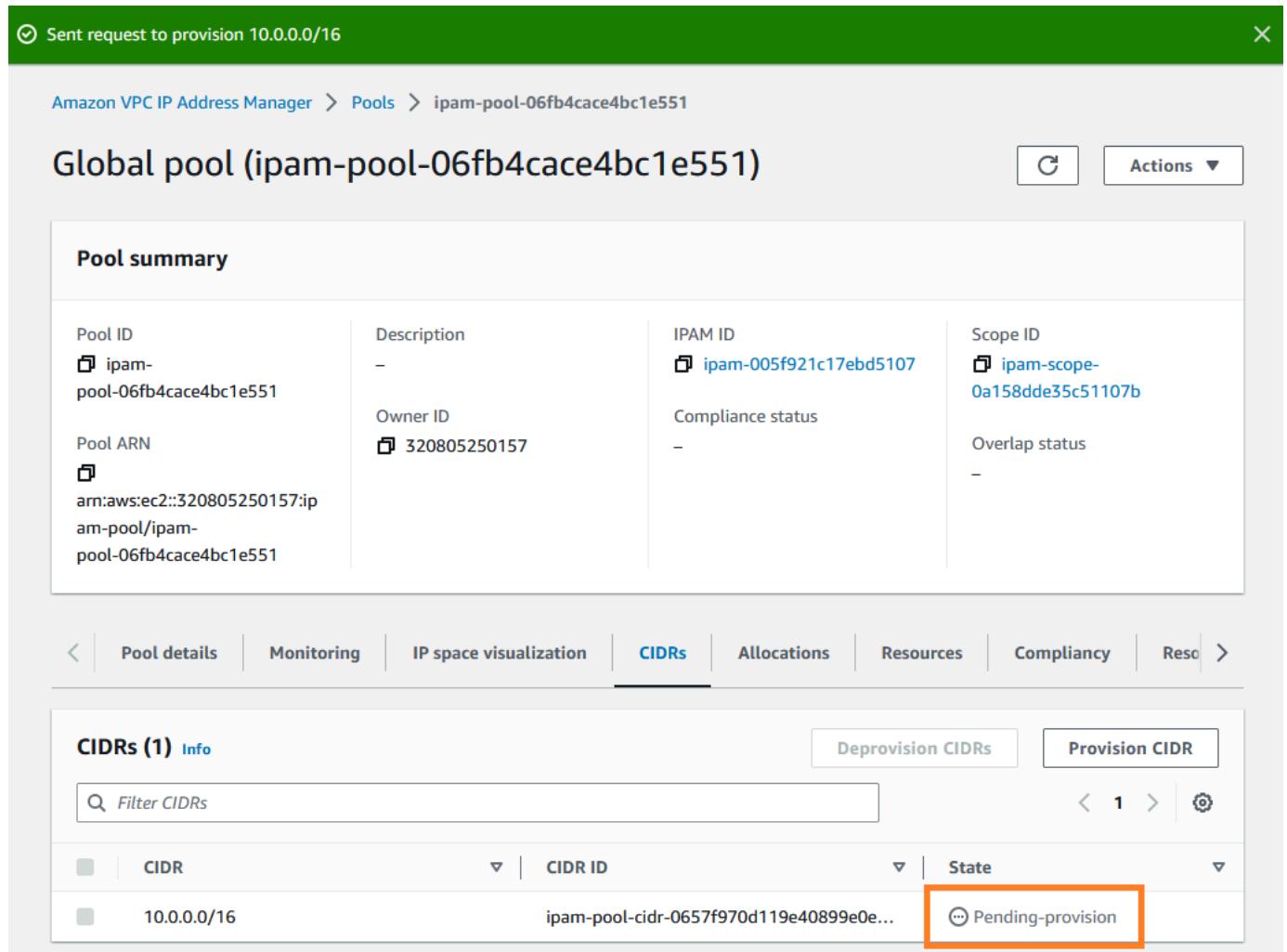
12. Laissez l'option Configurer les paramètres des règles d'allocation de ce groupe désactivées. Il s'agit de notre groupe de niveau supérieur, et vous n'allouerez pas de CIDR aux VPC directement à partir de ce groupe. Au lieu de cela, vous les allouerez à partir d'un sous-groupe que vous créerez à partir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

**Allocation rule settings - optional** Info**AWS best practice**

We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).

 Configure this pool's allocation rule settings

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



Sent request to provision 10.0.0.0/16

Amazon VPC IP Address Manager > Pools > ipam-pool-06fb4cace4bc1e551

## Global pool (ipam-pool-06fb4cace4bc1e551)

Pool summary

Pool ID ipam-pool-06fb4cace4bc1e551	Description -	IPAM ID ipam-005f921c17ebd5107	Scope ID ipam-scope-0a158dde35c51107b
Pool ARN arn:aws:ec2::320805250157:ipam-pool/ipam-pool-06fb4cace4bc1e551	Owner ID 320805250157	Compliance status -	Overlap status -

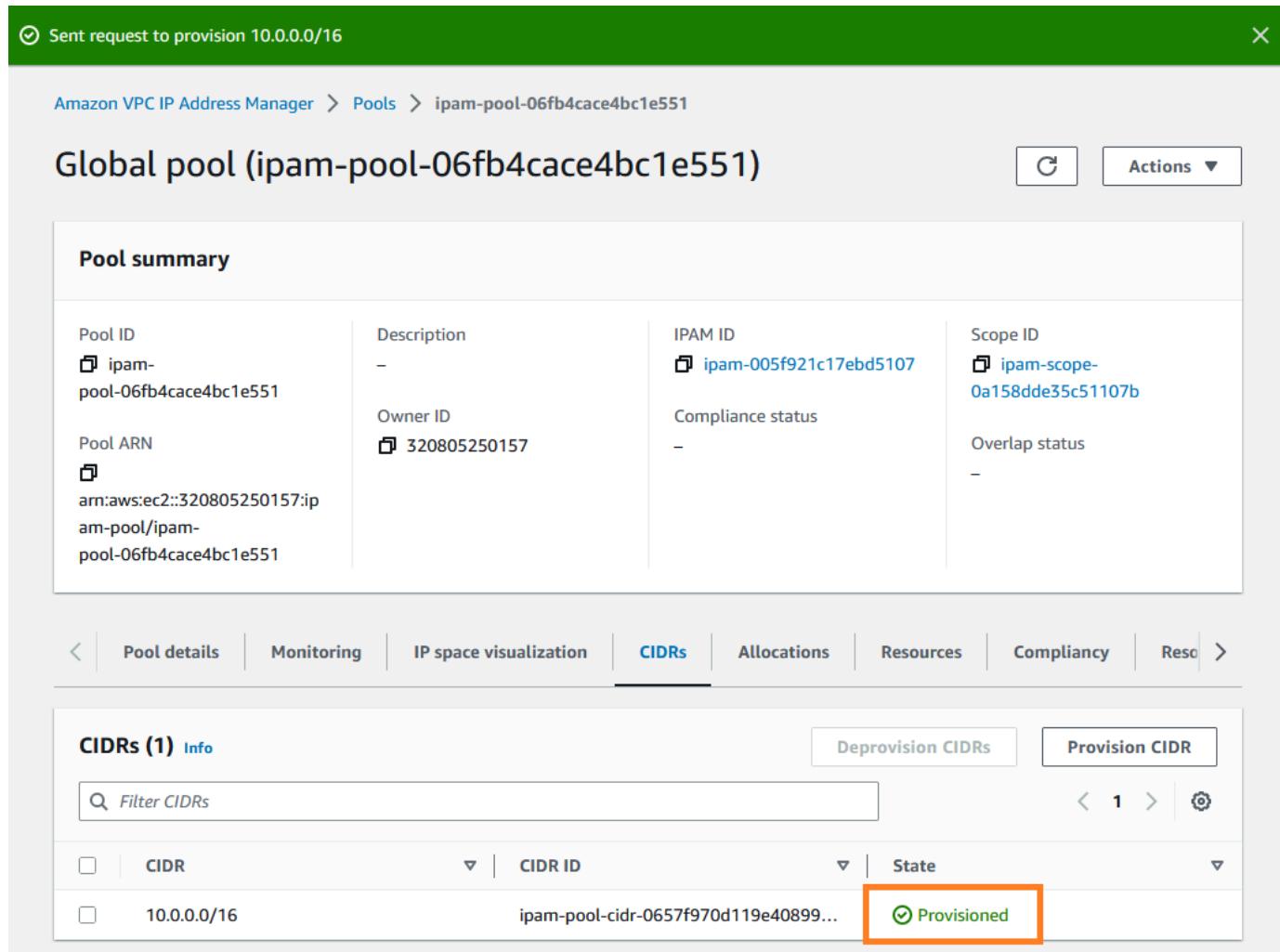
< Pool details Monitoring IP space visualization CIDRs Allocations Resources Compliancy Reso >

### CIDRs (1) Info

Deprovision CIDRs Provision CIDR

Filter CIDRs	CIDR	CIDR ID	State
	10.0.0.0/16	ipam-pool-cidr-0657f970d119e40899e0e...	Pending-provision

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



The screenshot shows the IP Address Manager interface for a global pool. At the top, a green banner indicates a request to provision 10.0.0.0/16. The main page displays the pool summary with details like Pool ID, Description, IPAM ID, Scope ID, and various ARNs and IDs. Below this, the CIDRs tab is selected, showing a table with one entry: 10.0.0.0/16, which is marked as 'Provisioned' with a green checkmark. The table also includes columns for CIDR, CIDR ID, and State.

CIDR	CIDR ID	State
10.0.0.0/16	ipam-pool-cidr-0657f970d119e40899...	Provisioned

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

- 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, sélectionnez 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.

### Pool hierarchy [Info](#)

**Source pool**  
To provision a CIDR into this pool, it must be available in the source pool. If no source pool is selected, then the space must be available in the scope.

Global pool (ipam-pool-023b91cf28c61a0fb) ▾

**▼ Source pool summary**

Name (Pool ID)	Provisioned CIDRs
Global pool (ipam-pool-023b91cf28c61a0fb)	10.0.0.0/16
Description	Locale
–	None

**Address family (inherited)**  
Select the address family for this pool.

IPv4  
 IPv6

Pools in the private scope must have address family IPv4.

**Locale**  
Select a locale for this pool to reside.

US West (N. California) - us-west-1 ▾

A locale can only be selected if there is no source pool, or if the source pool's locale is None.

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.

## CIDRs to provision Info

CIDRs to be provisioned must either be available in the source pool's space, or in the scope's space if no source pool.

### IP space visualization (source pool)

■ Zoom ■ Overlapping ■ New allocation ■ Allocated ■ Available

10.0.0.0/16 (100% available → 75% available after allocations)



#### CIDR

Enter a CIDR to be provisioned.

10.0.0.0/18

16K IPs

Remove

< > ^ ^

Add specific CIDR

Add CIDR by size

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.

## Allocation rule settings - *optional* Info



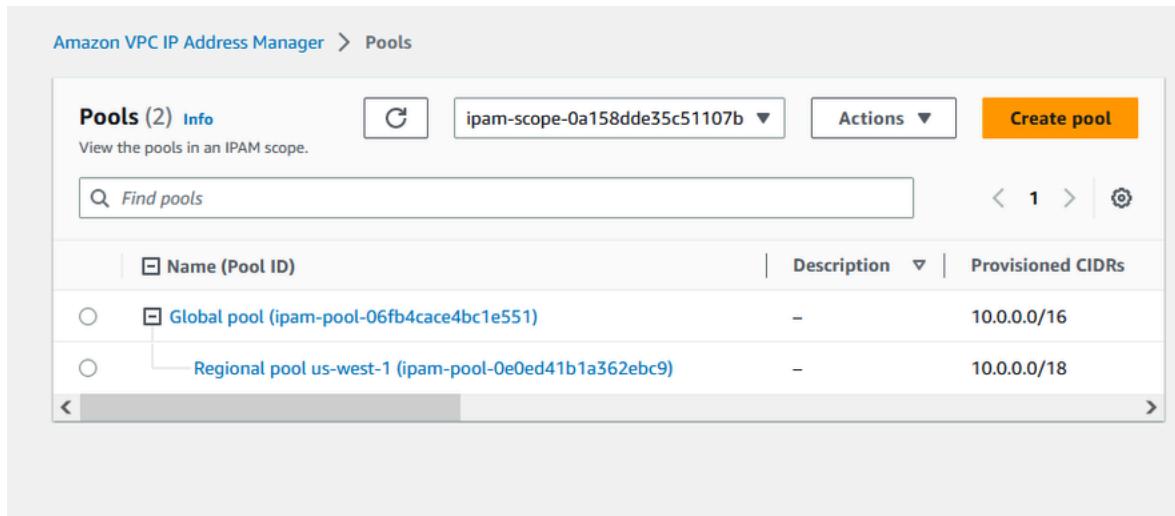
### AWS best practice

We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).



Configure this pool's allocation rule settings

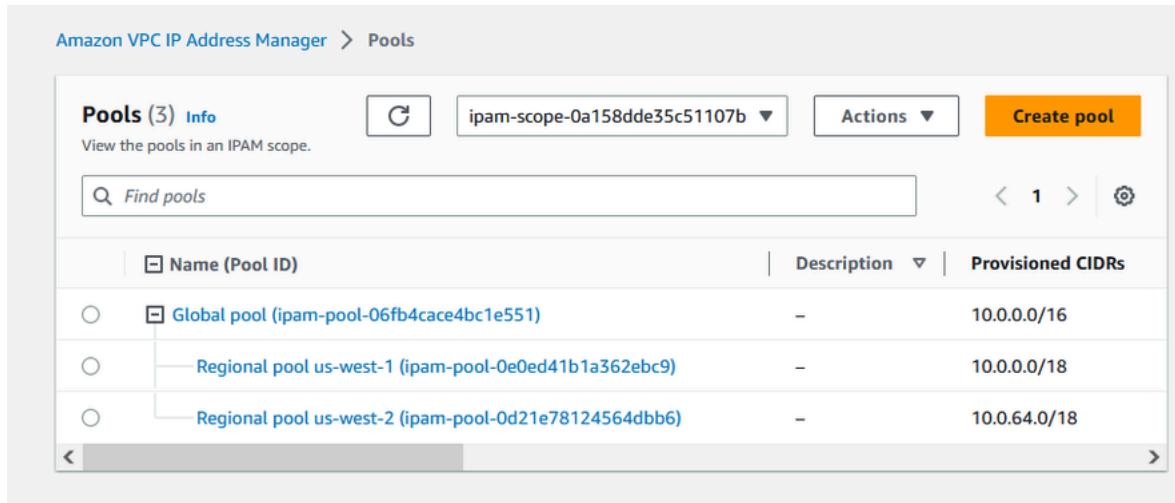
11. Sélectionnez Create pool (Créer un groupe).
12. Revenez à la vue Groupes pour voir la hiérarchie des groupes IPAM que vous avez créés.



The screenshot shows the 'Pools' section of the IP Address Manager. It displays two pools under the scope 'ipam-scope-0a158dde35c51107b'. The 'Global pool (ipam-pool-06fb4cace4bc1e551)' has a CIDR of 10.0.0.0/16. The 'Regional pool us-west-1 (ipam-pool-0e0ed41b1a362ebc9)' has a CIDR of 10.0.0.0/18. The table has columns for Name (Pool ID), Description, and Provisioned CIDRs.

Name (Pool ID)	Description	Provisioned CIDRs
Global pool (ipam-pool-06fb4cace4bc1e551)	-	10.0.0.0/16
Regional pool us-west-1 (ipam-pool-0e0ed41b1a362ebc9)	-	10.0.0.0/18

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 :



The screenshot shows the 'Pools' section of the IP Address Manager. It displays three pools under the scope 'ipam-scope-0a158dde35c51107b'. The 'Global pool (ipam-pool-06fb4cace4bc1e551)' has a CIDR of 10.0.0.0/16. The 'Regional pool us-west-1 (ipam-pool-0e0ed41b1a362ebc9)' has a CIDR of 10.0.0.0/18. The 'Regional pool us-west-2 (ipam-pool-0d21e78124564dbb6)' has a CIDR of 10.0.64.0/18. The table has columns for Name (Pool ID), Description, and Provisioned CIDRs.

Name (Pool ID)	Description	Provisioned CIDRs
Global pool (ipam-pool-06fb4cace4bc1e551)	-	10.0.0.0/16
Regional pool us-west-1 (ipam-pool-0e0ed41b1a362ebc9)	-	10.0.0.0/18
Regional pool us-west-2 (ipam-pool-0d21e78124564dbb6)	-	10.0.64.0/18

## 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.

## Create pool in ipam-scope-0cbdc40f8f04fa968

### Pool settings

**Name (IPAM ID)****DemolPAM (ipam-080d0c4b98089b437)****Name (Scope ID)****ipam-scope-0cbdc40f8f04fa968****Name tag - optional**

Creates a tag with a key of 'Name' and a value that you specify. Tags are not visible to other accounts even if a pool is shared.

**Pre-prod pool****Description - optional**

Write a brief description for the pool.

**My pool for VPCs**

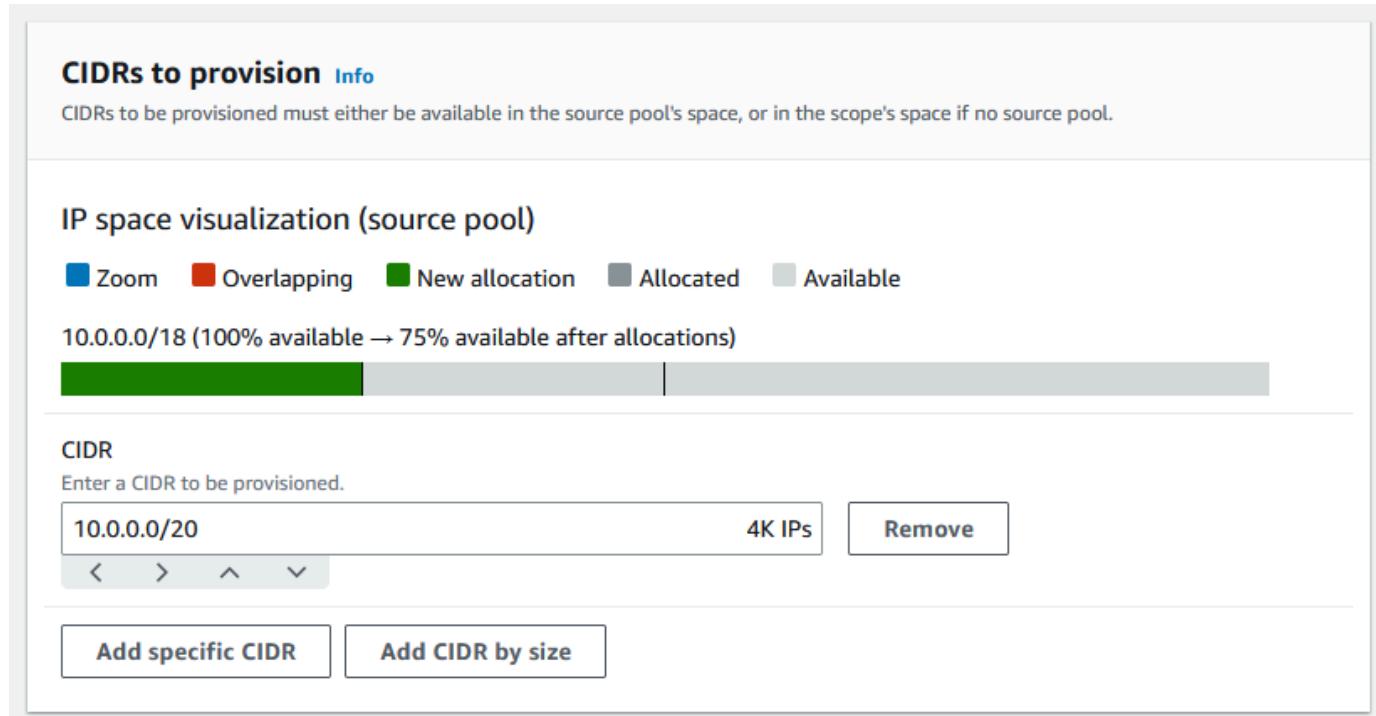
### Pool hierarchy Info

**Source pool**

To provision a CIDR into this pool, it must be available in the source pool. If no source pool is selected, then the space must be available in the scope.

**Regional pool us-west-1 (ipam-pool-03b74e706bb0df4ab)****▼ Source pool summary****Name (Pool ID)****Regional pool us-west-1 (ipam-pool-03b74e706bb0df4ab)****Provisioned CIDRs****10.0.0.0/18****Description****-****Locale****us-west-1**

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.

## Allocation rule settings - *optional* Info



### AWS best practice

We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize IPAM pools, see [Example IPAM pool plans](#).

- Configure this pool's allocation rule settings

## CIDR management

### Automatically import discovered resources

It is recommended to allow automatic import if this pool will be used to allocate CIDRs to resources such as VPCs.

- Allow automatic import  
 Don't allow

## Netmask compliancy

### Minimum netmask length

The minimum netmask length for allocating resources within the pool.

/24 (256 IPs)



### Default netmask length

The default netmask length used when IPAM allocates a CIDR from this pool to a resource.

/24 (256 IPs)



### Maximum netmask length

The maximum netmask length for allocating resources within the pool.

/24 (256 IPs)



## Tag compliancy

### Tagging requirements

Add tagging requirements for resources in this pool.

Key

environment

Value - *optional*

pre-prod



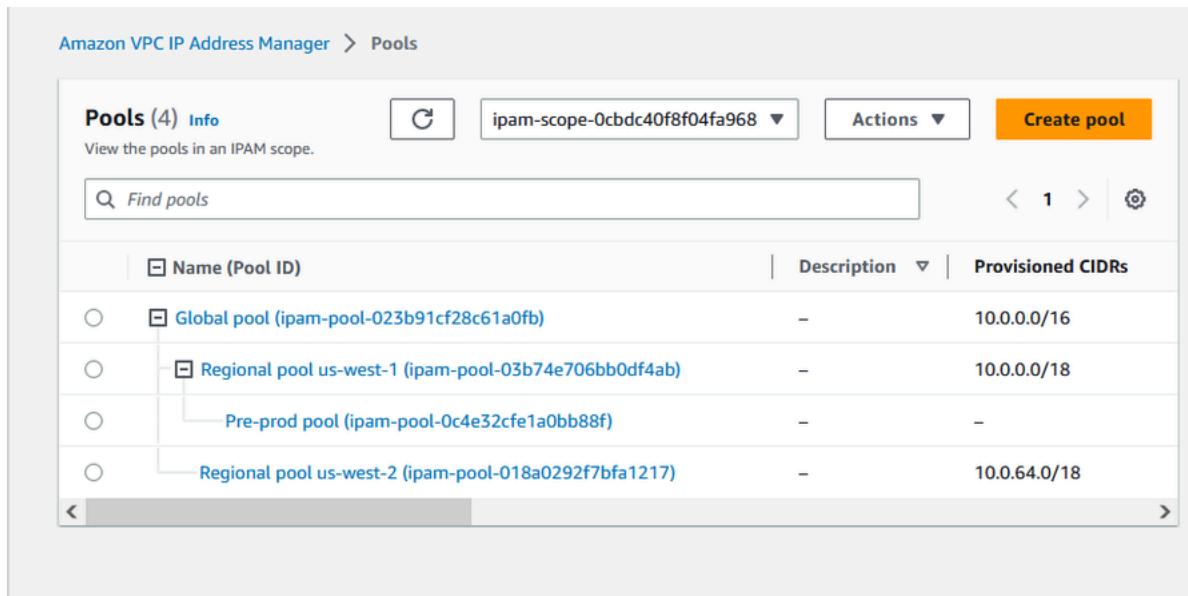
Remove

Add new required tag

You can add up to 49 more tags.

## 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 :



The screenshot shows the 'Pools' page in the Amazon VPC IP Address Manager. At the top, there are buttons for 'Info', 'Actions', and 'Create pool'. A dropdown menu shows 'ipam-scope-0cbdc40f8f04fa968'. The main table lists four pools:

Name (Pool ID)	Description	Provisioned CIDRs
Global pool (ipam-pool-023b91cf28c61a0fb)	-	10.0.0.0/16
Regional pool us-west-1 (ipam-pool-03b74e706bb0df4ab)	-	10.0.0.0/18
Pre-prod pool (ipam-pool-0c4e32cfe1a0bb88f)	-	-
Regional pool us-west-2 (ipam-pool-018a0292f7bfa1217)	-	10.0.64.0/18

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 :

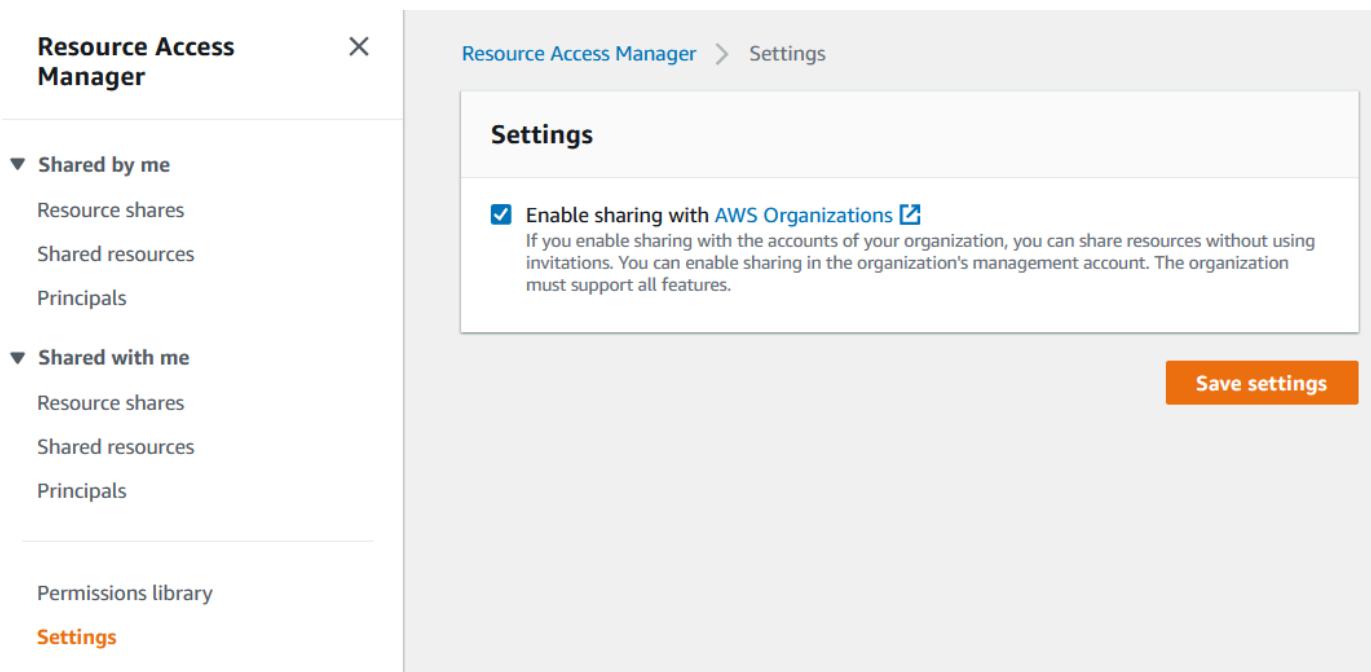
- [Étape 6.1. Activer le partage des ressources dans AWS RAM](#) : cette étape doit être réalisée par le compte de gestion AWS Organizations.
- [Étape 6.2. Partager d'un groupe IPAM à l'aide de AWS RAM](#) : cette étape doit être réalisée par l'administrateur IPAM.

### 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.

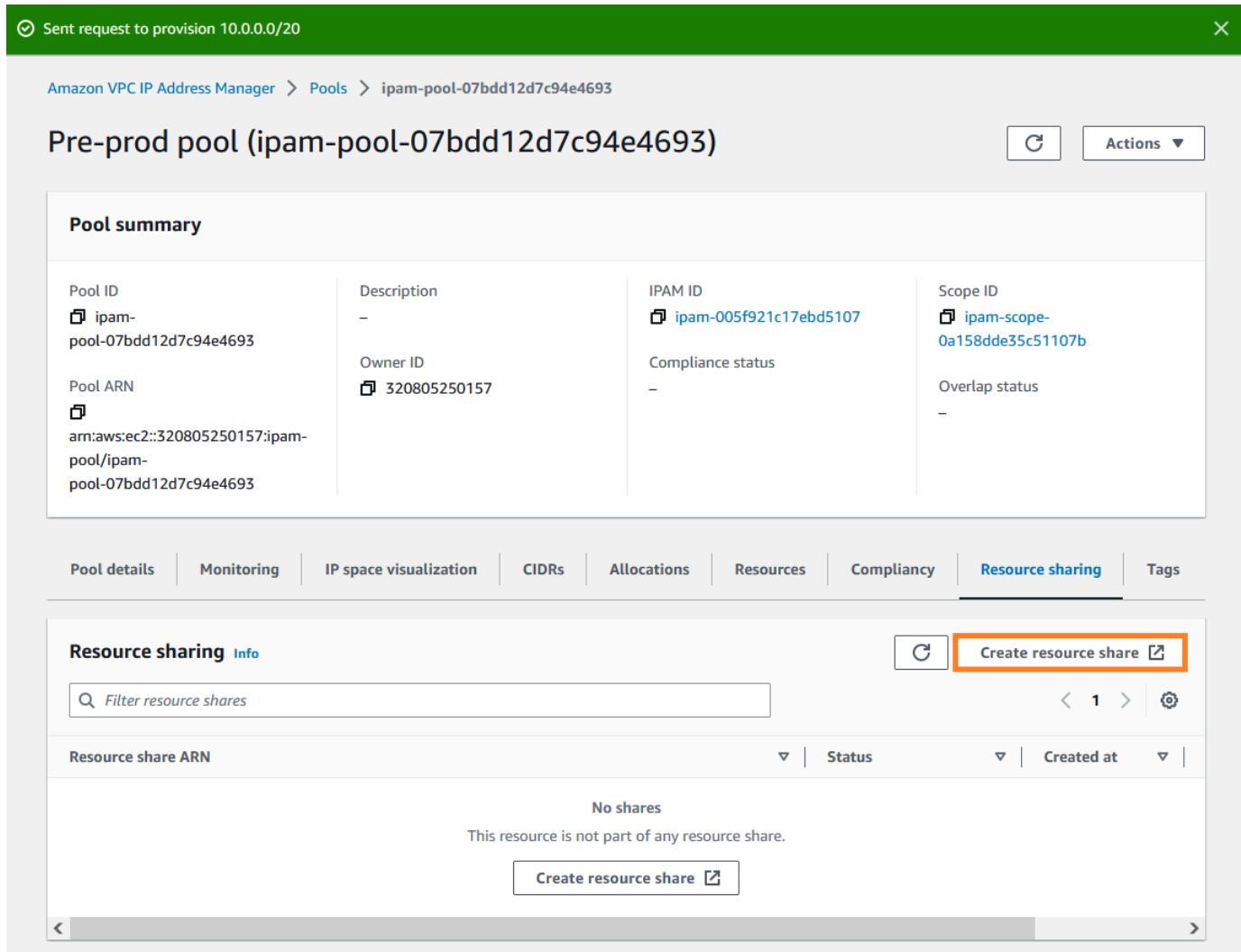
## Étape 6.2. Partager d'un groupe IPAM à l'aide de AWS RAM

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, sélectionnez 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).



The screenshot shows the AWS IP Address Manager interface. At the top, a green banner indicates a successful request to provision a resource share. Below this, the page title is "Pre-prod pool (ipam-pool-07bdd12d7c94e4693)". The main content area is titled "Pool summary" and displays the following details:

Pool ID	Description	IPAM ID	Scope ID
ipam-pool-07bdd12d7c94e4693	-	ipam-005f921c17ebd5107	ipam-scope-0a158dde35c51107b
Pool ARN	Owner ID	Compliance status	Overlap status
arn:aws:ec2::320805250157:ipam-pool/ipam-pool-07bdd12d7c94e4693	320805250157	-	-

Below the summary, a navigation bar includes tabs for "Pool details", "Monitoring", "IP space visualization", "CIDRs", "Allocations", "Resources", "Compliance", "Resource sharing" (which is highlighted in blue), and "Tags".

The "Resource sharing" section shows a table with one row, indicating "No shares". A message states "This resource is not part of any resource share." A "Create resource share" button is located at the bottom of this section.

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.

## Specify resource share details

Enter a name for the resource share and select the resources that you want to share.

### Resource share name

#### Name

Provide a descriptive name for the resource share.

### Resources - optional

Choose the resources to add to the resource share.

#### Select resource type

< 1 >

#### ARN

#### Locale

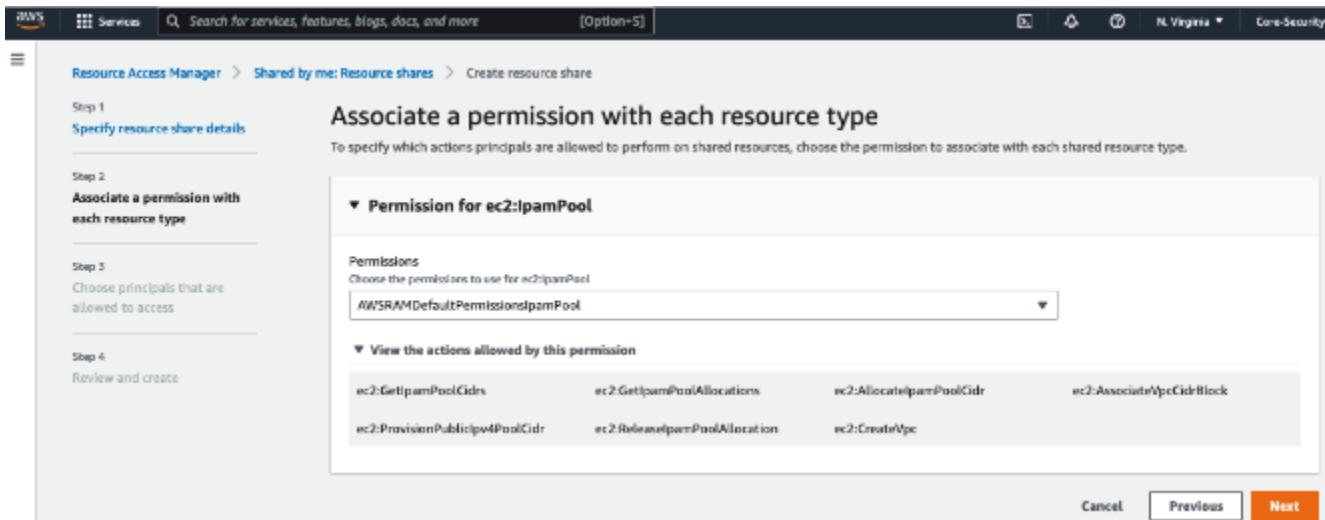
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-06fb4cace4bc1e551	None
<input checked="" type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-07bdd12d7c94e4693	us-west-1
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-0b8123821c7ef5319	us-east-1
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-0d21e78124564dbb6	us-west-2
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-0e0ed41b1a362ebc9	us-west-1

### Selected resources (1)

[Deselect](#)

<input type="checkbox"/>	Resource ID	Resource Type
<input type="checkbox"/>	ipam-pool-07bdd12d7c94e4693	ec2:IpamPool

9. Choisissez 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](#).



The screenshot shows the AWS Resource Access Manager interface. The top navigation bar includes the AWS logo, 'Services', a search bar, and 'IP Address Manager'. The main content area is titled 'Associate a permission with each resource type'. On the left, a sidebar lists 'Step 1: Specify resource share details', 'Step 2: Associate a permission with each resource type' (which is currently selected), and 'Step 3: Choose principals that are allowed to access'. The main panel shows a section for 'ec2:ipamPool' with a dropdown menu containing 'AWSRAMDefaultPermissions:ipamPool'. Below this, a table lists six actions: 'ec2:DescribeIpamPoolCidr', 'ec2:AllocateIpamPoolAllocation', 'ec2:AssociateIpamPoolAllocation', 'ec2:CreateVpc', 'ec2:ProvisionPublicIpv4PoolCidr', and 'ec2:ReleaseIpamPoolAllocation'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

11. Choisissez 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.

## Grant access to principals

Specify the principals that are allowed access to the shared resources. A principal can be any of the following: An entire organization or organizational unit (OU) in AWS Organizations, an AWS account, IAM role, or IAM user.

### Principals - *optional*

Allow sharing with anyone

You can share resources with any AWS accounts, roles, and users. If you are in an organization, you can also share with the entire organization or organizational units in that organization.

Allow sharing only within your organization

You can share resources with the entire organization, organizational units, or AWS accounts, roles, and users in that organization.

#### Principals

You can add multiple principals of different types.

Organizational unit (OU)

ou-fssg-q5brfv9c

Organizational unit ID format: ou-{4-32 characters}-{8-32 characters}.

Add

#### Selected principals (0)

The following principals will be allowed access to the shared resources.

Deselect

	Principal ID	Type
No selected principals.		

Cancel

Previous

Next

13. Choisissez 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'OU 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. À l'aide du 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.

VPC > Your VPCs > Create VPC

## Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

### VPC settings

Resources to create Info  
Create only the VPC resource or the VPC and other networking resources.

VPC only  VPC and more

Name tag - *optional*  
Creates a tag with a key of 'Name' and a value that you specify.  
Example VPC

IPv4 CIDR block Info  
 IPv4 CIDR manual input  IPAM-allocated IPv4 CIDR block

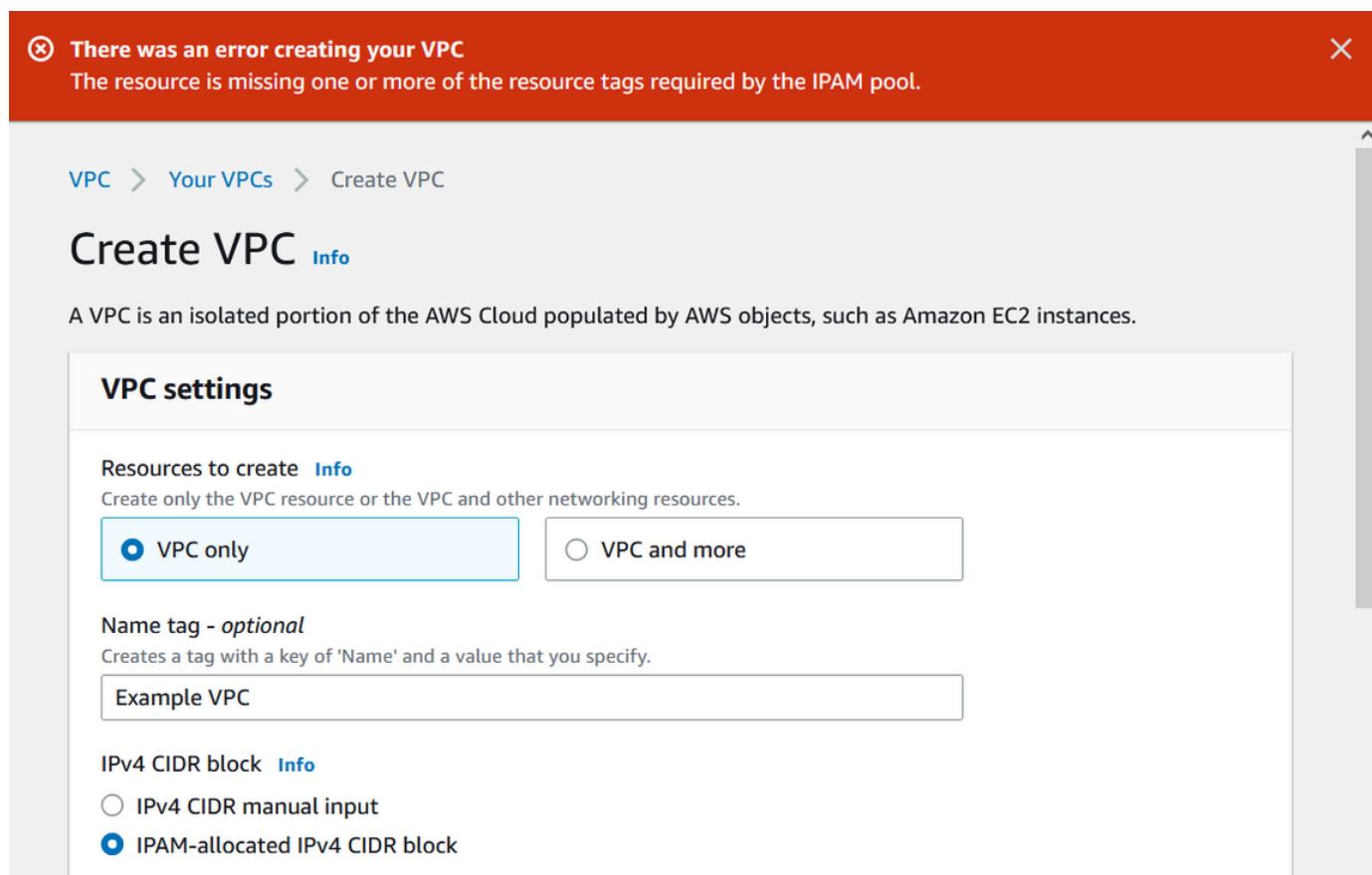
IPv4 IPAM pool  
ipam-pool-0c4e32cf1a0bb88f  
us-west-1

The locale of the IPAM pool must be equal to the current region.

Netmask  
/24 (allowed maximum) 256 IPs ▾

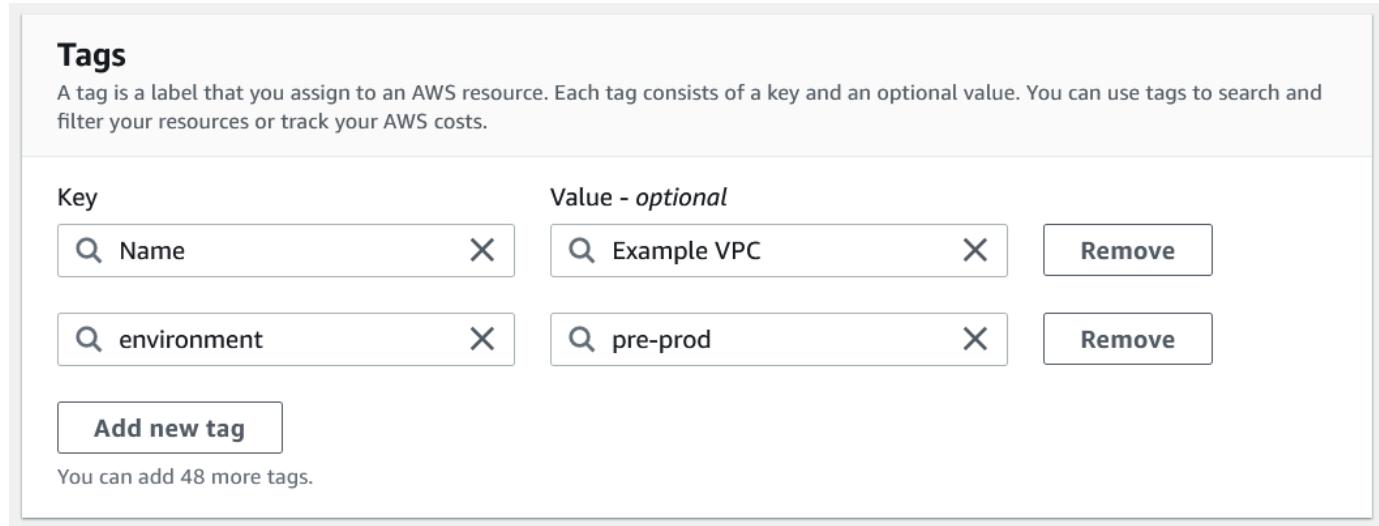
- À des fins de démonstration, sous Balises, n'ajoutez aucune balise supplémentaire pour le moment. Lorsque vous avez créé le groupe de préproduction (dans [Étape 5 : création d'un groupe de développement de pré-production](#)), vous avez ajouté une règle d'allocation qui exigeait que tous les VPC créés 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.
- Sélectionnez Create VPC (Créer un VPC).
- 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.



The screenshot shows the 'Create VPC' wizard. At the top, a red error box states: 'There was an error creating your VPC' and 'The resource is missing one or more of the resource tags required by the IPAM pool.' Below the error, the breadcrumb navigation shows 'VPC > Your VPCs > Create VPC'. The main section is titled 'Create VPC' with an 'Info' link. A description states: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' The 'VPC settings' section includes 'Resources to create' (radio buttons for 'VPC only' and 'VPC and more', with 'VPC only' selected), a 'Name tag - optional' input field containing 'Example VPC', and an 'IPv4 CIDR block' section with radio buttons for 'IPv4 CIDR manual input' and 'IPAM-allocated IPv4 CIDR block', with 'IPAM-allocated IPv4 CIDR block' selected.

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



The screenshot shows the 'Tags' configuration page. It defines a tag as a label assigned to an AWS resource, consisting of a key and an optional value. It allows searching and filtering resources or tracking AWS costs. The table shows two existing tags: 'Name' with value 'Example VPC' and 'environment' with value 'pre-prod'. There is a 'Remove' button for each tag and an 'Add new tag' button. A note indicates 48 more tags can be added.

Key	Value - optional	Remove
Name	Example VPC	Remove
environment	pre-prod	Remove

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

✓ You successfully created **vpc-07701f4fcc6549b8d / Example VPC**

VPC > Your VPCs > vpc-07701f4fcc6549b8d

## vpc-07701f4fcc6549b8d / Example VPC

Actions ▾

### Details Info

VPC ID	State	DNS hostnames	DNS resolution
 <b>vpc-07701f4fcc6549b8d</b>	 <b>Available</b>	Disabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	<b>dopt-0b14c6b1ccb2338bb</b>	<b>rtb-0a89b32824730ec5c</b>	<b>acl-0dee4236e2f7502c8</b>
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR
No	<b>10.0.0.0/24</b>	–	–
Network Address Usage metrics	Route 53 Resolver DNS	Owner ID	
Disabled	Firewall rule groups	 <b>320805250157</b>	

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

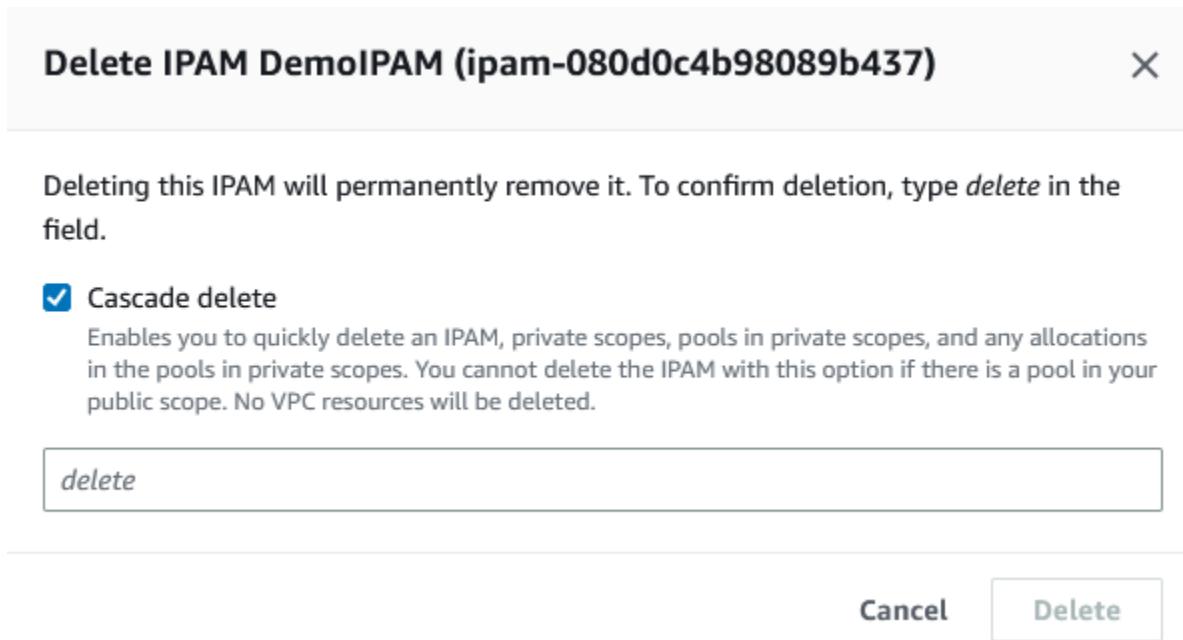
Dans ce didacticiel, vous avez créé un IPAM avec un administrateur délégué, créé plusieurs groupes et autorisé un compte membre de votre organisation à allouer un CIDR VPC à partir d'un groupe.

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 AWS 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, consultez [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 plus d'informations, consultez [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 [Intégration d'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 111111111111
```

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 plus d'informations, consultez [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 **--local** 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-0da89c821626f1e4b",  
      "ScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-scope-065e7dfe880df679c",  
      "ScopeType": "private",  
      "Arn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",  
      "Locale": "us-west-2",  

```

```
        "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-
fb525f6c2bf4e77a75690fc2d93479a",
        "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 [Intégration d'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, voir [Utilisation de AWS CLI](#) dans le AWS Guide 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 de l'AWS Région 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, voir [Afficher 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 autres AWS services), 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": "network-interface",  
      "ResourceId": "eni-0b4e53eb1733aba16",  
      "ResourceCidr": "10.0.0.176/32",  
      "VpcId": "vpc-0f5ee7e1ba908a378",  
      "SampledStartTime": "2021-12-27T20:08:46.672000+00:00",  
      "SampledEndTime": null  
    },  
    {  
      "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",  
      "SampledEndTime": null  
    }  
  ]  
}
```

```
{
    "ResourceOwnerId": "123456789012",
    "ResourceRegion": "us-east-1",
    "ResourceType": "subnet",
    "ResourceId": "subnet-0864c82a42f5bfffed",
    "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-0a8347f594bea5901"
  }
]
```

```
        "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 /24 sont retournés, pas tous /32 au sein du /24 CIDR. 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-0864c82a42f5bfffed",  
      "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 approuvées et des numéros de système autonome (ASN) que vos partenaires ou clients ont autorisés sur leur réseau, vous pouvez exécuter ces applications dans 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.

Apportez votre propre numéro de système autonome (BYOASN) vous permet de publier les adresses IPv4 ou IPv6 que vous apportez à 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'ASN AWS 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 suppose que vous possédez l'ASN public que vous souhaitez apporter à l'IPAM et que vous avez déjà apporté un CIDR BYOIP à AWS et l'avez provisionné dans un groupe dans votre portée publique. 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 ASN AWS, mais vous êtes limité à passer d'un ASN AWS 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 avec [Didacticiel : apporter vos adresses IP à IPAM](#), vous avez besoin de la plage d'adresses IP CIDR. 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 dans AWS, ou vous pouvez créer une nouvelle clé privée comme décrit dans la section [Create a private key and generate an X.509 certificate](#) du Guide d'utilisation d'Amazon EC2.
- Lorsque vous apportez une plage d'adresses IPv4 ou IPv6 à AWS avec [Didacticiel : apporter vos adresses IP à IPAM](#), vous [créez un certificat X.509](#) et vous [chargez ce certificat X.509 dans le registre 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](mailto: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.
- Lorsque vous apportez une plage d'adresses IP à IPAM, vous créez un ROA pour vérifier que vous contrôlez l'espace d'adresses IP que vous apportez à IPAM. En plus de ce ROA, vous devez avoir un deuxième ROA dans votre RIR avec l'ASN que vous apportez à IPAM. Si vous n'avez pas ce deuxième ROA pour l'ASN dans votre RIR, complétez [3. Créez un objet ROA dans votre RIR](#). Ignorez les autres étapes.

## Étapes du didacticiel

Effectuez les étapes ci-dessous à l'aide de la console AWS ou de la 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 compte AWS, ASN est l'ASN que vous apportez à IPAM et AAAAMMJJ 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. Signer 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 provisionner 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 BYOASNs associés, choisissez l'ASN que vous avez apporté à 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, le ProvisionStatus devrait être défini sur 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 publié, vous devez appeler `advertise-byoip-cidr` avec la valeur spéciale `AWS` 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 répartir votre public IPs entre les régions vers des ressources telles que des EC2 instances et des équilibreurs de charge d'applications. Sans l'IPAM, vous devez intégrer votre public IPs pour chaque AWS région.

### Table des matières

- [Vérification du contrôle du domaine](#)
- [Apporter votre propre IP à IPAM en utilisant à la fois la console de gestion AWS et l'AWS CLI](#)
- [Apportez votre propre CIDR IP sur IPAM en utilisant uniquement la AWSCLI](#)

- [Utilisez votre propre adresse IP pour CloudFront utiliser IPAM](#)

## Vérification du contrôle du domaine

Avant de transférer une plage d'adresses IP à AWS, vous devez utiliser l'une des options décrites dans cette section pour vérifier que vous contrôlez l'espace d'adresses IP. Plus tard, lorsque vous amenez la plage d'adresses IP à AWS, cela AWS confirme que vous contrôlez la plage d'adresses IP. Cette validation empêche les clients d'utiliser des plages d'adresses IP appartenant à d'autres, ce qui permet d'éviter les problèmes de routage et de sécurité.

Il existe deux méthodes pour vérifier que vous contrôlez la plage :

- Certificat X.509 : si votre plage d'adresses IP est enregistrée auprès d'un registre Internet qui prend en charge le protocole RDAP (tel que ARIN, RIPE et APNIC), vous pouvez utiliser un certificat X.509 pour vérifier la propriété de votre domaine.
- Enregistrement DNS TXT : que votre registre Internet prenne en charge le protocole RDAP ou non, vous pouvez utiliser un jeton de vérification et un enregistrement DNS TXT pour vérifier la propriété de votre domaine.

### Table des matières

- [Vérifiez votre domaine avec un certificat X.509](#)
- [Vérifiez votre domaine à l'aide d'un enregistrement DNS TXT](#)

### Vérifiez votre domaine avec un certificat X.509

Cette section explique comment vérifier votre domaine à l'aide d'un certificat X.509 avant de transférer votre plage d'adresses IP à IPAM.

#### Vérification de votre domaine avec un certificat X.509

1. Suivez les trois étapes décrites dans la section [Prérequis pour le BYOIP sur Amazon dans EC2 le guide](#) de l'utilisateur Amazon EC2 .

 Note

Lorsque vous créez le ROAs, pour, IPv4 CIDRs vous devez définir la longueur maximale d'un préfixe d'adresse IP sur/24. En IPv6 CIDRs effet, si vous les ajoutez à un pool

publicitaire, la longueur maximale d'un préfixe d'adresse IP doit être de /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 qu'il /24 s'agit du plus petit IPv4 bloc et /48 du plus petit IPv6 bloc que vous pouvez annoncer depuis une région sur Internet.

- Effectuez les étapes 1 et 2 uniquement dans la [section Proposer une plage d'adresses pouvant faire l'objet d'une publicité publique AWS dans](#) le Guide de EC2 l'utilisateur Amazon, et ne fournissez pas encore la plage d'adresses (étape 3). Enregistrez le `text_message` et `signed_message`. Vous en aurez besoin plus tard dans ce processus.

Lorsque vous avez terminé ces étapes, continuez avec [Apporter votre propre IP à IPAM en utilisant à la fois la console de gestion AWS et l'AWS CLI](#) ou [Apportez votre propre CIDR IP sur IPAM en utilisant uniquement laAWSCLI](#).

## Vérifiez votre domaine à l'aide d'un enregistrement DNS TXT

Suivez les étapes décrites dans cette section pour vérifier votre domaine à l'aide d'un enregistrement DNS TXT avant de transférer votre plage d'adresses IP à IPAM.

Vous pouvez utiliser les enregistrements DNS TXT pour vérifier que vous contrôlez une plage d'adresses IP publiques. Les enregistrements DNS TXT sont un type d'enregistrement DNS qui contient des informations sur votre nom de domaine. Cette fonctionnalité vous permet d'importer les adresses IP enregistrées dans n'importe quel registre Internet (tel que JPNIC, LACNIC et AFRINIC), et pas seulement celles qui prennent en charge les validations basées sur des enregistrements RDAP (Registration Data Access Protocol) (telles que ARIN, RIPE et APNIC).

### Important

Avant de pouvoir continuer, vous devez avoir créé un IPAM dans le niveau gratuit ou avancé. Si vous n'avez pas d'IPAM, complétez [Création d'un IPAM](#) d'abord.

## Table des matières

- [Étape 1 : créer une ROA si vous n'en avez pas](#)
- [Étape 2. Créez un jeton de vérification](#)
- [Étape 3. Configuration de la zone DNS et de l'enregistrement TXT](#)

### Étape 1 : créer une ROA si vous n'en avez pas

Vous devez disposer d'une autorisation d'origine d'éitinéraire (ROA) dans votre registre Internet régional (RIR) pour les plages d'adresses IP que vous souhaitez promouvoir. Si vous n'avez pas de ROA dans votre RIR, complétez [3. Créez un objet ROA dans votre RIR](#) dans le guide de l' EC2 utilisateur Amazon. Ignorez les autres étapes.

La plage d' IPv4 adresses la plus précise que vous pouvez apporter est /24. La plage d' IPv6 adresses la plus précise que vous pouvez apporter est /48 pour celles CIDRs qui sont publiables et /60 pour celles CIDRs qui ne le sont pas.

### Étape 2. Créez un jeton de vérification

Un jeton de vérification est une valeur aléatoire AWS générée que vous pouvez utiliser pour prouver le contrôle d'une ressource externe. Par exemple, vous pouvez utiliser un jeton de vérification pour vérifier que vous contrôlez une plage d'adresses IP publiques lorsque vous transmettez une plage d'adresses IP à AWS (BYOIP).

Suivez les étapes décrites dans cette section pour créer un jeton de vérification dont vous aurez besoin ultérieurement dans ce tutoriel pour transférer votre plage d'adresses IP vers IPAM. Suivez les instructions ci-dessous pour la AWS console ou le AWS CLI.

#### AWS Management Console

##### Création d'un jeton de vérification

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans la console AWS de gestion, choisissez la AWS région dans laquelle vous avez créé votre IPAM.
3. Dans le panneau de navigation de gauche, choisissez IPAMs.
4. Choisissez votre IPAM, puis cliquez sur l'onglet Jetons de vérification.
5. Sélectionnez Créez un jeton de vérification.

- Après avoir créé le jeton, laissez cet onglet de navigateur ouvert. Vous aurez besoin de la valeur du jeton, du nom du jeton à l'étape suivante et de l'identifiant du jeton à une étape ultérieure.

Notez ce qui suit :

- Une fois que vous avez créé un jeton de vérification, vous pouvez le réutiliser pour plusieurs BYOIP CIDRs que vous fournissez depuis votre IPAM dans les 72 heures. Si vous souhaitez en approvisionner davantage CIDRs après 72 heures, vous avez besoin d'un nouveau jeton.
- Vous pouvez créer jusqu'à 100 jetons. Si vous atteignez cette limite, supprimez les jetons expirés.

## Command line

- Demandez à l'IPAM de créer un jeton de vérification que vous utiliserez pour la configuration DNS avec [create-ipam-external-resource-verification-token](#) :

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

Cela renverra un jeton IpamExternalResourceVerificationTokenId et avec TokenName etTokenValue, ainsi que le délai d'expiration (NotAfter) du jeton.

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

Notez ce qui suit :

- Une fois que vous avez créé un jeton de vérification, vous pouvez le réutiliser pour plusieurs BYOIP CIDRs que vous fournissez depuis votre IPAM dans les 72 heures. Si vous souhaitez en approvisionner davantage CIDRs après 72 heures, vous avez besoin d'un nouveau jeton.
- Vous pouvez consulter vos jetons à l'aide de [describe-ipam-external-resource-verification-tokens](#).
- Vous pouvez créer jusqu'à 100 jetons. Si vous atteignez la limite, vous pouvez supprimer les jetons expirés à l'aide de [delete-ipam-external-resource-verification-token](#).

### Étape 3. Configuration de la zone DNS et de l'enregistrement TXT

Effectuez les étapes décrites dans cette section pour configurer la zone DNS et l'enregistrement TXT. Si vous n'utilisez pas Route53 comme DNS, suivez la documentation fournie par votre fournisseur DNS pour configurer une zone DNS et ajouter un enregistrement TXT.

Si vous utilisez Route53, prenez les éléments suivants en considération :

- Pour créer une zone de recherche inversée dans la AWS console, consultez la section [Création d'une zone hébergée publique](#) dans le guide du développeur Amazon Route 53 ou utilisez la AWS CLI commande [create-hosted-zone](#).
- Pour créer un enregistrement dans la zone de recherche inversée de la AWS console, consultez la section [Création d'enregistrements à l'aide de la console Amazon Route 53](#) dans le manuel du développeur Amazon Route 53 ou utilisez la AWS CLI commande [change-resource-record-sets](#).
- Une fois que vous avez créé votre zone hébergée, déléguez la zone hébergée de votre RIR aux serveurs de noms fournis par Route53 (par exemple pour [LACNIC](#) ou [APNIC](#)).

Que vous utilisez un autre fournisseur DNS ou Route53, tenez compte des points suivants lorsque vous configurez l'enregistrement TXT :

- Le nom de l'enregistrement doit être le nom de votre jeton.
- Le type d'enregistrement doit être TXT.
- ResourceRecord La valeur doit être la valeur du jeton.

Exemple :

- Nom: 86950620.113.0.203.in-addr.arpa
- Type : TXT

- ResourceRecords Value (Valeur) : a34597c3-5317-4238-9ce7-50da5b6e6dc8

Où :

- 86950620 est le nom du jeton de vérification.
- 113.0.203.in-addr.arpa est le nom de la zone de recherche inversée.
- TXT est le type d'enregistrement.
- a34597c3-5317-4238-9ce7-50da5b6e6dc8 est la valeur du jeton de vérification.

### Note

En fonction de la taille du préfixe à apporter à IPAM avec BYOIP, un ou plusieurs enregistrements d'authentification doivent être créés dans le DNS. Ces enregistrements d'authentification sont de type TXT et doivent être placés dans la zone inverse du préfixe lui-même ou de son préfixe parent.

- En effet IPv4, les enregistrements d'authentification doivent s'aligner sur les plages situées à la limite d'un octet qui constitue le préfixe.
  - Exemples
    - Pour 198.18.123.0/24, qui est déjà aligné à la limite d'un octet, vous devez créer un enregistrement d'authentification unique à l'adresse suivante :
      - *token-name.123.18.198.in-addr.arpa. IN TXT "token-value"*
    - Pour 198.18.12.0/22, qui lui-même n'est pas aligné sur la limite des octets, vous devez créer quatre enregistrements d'authentification. Ces enregistrements doivent couvrir les sous-réseaux 198.18.12.0/24, 198.18.13.0/24, 198.18.14.0/24 et 198.18.15.0/24 qui sont alignés à la limite d'un octet. Les entrées DNS correspondantes doivent être :
      - *token-name.12.18.198.in-addr.arpa. IN TXT "token-value"*
      - *token-name.13.18.198.in-addr.arpa. IN TXT "token-value"*
      - *token-name.14.18.198.in-addr.arpa. IN TXT "token-value"*
      - *token-name.15.18.198.in-addr.arpa. IN TXT "token-value"*
    - Pour 198.18.0.0/16, qui est déjà aligné à la limite d'un octet, vous devez créer un enregistrement d'authentification unique :
      - *token-name.18.198.in-addr.arpa. IN TXT "token-value"*

- En effet IPv6, les enregistrements d'authentification doivent s'aligner sur les plages situées à la limite du nibble qui constituent le préfixe. Les valeurs de nibble valides sont par exemple 32, 36, 40, 44, 48, 52, 56 et 60.
- Exemples
  - Pour 2001:0db8::/40, qui est déjà aligné à la limite de nibble, vous devez créer un enregistrement d'authentification unique :
    - *token-name.0.0.8.b.d.0.1.0.0.2.ip6.arpa* TXT "*token-value*"
  - Pour 2001:0db8:80::/42, qui n'est pas alignée à la limite de nibble, vous devez créer quatre enregistrements d'authentification. Ces enregistrements doivent couvrir les sous-réseaux 2001:db8:80::/44, 2001:db8:90::/44, 2001:db8:a0::/44, et 2001:db8:b0::/44 qui sont alignés sur une limite de nibble. Les entrées DNS correspondantes doivent être :
    - *token-name.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa* TXT "*token-value*"
    - *token-name.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa* TXT "*token-value*"
    - *token-name.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa* IN TXT "*token-value*"
    - *token-name.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa* IN TXT "*token-value*"
  - Pour la plage non annoncée 2001:db8:0:1000::/54, qui n'est elle-même pas alignée à une limite de nibble, vous devez créer quatre enregistrements d'authentification. Ces enregistrements doivent couvrir les sous-réseaux 2001:db8:0:1000::/56, 2001:db8:0:1100::/56, 2001:db8:0:1200::/56 et 2001:db8:0:1300::/56 qui sont alignés à une limite de nibble. Les entrées DNS correspondantes doivent être :
    - *token-name.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa* IN TXT "*token-value*"
    - *token-name.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa* IN TXT "*token-value*"
    - *token-name.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa* IN TXT "*token-value*"
    - *token-name.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa* IN TXT "*token-value*"
  - Pour valider le nombre correct de nombres hexadécimaux entre le nom du jeton et la chaîne « ip6.arpa », multipliez le nombre par quatre. Le résultat doit correspondre à la longueur du préfixe. Par exemple, pour un préfixe /56, vous devez avoir 14 chiffres hexadécimaux.

Lorsque vous avez terminé ces étapes, continuez avec [Apporter votre propre IP à IPAM en utilisant à la fois la console de gestion AWS et l'AWS CLI](#) ou [Apportez votre propre CIDR IP sur IPAM en utilisant uniquement la AWSCLI](#).

## Apporter votre propre IP à IPAM en utilisant à la fois la console de gestion AWS et l'AWS CLI

Intégrer votre propre adresse IP (BYOIP) à IPAM vous permet d'utiliser les plages d'adresses IPv4 et IPv6 existantes de votre organisation dans AWS. Vous pouvez ainsi maintenir une image de marque cohérente, améliorer les performances du réseau, renforcer la sécurité et simplifier la gestion en unifiant les environnements sur site et en nuage sous votre propre espace d'adresses IP.

Suivez ces étapes pour apporter un CIDR IPv4 ou IPv6 à IPAM à l'aide du AWS console de gestion et de la AWSCLI.

### Note

Avant de commencer, vous devez disposer d'un [contrôle de domaine vérifié](#).

Une fois que vous avez apporté une plage d'adresses IPv4 vers 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 IPv4 CIDR 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 AWSConsole de gestion](#)

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

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

### Important

- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :

- [Intégration d'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 dans [Intégration d'IPAM aux comptes d'une organisation AWS.](#) Dans ce tutoriel, ce compte sera appelé compte IPAM.
  - Le compte membre de votre organisation qui sera alloué CIDRs à partir d'un pool 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 : publication du CIDR](#)
- [Étape 5. Partager le groupe régional](#)
- [Étape 6 : allocation d'une adresse IP Elastic à partir du groupe](#)
- [Étape 7 : associer l'adresse IP élastique à une EC2 instance](#)
- [Étape 8 : nettoyage](#)
- [Alternative à l'étape 6](#)

## 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 le AWS CLI](#)

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 sera alloué CIDRs 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'--profileoption 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 <https://console.aws.amazon.com/ipam/> l'adresse.
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. Sous Famille d'adresses, sélectionnez IPv4.
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 Locale (paramètre régional), choisissez Aucun.

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, choisissez BYOIP.
11. Sous CIDRs provision, effectuez l'une des opérations suivantes :

- Si vous avez [vérifié le contrôle de votre domaine à l'aide d'un certificat X.509](#), vous devez inclure le CIDR, le message BYOIP et la signature du certificat que vous avez créés lors de cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.
- Si vous avez [vérifié le contrôle de votre domaine avec un enregistrement DNS TXT](#), vous devez inclure le jeton de vérification CIDR et IPAM que vous avez créé dans cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.

Notez que lors du provisionnement d'un IPv4 CIDR vers un pool au sein du pool de niveau supérieur, le IPv4 CIDR minimum que vous pouvez provisionner est le suivant /24 ; les informations plus spécifiques CIDRs (telles que/25) ne sont pas autorisées.

 Important

Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'allocation des plages qui peuvent être annoncées publiquement peut durer jusqu'à une semaine.

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 du provisionnement dans l'CIDR songlet de la page de détails du pool.

### 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 Local doit faire partie de l'une des régions d'exploitation que vous avez configurées lorsque vous avez créé l'IPAM. Par exemple, un paramètre régional us-east-1 signifie que us-east-1 doit être une région opérationnelle pour l'IPAM. Une paramètre régional us-east-1-scl-1 (un groupe frontalier de réseau utilisé pour les zones locales) signifie que l'IPAM doit avoir une région opérationnelle us-east-1.

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 <https://console.aws.amazon.com/ipam/> l'adresse.
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.

Les paramètres régionaux du groupe doivent être l'une des options suivantes :

- AWS Région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour des allocations.
- Le groupe de bordure du réseau pour une zone AWS locale dans laquelle vous souhaitez que ce pool IPAM soit disponible pour des allocations ([zones locales prises en charge](#)). Cette option n'est disponible que pour les IPv4 pools IPAM du périmètre public.
- Une [zone locale AWS dédiée](#). Pour créer un pool dans une zone locale AWS dédiée, entrez la zone locale AWS dédiée dans l'entrée du sélecteur.
- Global lorsque vous souhaitez utiliser des adresses IP dans le monde entier dans toutes les AWS régions, telles que les CloudFront sites. La Global localisation n'est disponible que pour les IPv4 piscines publiques.

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 pool, 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, sélectionnez 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 le CIDRs montant alloué à partir de ce pool sera publicisé pour le EC2 service Amazon (pour les adresses IP élastiques) et le service Amazon VPC (pour les adresses associées à). CIDRs VPCs
10. Sous CIDRs provisionnement, choisissez un CIDR à provisionner pour le pool.

#### Note

Lorsque vous fournissez un CIDR à un pool régional au sein du pool de niveau supérieur, le IPv4 CIDR le plus spécifique que vous puissiez provisionner est le suivant /24 ; les informations plus spécifiques CIDRs (telles que/25) ne sont pas autorisées. Après avoir créé le groupe régional, vous pouvez créer des groupes plus petits (tels

que /25) au sein du même groupe régional. Notez que si vous partagez le groupe régional ou les groupes qu'il contient, ces groupes ne peuvent être utilisés que dans les paramètres régionaux définis sur le même groupe 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 du provisionnement dans l'CIDRsonglet de la page de détails du pool.

#### Étape 4 : 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 AWS et qui se trouve dans le pool sur lequel le EC2 Service (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.

##### Note

Le statut de la publicité ne limite pas votre capacité à attribuer des adresses IP Elastic. Même si votre BYOIPv4 CIDR n'est pas annoncé, vous pouvez toujours créer EIPs à partir du pool IPAM.

#### Pour publier le CIDR

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
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 CIDRs.
6. Sélectionnez le CIDR BYOIP et cliquez sur Actions >Publicité.
7. Cliquez sur Publicité CIDR.

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

#### Étape 5. 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. <https://console.aws.amazon.com/ipam/>
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez le périmètre privé, choisissez le groupe 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 Groupes IPAM, puis choisissez l'ARN du groupe 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 procéderiez 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. 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 6 : allocation d'une adresse IP Elastic à partir du groupe

Suivez les étapes de cette section pour allouer une adresse IP Elastic à partir du groupe. Notez que si vous utilisez des IPv4 pools publics pour allouer des adresses IP élastiques, vous pouvez utiliser les étapes alternatives [Alternative à l'étape 6](#) plutôt que celles de cette section.

### Important

Si vous voyez une erreur liée au fait que vous ne disposez pas des autorisations nécessaires pour appeler `ec2 :AllocateAddress`, l'autorisation gérée actuellement attribuée au pool IPAM qui a été partagé avec vous doit être mise à jour. Contactez la personne qui a créé le partage de ressources 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

Suivez les étapes décrites dans la [section Allouer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour attribuer l'adresse, mais notez ce qui suit :

- Cette étape doit être effectuée par le compte membre.
- Assurez-vous que la AWS région dans laquelle vous vous trouvez dans la EC2 console correspond à l'option locale que vous avez choisie lors de la création du pool régional.
- Lorsque vous choisissez le pool d'adresses, choisissez l'option Allouer à l'aide d'un pool IPv4 IPAM et choisissez le pool régional que vous avez créé.

## Command line

Allouez une adresse depuis le groupe à l'aide de la commande [allocate-address](#). L'option `--region` utilisée doit correspondre à l'option `-local` que vous avez choisie lors de la création du groupe à l'étape 2. Incluez l'ID du groupe IPAM que vous avez créé à l'étape 2 dans `--ipam-pool-id`. En option, vous pouvez également choisir un élément spécifique `/32` dans votre groupe IPAM en utilisant l'option `--address`.

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

Exemple de réponse :

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

Pour plus d'informations, consultez la section [Allocation d'une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon.

## Étape 7 : associer l'adresse IP élastique à une EC2 instance

Suivez les étapes décrites dans cette section pour associer l'adresse IP élastique à une EC2 instance.

### AWS Management Console

Suivez les étapes décrites dans [Associer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour attribuer une adresse IP élastique à partir du pool IPAM, mais notez ce qui suit : lorsque vous utilisez l'option AWS Management Console, la AWS région à laquelle vous associez l'adresse IP élastique doit correspondre à l'option locale que vous avez choisie lors de la création du pool régional.

Cette étape doit être effectuée par le compte membre.

### Command line

Cette étape doit être effectuée par le compte membre. Utilisez l'option **--profile member-account**.

Utilisez la commande [associate-address](#) pour associer une adresse IP Elastic à une instance. L'option **--region** à laquelle vous associez l'adresse IP Elastic doit correspondre à l'option **--locale** que vous avez choisie lors de la création du groupe régional.

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

Exemple de réponse :

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

Pour plus d'informations, consultez [Associer une adresse IP élastique à une instance ou à une interface réseau](#) dans le guide de EC2 l'utilisateur Amazon.

## Étape 8 : 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 <https://console.aws.amazon.com/ipam/> l'adresse.
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 CIDRs.
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' EC2 utilisateur Amazon 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 EC2 l'utilisateur Amazon pour libérer une adresse IP élastique (EIP) depuis le IPv4 pool public. Lorsque vous ouvrez EC2 dans la console de AWS gestion, la AWS région dans laquelle vous allouez l'EIP doit correspondre à l'Localeoption que vous avez choisie lors de la création du pool qui sera utilisé pour le CIDR BYOIP.

### Étape 4 : 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 5 : Déprovisionner le CIDRs pool régional et le pool 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.

- Effectuez les étapes [Pour désapprovisionner un CIDR de groupe](#) pour déprovisionner le CIDRs pool régional puis le pool de niveau supérieur, dans cet ordre.

### Étape 6 : 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 groupe](#) pour supprimer le groupe régional et ensuite le groupe de niveau supérieur, dans cet ordre.

## Alternative à l'étape 6

Si vous utilisez des IPv4 pools publics pour allouer des adresses IP élastiques, vous pouvez suivre les étapes de cette section plutôt que celles de la section précédente [Étape 6 : allocation d'une adresse IP Elastic à partir du groupe](#).

## Table des matières

- [Étape 1 : créer un IPv4 pool public](#)
- [Étape 2 : Fournir le IPv4 CIDR public à votre piscine publique IPv4](#)
- [Étape 3 : Allouer une adresse IP élastique depuis le IPv4 pool public](#)
- [Alternative au nettoyage de l'étape 6](#)

## Étape 1 : créer un IPv4 pool public

Cette étape doit être effectuée par le compte membre qui fournira une adresse IP élastique.

### Note

- Cette étape doit être effectuée par le compte membre en utilisant le AWS CLI.
- Les IPv4 pools publics et les pools IPAM sont gérés par des ressources distinctes dans AWS. Les IPv4 pools publics sont des ressources à compte unique qui vous permettent de convertir vos adresses IP publiques CIDRs en adresses IP élastiques. Les pools IPAM peuvent être utilisés pour allouer votre espace public à des IPv4 pools publics.

## Pour créer un IPv4 pool 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 le résultat, vous verrez l'ID du IPv4 pool public. Vous aurez besoin de cet ID à la prochaine étape.

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

## Étape 2 : Fournir le IPv4 CIDR public à votre piscine publique IPv4

Fournissez le IPv4 CIDR public à votre IPv4 pool 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 public. La valeur ne peut pas être supérieure à la longueur du masque réseau du groupe IPAM. Le `--netmask-length` le moins précis que vous puissiez définir 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.
- Cette étape doit être effectuée par le compte membre en utilisant le AWS CLI.

Pour créer un IPv4 pool 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 pool public IPv4 .

```
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 IPv4 pool public, pour afficher le IPv4 pool public alloué dans le pool régional IPAM, ouvrez la console IPAM et consultez l'allocation dans le pool régional sous **Allocations ou Ressources**.

## Étape 3 : Allouer une adresse IP élastique depuis le IPv4 pool public

Suivez les étapes décrites dans la [section Allouer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour attribuer une EIP depuis le IPv4 pool 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.

Une fois ces trois étapes terminées, revenez au tutoriel [Étape 7 : associer l'adresse IP élastique à une EC2 instance](#) et continuez jusqu'à ce que vous ayez terminé.

### Alternative au nettoyage de l'étape 6

Procédez comme suit pour nettoyer les IPv4 piscines publiques créées à l'aide de l'alternative à l'étape 9. Vous devez effectuer ces étapes après avoir publié l'adresse IP Elastic au cours du processus de nettoyage standard dans [Étape 8 : nettoyage](#).

## Étape 1 : Déprovisionner le IPv4 CIDR public de votre pool public IPv4

### ⚠️ Important

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

### 1. Consultez votre BYOIP CIDRs.

```
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 le CIDR du IPv4 pool public.

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

3. Consultez à CIDRs nouveau votre BYOIP et assurez-vous 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 le résultat, vous verrez le nombre d'adresses IP dans votre IPv4 pool public.

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

### Note

L'IPAM peut mettre un certain temps à découvrir que les allocations de IPv4 pool public 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 2 : Supprimer le IPv4 pool public

Cette étape doit être effectuée par le compte membre.

- Exécutez la commande suivante pour supprimer le IPv4 pool public, 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. 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.

## Apportez votre propre CIDR IPv6 sur IPAM à l'aide du AWSConsole de gestion

Suivez les étapes de ce didacticiel pour apporter un CIDR IPv6 à IPAM et allouer un VPC avec le CIDR à l'aide de la Console de gestion AWS et du AWS CLI.

Si vous n'avez pas besoin de publier vos adresses IPv6 sur Internet, vous pouvez fournir une adresse IPv6 GUA privée à un IPAM. Pour plus d'informations, consultez [Activer le provisionnement de CIDR GUA IPv6 privés](#).

## ⚠️ Important

- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :
  - [Intégration d'IPAM aux comptes d'une organisation AWS](#).
  - [Création d'un IPAM](#).
- Chaque étape de ce tutoriel doit être effectuée par l'un des trois comptes Organisations AWS :
  - Le compte de gestion
  - Le compte de membre configuré pour être votre administrateur IPAM dans [Intégration d'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 groupe IPAM de niveau supérieur contenant un groupe régional et que nous allons allouer de l'espace à une ressource 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.

## 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, sélectionnez 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. Sous Address family (Famille d'adresses), choisissez IPv6.
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 Locale (paramètre régional), choisissez 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.

 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, BYOIP est sélectionné par défaut.
11. Dans la section CIDR à provisionner, effectuez l'une des opérations suivantes :

- Si vous avez [vérifié le contrôle de votre domaine à l'aide d'un certificat X.509](#), vous devez inclure le CIDR, le message BYOIP et la signature du certificat que vous avez créés lors de cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.
- Si vous avez [vérifié le contrôle de votre domaine avec un enregistrement DNS TXT](#), vous devez inclure le jeton de vérification CIDR et IPAM que vous avez créé dans cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.

Notez que lors du provisionnement d'un CIDR IPv6 dans un groupe au sein du groupe de premier niveau, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR qui peuvent être annoncés publiquement et /60 pour les CIDR qui ne peuvent pas être annoncés publiquement.

 **Important**

Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'allocation des plages qui peuvent être annoncées publiquement peut durer jusqu'à une semaine.

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 CIDR dans 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, sélectionnez 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.

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.

9. 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 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 du provisionnement d'un CIDR IPv6 dans un groupe au sein du groupe de premier niveau, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR qui

peuvent être annoncés publiquement et /60 pour les CIDR qui ne peuvent pas être annoncés publiquement.

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.  
Remarques :
  - 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. (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 CIDR dans la page des détails du groupe.

### Étape 3. Partager le groupe régional

Suivez les étapes de cette section pour partager le groupe IPAM en utilisant 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 groupe IPAM, suivez les étapes de cette section pour activer le partage des ressources avec AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'option **--profile management-account**.

#### 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.

#### Partager d'un groupe IPAM à l'aide de AWS RAM

Dans cette section, vous partagerez le groupe régional 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](#). Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'option `--profile ipam-account`.

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, sélectionnez Pools (Groupes).
3. Choisissez le périmètre privé, choisissez le groupe IPAM, 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 partagez le groupe en utilisant AWS RAM.
5. Sélectionnez Create a resource share (Créer un partage de ressources).
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 que vous souhaitez partager.
9. Choisissez Suivant.
10. Sélectionnez l'autorisation AWSRAMPermissionIpamPoolByoipCidrImport. 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. 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 [Create a VPC](#) du Guide d'utilisation d'Amazon VPC.

Cette étape doit être effectuée par le compte membre.

### Note

- Lorsque vous ouvrez VPC dans le AWSConsole de gestion, la AWSrégion dans laquelle vous allouez le VPC doit correspondre à l'option Locale que vous avez choisie lors de la création du groupe 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 allouez 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 publier le CIDR que vous avez fourni à AWS et qui est dans le groupe ayant défini le Service EC2 (EIP/VPC). 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, sélectionnez 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. Cliquez sur Publicité CIDR.

Par conséquent, le CIDR BYOIP est annoncé et la valeur dans la colonne Publicité passe de Retiré 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, sélectionnez 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 : Supprimer le VPC.

Cette étape doit être effectuée par le compte membre.

- Suivez les étapes décrites dans la section [Delete a VPC](#) du Guide d'utilisation d'Amazon VPC pour supprimer le VPC. Lorsque vous ouvrez VPC dans le AWSConsole de gestion, la AWSrégion dans laquelle vous supprimez le VPC doit correspondre à l'option Locale que vous avez choisie lors de la création du groupe 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. Allocation songlet.

#### Étape 3 : 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.

- Suivez les étapes décrites dans les sections [Deleting a resource share in AWS RAM](#) et [Disabling resource sharing with AWS Organizations](#) du Guide d'utilisation d'AWS RAM, dans cet ordre, pour supprimer les partages RAM et désactiver l'intégration de RAM à AWS Organizations.

#### 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 groupe](#) pour 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 groupe](#) pour supprimer le groupe régional et ensuite le groupe de niveau supérieur, dans cet ordre.

### Apportez votre propre CIDR IP sur IPAM en utilisant uniquement la AWS CLI

Intégrer votre propre adresse IP (BYOIP) à IPAM vous permet d'utiliser les plages d'adresses IPv4 et IPv6 existantes de votre organisation dans AWS. Vous pouvez ainsi maintenir une image de marque cohérente, améliorer les performances du réseau, renforcer la sécurité et simplifier la gestion en unifiant les environnements sur site et en nuage sous votre propre espace d'adresses IP.

Suivez ces étapes pour apporter un CIDR IPv4 ou IPv6 à IPAM à l'aide de la AWS CLI uniquement.

**Note**

Avant de commencer, vous devez disposer d'un [contrôle de domaine vérifié](#).

Une fois que vous avez apporté une plage d'adresses IPv4 vers 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 IPv4 CIDR public à IPAM en utilisant uniquement la CLI AWS](#)
- [Apportez votre propre CIDR IPv6 sur IPAM en utilisant uniquement la AWS CLI](#)

## Apportez votre propre IPv4 CIDR public à IPAM en utilisant uniquement la CLI AWS

Procédez comme suit pour transférer un IPv4 CIDR vers IPAM et attribuer une adresse IP élastique (EIP) au CIDR en utilisant uniquement le AWS CLI

**⚠️ Important**

- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :
  - [Intégration d'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 dans [Intégration d'IPAM aux comptes d'une organisation AWS](#). Dans ce tutoriel, ce compte sera appelé compte IPAM.
  - Le compte membre de votre organisation qui sera alloué CIDRs à partir d'un pool 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 : publication du CIDR](#)
- [Étape 8 : partager le groupe régional](#)
- [Étape 9 : allocation d'une adresse IP Elastic à partir du groupe](#)
- [Étape 10 : associer l'adresse IP élastique à une EC2 instance](#)
- [Étape 11 : nettoyage](#)
- [Alternative à l'étape 9](#)

## 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 le AWS CLI](#)

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

- Un profil appelé `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 appelé `member-account` le compte membre AWS Organizations de votre organisation, qui sera alloué CIDRs 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 le champ public car les BYOIP CIDRs sont des adresses IP publiques, ce à quoi le champ public est destiné.

```
{
  "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' IPv4 adresses 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 du provisionnement d'un IPv4 CIDR vers un pool au sein du pool de niveau supérieur, le IPv4 CIDR minimum que vous pouvez provisionner est le suivant /24 ; les informations plus spécifiques CIDRs (telles que/25) ne sont pas autorisées.

##### Note

- Si vous avez [vérifié le contrôle de votre domaine à l'aide d'un certificat X.509](#), vous devez inclure le CIDR, le message BYOIP et la signature du certificat que vous avez créés lors de cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.

- Si vous avez [vérifié le contrôle de votre domaine avec un enregistrement DNS TXT](#), vous devez inclure le jeton de vérification CIDR et IPAM que vous avez créé dans cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.

Vous devez uniquement vérifier le contrôle du domaine 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 de vérification de la propriété du domaine.

Cette étape doit être réalisée par le compte IPAM.

### Important

Vous devez uniquement vérifier le contrôle du domaine 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 de contrôle de domaine. 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. Pour fournir au CIDR des informations de certificat, utilisez l'exemple de commande suivant. En plus de remplacer les valeurs selon les besoins dans l'exemple, assurez-vous de remplacer les valeurs Message et Signature par les valeurs `text_message` et `signed_message` que vous avez saisies dans [Vérifiez votre domaine avec un certificat X.509](#).

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-
pool-id ipam-pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --
verification-method remarks-x509 --cidr-authorization-context
  Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsMaU0P7EN07VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRY0dRaNx8yt-uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXE1T5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZ1afBbrFxRjFWRCTJhc7Cg3ASbR0-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

Pour fournir au CIDR des informations sur les jetons de vérification, utilisez l'exemple de commande suivant. En plus de remplacer les valeurs comme nécessaire dans l'exemple,

assurez-vous de remplacer **ipam-ext-res-ver-token-0309ce7f67a768cf0** par l'ID du jeton **IpamExternalResourceVerificationTokenId** que vous avez obtenu dans [Vérifiez votre domaine à l'aide d'un enregistrement DNS TXT](#).

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

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'allocation des plages qui peuvent être annoncées publiquement peut durer 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

### Création d'un groupe régional dans le groupe de niveau supérieur

Les paramètres régionaux du groupe doivent être l'une des options suivantes :

- AWS Région dans laquelle vous souhaitez que ce pool IPAM soit disponible pour des allocations.
- Le groupe de bordure du réseau pour une zone AWS locale dans laquelle vous souhaitez que ce pool IPAM soit disponible pour des allocations ([zones locales prises en charge](#)). Cette option n'est disponible que pour les IPv4 pools IPAM du périmètre public.
- Une [zone locale AWS dédiée](#). Pour créer un pool dans une zone locale AWS dédiée, entrez la zone locale AWS dédiée dans l'entrée du sélecteur.
- Global lorsque vous souhaitez utiliser des adresses IP dans le monde entier dans toutes les AWS régions, telles que les CloudFront sites. La Global localisation n'est disponible que pour les IPv4 piscines publiques.

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 pool, 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.

Lorsque vous exécutez les commandes dans cette section, la valeur de `--region` doit inclure l'option `--local` que vous avez saisie lorsque vous avez créé le groupe qui sera utilisé pour le CIDR BYOIP. Par exemple, si vous avez créé le groupe BYOIP avec une locale `us-east-1`, le `--region` devrait être `us-east-1`. Si vous avez créé le groupe BYOIP avec une locale `us-east-1-scl-1` (un groupe de frontières réseau utilisé pour les zones locales), le `--region` devrait être `us-east-1`, car cette région gère la locale `us-east-1-scl-1`.

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 la `ec2` suivante : le CIDRs montant alloué à partir de ce pool sera publicisé pour le EC2 service Amazon (pour les adresses IP élastiques) et le service Amazon VPC ( CIDRs pour les adresses associées à VPCs).

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.

### Note

Lorsque vous fournissez un CIDR à un pool régional au sein du pool de niveau supérieur, le IPv4 CIDR le plus spécifique que vous puissiez provisionner est le suivant /24 ; les informations plus spécifiques CIDRs (telles que/25) ne sont pas autorisées. Après avoir créé le groupe régional, vous pouvez créer des groupes plus petits (tels que /25) au sein du même groupe régional. Notez que si vous partagez le groupe régional ou les groupes qu'il contient, ces groupes ne peuvent être utilisés que dans les paramètres régionaux définis sur le même groupe 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 : 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 --local de 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.

### Note

Le statut de la publicité ne limite pas votre capacité à attribuer des adresses IP Elastic. Même si votre BYOIPv4 CIDR n'est pas annoncé, vous pouvez toujours créer EIPs à partir du pool 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 8 : 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. <https://console.aws.amazon.com/ipam/>
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. Choisissez le périmètre privé, choisissez le groupe 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 Groupes IPAM, puis choisissez l'ARN du groupe que vous souhaitez partager.
9. Choisissez Suivant.
10. Choisissez l'AWSRAMPermissionIpamPoolByIpCidrImport autorisation. 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`. 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 9 : allocation d'une adresse IP Elastic à partir du groupe

Suivez les étapes de cette section pour allouer une adresse IP Elastic à partir du groupe. Notez que si vous utilisez des IPv4 pools publics pour allouer des adresses IP élastiques, vous pouvez utiliser les étapes alternatives [Alternative à l'étape 9](#) plutôt que celles de cette section.

##### Important

Si vous voyez une erreur liée au fait que vous ne disposez pas des autorisations nécessaires pour appeler `ec2 :AllocateAddress`, l'autorisation gérée actuellement attribuée au pool IPAM qui a été partagé avec vous doit être mise à jour. Contactez la personne qui a créé le partage de ressources 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

Suivez les étapes décrites dans la [section Allouer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour attribuer l'adresse, mais notez ce qui suit :

- Cette étape doit être effectuée par le compte membre.
- Assurez-vous que la AWS région dans laquelle vous vous trouvez dans la EC2 console correspond à l'option locale que vous avez choisie lors de la création du pool régional.
- Lorsque vous choisissez le pool d'adresses, choisissez l'option Allouer à l'aide d'un pool IPv4 IPAM et choisissez le pool régional que vous avez créé.

## Command line

Allouez une adresse depuis le groupe à l'aide de la commande [allocate-address](#). L'option `--region` utilisée doit correspondre à l'option `-locale` que vous avez choisie lors de la création du groupe à l'étape 2. Incluez l'ID du groupe IPAM que vous avez créé à l'étape 2 dans `--ipam-pool-id`. En option, vous pouvez également choisir un élément spécifique `/32` dans votre groupe IPAM en utilisant l'option `--address`.

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

Exemple de réponse :

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

Pour plus d'informations, consultez la section [Allocation d'une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon.

## Étape 10 : associer l'adresse IP élastique à une EC2 instance

Suivez les étapes décrites dans cette section pour associer l'adresse IP élastique à une EC2 instance.

### AWS Management Console

Suivez les étapes décrites dans [Associer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour attribuer une adresse IP élastique à partir du pool IPAM, mais notez ce qui suit : lorsque vous utilisez l'option AWS Management Console, la AWS région à laquelle vous associez l'adresse IP élastique doit correspondre à l'option locale que vous avez choisie lors de la création du pool régional.

Cette étape doit être effectuée par le compte membre.

## Command line

Cette étape doit être effectuée par le compte membre. Utilisez l'option **--profile member-account**.

Utilisez la commande [associate-address](#) pour associer une adresse IP Elastic à une instance. L'option **--region** à laquelle vous associez l'adresse IP Elastic doit correspondre à l'option **--locale** que vous avez choisie lors de la création du groupe régional.

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

Exemple de réponse :

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

Pour plus d'informations, consultez [Associer une adresse IP élastique à une instance ou à une interface réseau](#) dans le guide de EC2 l'utilisateur Amazon.

## Étape 11 : 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 inclure 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 de la publicité pour le IPv4 CIDR.

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 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 `--local` 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": []  
}
```

5. 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 désapprovisionnement prend un certain temps. Vérifiez le statut du désapprovisionnement.

```
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"  
  }  
}
```

6. 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.

7. 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"
    }
}
```

8. 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"  
  
  }  
  
}
```

9. 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"  
    }  
}
```

10. 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"  
            }  
        ],  
    }  
}
```

## Alternative à l'étape 9

Si vous utilisez des IPv4 pools publics pour allouer des adresses IP élastiques, vous pouvez suivre les étapes de cette section plutôt que celles de la section précédente [Étape 9 : allocation d'une adresse IP Elastic à partir du groupe](#).

### Table des matières

- [Étape 1 : créer un IPv4 pool public](#)
- [Étape 2 : Fournir le IPv4 CIDR public à votre piscine publique IPv4](#)
- [Étape 3 : créer une adresse IP élastique à partir du IPv4 pool public](#)
- [Alternative au nettoyage de l'étape 9](#)

### Étape 1 : créer un IPv4 pool public

Cette étape est généralement effectuée par un autre AWS compte qui souhaite fournir une adresse IP élastique, telle que le compte membre.

#### ⚠ Important

Les IPv4 pools publics et les pools IPAM sont gérés par des ressources distinctes dans AWS. Les IPv4 pools publics sont des ressources à compte unique qui vous permettent de convertir vos adresses IP publiques CIDRs en adresses IP élastiques. Les pools IPAM peuvent être utilisés pour allouer votre espace public à des IPv4 pools publics.

### Pour créer un IPv4 pool 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 `--local` 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 le résultat, vous verrez l'ID du IPv4 pool public. Vous aurez besoin de cet ID à la prochaine étape.

```
{
```

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

{

## Étape 2 : Fournir le IPv4 CIDR public à votre piscine publique IPv4

Fournissez le IPv4 CIDR public à votre IPv4 pool 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. Le `--netmask-length` le moins précis que vous puissiez définir est 24.

Cette étape doit être effectuée par le compte membre.

Pour créer un IPv4 pool 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 pool public IPv4 .

```
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 3 : créer une adresse IP élastique à partir du IPv4 pool public

Créez une adresse IP élastique (EIP) à partir du IPv4 pool public. Lorsque vous exécutez les commandes dans cette section, la valeur de `--region` doit correspondre à l'option `--local` 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 IPv4 pool 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"  
    }  
  ]  
}
```

Alternative au nettoyage de l'étape 9

Procédez comme suit pour nettoyer les IPv4 piscines publiques créées à l'aide de l'alternative à l'étape 9. Vous devez effectuer ces étapes après avoir publié l'adresse IP Elastic au cours du processus de nettoyage standard dans [Étape 10 : nettoyage](#).

1. Consultez votre BYOIP CIDRs.

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": []
}
]
}
```

2. Libérez le CIDR du IPv4 pool public. 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 130.137.245.0/24 --profile member-account
```

3. Consultez à CIDRs nouveau votre BYOIP et assurez-vous 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 le résultat, vous verrez le nombre d'adresses IP dans votre IPv4 pool public.

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

## Apportez votre propre CIDR IPv6 sur IPAM en utilisant uniquement la AWS CLI

Suivez ces étapes pour fournir un CIDR IPv6 à IPAM et allouer un VPC en utilisant uniquement AWS CLI.

Si vous n'avez pas besoin de publier vos adresses IPv6 sur Internet, vous pouvez fournir une adresse IPv6 GUA privée à un IPAM. Pour plus d'informations, consultez [Activer le provisionnement de CIDR GUA IPv6 privés](#).

### Important

- Le didacticiel présume que vous ayez déjà effectué les étapes suivantes dans les sections suivantes :
  - [Intégration d'IPAM aux comptes d'une organisation AWS](#).
  - [Création d'un IPAM](#).
- Chaque étape de ce tutoriel doit être effectuée par l'un des trois comptes Organisations AWS :
  - Le compte de gestion
  - Le compte de membre configuré pour être votre administrateur IPAM dans [Intégration d'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 d'AWS CLI nommés et de 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 : Création de profils d'AWS CLI nommés et de rôles IAM

Pour suivre ce didacticiel en tant qu'utilisateur AWS unique, vous pouvez utiliser des profils nommés AWS CLI 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 comptes AWS, consultez la section [Using an IAM role in the AWS CLI](#).

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

- Un profil appelé `management-account` pour le AWSCompte de gestion Organizations.
- Un profil appelé `ipam-account` pour le AWSCompte membre Organizations configuré pour être votre administrateur IPAM.
- Un profil appelé `member-account` pour le AWSCompte membre Organizations de votre organisation qui allouera des CIDR à partir d'un groupe 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 tout au long de ce didacticiel que l'échantillon AWS CLI commande l'utilisation de `--profile` l'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 PublicDefaultScopeId. 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-08b70b04fb524f8d",
    "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.

Déterminez si vous souhaitez que ce CIDR de groupe IPAM soit publié par AWS sur l'Internet public (--publicly-advertisible ou --no-publicly-advertisible).

**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 groupe d'adresses IPv6 pour toutes vos ressources AWS à l'aide de l'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-advertisible --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 lors du provisionnement d'un CIDR IPv6 dans un groupe au sein du groupe de premier niveau, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR qui peuvent être annoncés publiquement et /60 pour les CIDR qui ne peuvent pas être annoncés publiquement.

##### Note

- Si vous avez [vérifié le contrôle de votre domaine à l'aide d'un certificat X.509](#), vous devez inclure le CIDR, le message BYOIP et la signature du certificat que vous avez créés lors de cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.
- Si vous avez [vérifié le contrôle de votre domaine avec un enregistrement DNS TXT](#), vous devez inclure le jeton de vérification CIDR et IPAM que vous avez créé dans cette étape afin que nous puissions vérifier que vous contrôlez l'espace public.

Vous devez uniquement vérifier le contrôle du domaine 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 de propriété du domaine.

Cette étape doit être réalisée par le compte IPAM.

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

1. Pour fournir au CIDR des informations de certificat, utilisez l'exemple de commande suivant. En plus de remplacer les valeurs selon les besoins dans l'exemple, assurez-vous de remplacer les valeurs `Message` et `Signature` par les valeurs `text_message` et `signed_message` que vous avez saisies dans [Vérifiez votre domaine avec un certificat X.509](#).

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6vdccfvL88g8d~YAuai-CR7HqMwzcgdS9R1pBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfd00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~Cv6L0N3y00XMp4JENB9uM7sMlu6oeoutGyyhXFeYPz1GSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa~wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

Pour fournir au CIDR des informations sur les jetons de vérification, utilisez l'exemple de commande suivant. En plus de remplacer les valeurs comme nécessaire dans l'exemple, assurez-vous de remplacer **ipam-ext-res-ver-token-0309ce7f67a768cf0** par l'ID du jeton **IpamExternalResourceVerificationTokenId** que vous avez obtenu dans [Vérifiez votre domaine à l'aide d'un enregistrement DNS TXT](#).

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

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'allocation des plages qui peuvent être annoncées publiquement peut durer 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. `--local` 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 service AWS où le CIDR pourra être annoncé. 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 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 lors du provisionnement d'un CIDR dans un groupe au sein du groupe de premier niveau, la plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR qui peuvent être annoncés publiquement et /60 pour les CIDR qui ne peuvent pas être annoncés publiquement.

Cette étape doit être réalisée par le compte IPAM.

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-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 de cette section pour partager le groupe IPAM en utilisant 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 groupe IPAM, suivez les étapes de cette section pour activer le partage des ressources avec AWS RAM. Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'option `--profile management-account`.

#### 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.

### Partager d'un groupe IPAM à l'aide de AWS RAM

Dans cette section, vous partagerez le groupe régional 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](#). Si vous utilisez le AWS CLI pour activer le partage des ressources, utilisez l'option `--profile ipam-account`.

#### 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, sélectionnez Pools (Groupes).
3. Choisissez le périmètre privé, choisissez le groupe IPAM, 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 partagez le groupe en utilisant AWS RAM.

5. Sélectionnez Create a resource share (Créer un partage de ressources).
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 que vous souhaitez partager.
9. Choisissez Suivant.
10. Sélectionnez l'autorisation AWSRAMPermissionIpamPoolByoipCidrImport. 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 procédez 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. 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 --local 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 de l' 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"  
      }  

```

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 publier le CIDR que vous avez fourni à AWS, et qui est dans un groupe ayant --aws-service ec2 défini. Dans ce tutoriel, 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 --local de 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 publier le CIDR à l'aide de l' 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.

### Nettoyage à l'aide de l' 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 figurant dans les sections [Deleting a resource share in AWS RAM](#) et [Disabling resource sharing with AWS Organizations](#) du Guide d'utilisation d'AWS RAM, dans cet ordre, pour supprimer les partages RAM et désactiver l'intégration de RAM à AWS Organizations.

Cette étape doit être effectuée par le compte IPAM et le compte de gestion respectivement. Si vous utilisez l'AWS CLI pour supprimer les partages RAM et désactiver l'intégration de la RAM, utilisez les options `--profile ipam-account` et `--profile management-account`.

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"
            }
        ]
    }
}
```

## Utilisez votre propre adresse IP pour CloudFront utiliser IPAM

Le BYOIP d'IPAM pour les services mondiaux vous permet d'utiliser vos propres IPv4 adresses avec des services AWS mondiaux tels que CloudFront. Contrairement au BYOIP régional, vos adresses IP sont annoncées simultanément à partir de plusieurs emplacements périphériques via le routage anycast.

### Pourquoi utiliser cette fonctionnalité ?

- Maintenir la liste des adresses IP autorisées : utilisez les adresses IP approuvées existantes au lieu de mettre à jour les configurations du pare-feu
- Simplifiez les migrations : migrez depuis un autre CDNs sans modifier l'infrastructure IP
- Image de marque cohérente — Conservez votre espace d'adresse IP existant lorsque vous passez à AWS

### Qui doit utiliser cette fonctionnalité ?

Organisations qui ont besoin de leurs propres adresses IP pour diffuser du contenu dans le monde entier :

- Grandes entreprises soumises à des exigences en matière de liste d'adresses IP autorisées
- Entreprises qui migrent depuis d'autres entreprises CDNs avec des adresses IP existantes
- Organisations dotées de politiques de sécurité strictes exigeant des plages d'adresses IP spécifiques

### Quand utiliser cette fonctionnalité ?

Utilisez le BYOIP pour des services internationaux lorsque vous devez :

- Maintenir la liste d'adresses IP autorisées existante auprès des partenaires/clients
- Migrez depuis un autre CDN à l'aide de vos adresses IP
- Respectez les exigences de conformité pour des plages d'adresses IP spécifiques

#### Note

Nécessite /24 blocs IPv4 CIDR. Actuellement disponible CloudFront uniquement pour.

## Conditions préalables

Effectuez les étapes suivantes avant de commencer :

- Configuration de l'IPAM — et [Intégration d'IPAM aux comptes d'une organisation AWS](#) [Création d'un IPAM](#)
- Vérification du domaine — [Vérification du contrôle du domaine](#)
- Créez un pool de premier niveau — Suivez les étapes 1 et 2 de la section [Apportez votre propre IPv4 CIDR](#) à l'IPAM

## Étapes de configuration globale du service

Les étapes suivantes diffèrent du processus BYOIP régional standard et définissent le modèle des services mondiaux :

Étape 1 : créer un pool mondial pour les services anycast

Au lieu de créer un pool régional, créez un pool mondial pour les services anycast :

Console

Pour créer un pool global à l'aide de la console :

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans le volet de navigation, sélectionnez Pools
3. Choisissez Créer un pool
4. Source : Choisissez votre pool BYOIP de haut niveau
5. Lieu : Choisissez Global
6. Service : Choisissez les services globaux (apparaît lorsque Global est sélectionné)
7. Source IP publique : Choisissez BYOIP
8. CIDRs à approvisionner : Spécifiez votre plage CIDR /24
9. Choisissez Créer un pool

## INTERFACE DE LIGNE DE COMMANDE (CLI)

À utiliser `aws ec2 create-ipam-pool` avec les paramètres régionaux définis sur « Global » et la famille d'adresses « ipv4 ».

Provisionnez ensuite le CIDR à l'aide `aws ec2 provision-ipam-pool-cidr` de.

### Important

Vous devez allouer le bloc /24 complet à ce pool. Vous pouvez configurer des plages plus spécifiques au sein de ce bloc pour différentes utilisations.

## Étape 2 : créer des ressources spécifiques aux services

Pour CloudFront créer une liste d'adresses IP anycast qui utilise votre pool IPAM. Pour des instructions détaillées, consultez la documentation CloudFront BYOIP (lien à déterminer).

Principaux paramètres de l'intégration IPAM :

- Type d'adresse IP — Choisissez BYOIP
- Pool IPAM — Sélectionnez votre pool mondial à l'étape 1
- Nombre d'adresses IP — Entrez 3 (obligatoire pour CloudFront)

## Étape 3 : Associer aux ressources du service

Associez votre liste d'adresses IP Anycast Static à une CloudFront distribution. Pour des instructions détaillées, consultez la documentation CloudFront BYOIP (lien à déterminer).

Configuration des clés :

- Dans les paramètres de distribution, sélectionnez votre liste d'adresses IP Anycast à l'étape 2

## Étape 4 : Préparation à la migration

- Réduction du TTL DNS — Définissez le TTL DNS pour vos enregistrements sur 60 secondes ou moins
- Attendre la propagation — Laissez le temps au nouveau TTL de prendre effet sur Internet

## Étape 5 : Faites la promotion du CIDR dans le monde entier

Utilisez la commande de publicité globale IPAM :

Console

Pour annoncer le CIDR à l'aide de la console :

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans le volet de navigation, sélectionnez Pools
3. Sélectionnez votre pool mondial
4. Choisissez l'CIDRsonglet
5. Sélectionnez votre CIDR et choisissez Actions > Annoncer le CIDR
6. Confirmez la publicité

## INTERFACE DE LIGNE DE COMMANDE (CLI)

`aws ec2 advertise-ipam-byoip-cidr` à utiliser avec votre identifiant de pool IPAM et votre CIDR.

### Important

- Supprimez la publicité de votre ancien fournisseur avant d'exécuter cette commande
- Mettez à jour les enregistrements DNS de manière à ce qu'ils CloudFront pointent vers pour terminer la migration

## Nettoyage

Pour nettoyer les ressources créées dans ce didacticiel :

- Supprimer CloudFront des ressources — Suivez les instructions de nettoyage de la documentation CloudFront BYOIP (lien à déterminer)
- Retirez le CIDR et supprimez les pools IPAM : suivez le processus de nettoyage standard dans [Étape 8 : nettoyage](#)

### Important

Supprimez d'abord les CloudFront ressources, puis procédez au nettoyage IPAM pour éviter les interruptions de service.

# Didacticiel : transfert d'un CIDR IPv4 BYOIP vers IPAM

Suivez ces étapes pour transférer un CIDR IPv4 existant vers IPAM. Si vous disposez déjà d'un CIDR BYOIP IPv4 avec AWS, vous pouvez déplacer le CIDR vers IPAM à partir d'un groupe IPv4 public. Vous ne pouvez pas déplacer un CIDR IPv6 vers IPAM.

Ce tutoriel suppose que vous avez déjà réussi à faire passer une plage d'adresses IP à AWS à l'aide du processus décrit dans [Fourniture de vos propres adresses IP \(BYOIP\) dans Amazon EC2](#) et que vous voulez maintenant transférer cette plage d'adresses IP à IPAM. Si vous intégrez une nouvelle adresse IP à AWS pour la première fois, suivez les étapes de [Didacticiel : 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](#).

## Note

- Ce didacticiel suppose que vous avez terminé cette procédure en [Création d'un IPAM](#).
- Chaque étape de ce didacticiel doit être effectuée par l'une des deux AWScomptes :
  - 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 d'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 groupe IPAM en utilisant 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 d'AWS CLI nommés et de rôles IAM

Pour suivre ce didacticiel en tant qu'utilisateur AWS unique, vous pouvez utiliser des profils nommés AWS CLI 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 comptes AWS, consultez la section [Using an IAM role in the AWS CLI](#).

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

- Un profil appelé `ipam-account` pour la AWS compte qui est l'administrateur IPAM.
- Un profil appelé `yoip-owner-account` pour la AWS compte de votre organisation propriétaire du CIDR BYOIP.

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 tout au long de ce didacticiel que l'échantillon AWS CLI commande l'utilisation de `--profile` l'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 service AWS où le CIDR pourra être annoncé. 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 aurez besoin de cet `OwnerId` à la prochaine étape.

```
{  
  "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 groupe IPAM en utilisant AWS RAM

Suivez les étapes de cette section pour partager un groupe IPAM en utilisant AWS RAM afin qu'un autre compte AWS puisse transférer un CIDR IPV4 BYOIP existant vers le groupe IPAM et l'utiliser. Cette étape doit être effectuée par le compte **ipam-account**.

Pour partager un groupe d'adresses IPv4 en utilisant AWS CLI

1. Consultez les autorisations AWS RAM disponibles pour les groupes 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",
    "is ResourceTypeDefault": false
}
]
}

```

- 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 RAM, le compte **byoip-owner-account** peut désormais déplacer les CIDR vers RAM.

## 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 apporté une plage d'adresses IPv4 vers 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`

### ℹ Note

Vous pouvez utiliser l'AWS Management Console ou l'AWS CLI pour effectuer cette étape.

### AWS Management Console

Pour transférer un CIDR BYOIP vers le groupe IPAM :

1. Ouvrez la console IPAM à partir de l'adresse <https://console.aws.amazon.com/ipam/> en tant que compte **byoip-owner-account**.
2. Dans le panneau de navigation, sélectionnez 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 commandes de l'AWS CLI suivantes pour transférer un CIDR BYOIP vers le groupe IPAM à l'aide de l'AWS CLI :

1. Exécutez la commande suivante pour transférer le CIDR. Assurez-vous que la valeur `--region` correspond à la Région AWS 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 groupe IPAM à l'aide d' AWS CLI

- Exécutez la commande suivante pour afficher l'allocation gérée dans IPAM. Assurez-vous que la valeur `--region` correspond à la Région AWS 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 tutoriel à l'aide d' 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 groupe IPAM en utilisant 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 valeur `--region` correspond à la Région AWS 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 le CIDR à partir du groupe IPv4 public. 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 130.137.249.0/24
```

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 tutoriel à l'aide d'une plage CIDR IPv6 en créant le VPC avec l'option de bloc d'adresse CIDR IPv6 fournie par Amazon dans la 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 : Création d'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. Sélectionnez Delete (Supprimer).
7. [Supprimer les sous-réseaux](#).
8. [Supprimer le VPC](#).

Le nettoyage est terminé.

## Allouer des adresses IP Elastic séquentielles à partir d'un groupe IPAM

L'IPAM vous permet de fournir des IPv4 blocs publics appartenant à Amazon aux pools IPAM et d'allouer des [adresses IP élastiques](#) séquentielles de ces pools aux ressources. AWS

Les adresses IP élastiques allouées de manière contiguë sont des IPv4 adresses publiques allouées de manière séquentielle. Par exemple, si Amazon vous fournit un bloc d'adresse IPv4 CIDR public de 192.0.2.0/30 et que vous allouez les quatre IPv4 adresses publiques disponibles à partir de ce bloc d'adresse CIDR, un exemple de quatre adresses IP élastiques séquentielles est 192.0.2.0, 192.0.2.1, 192.0.2.2 et 192.0.2.3

Les adresses IP Elastic allouées de manière contiguë vous permettent de simplifier vos règles de sécurité et de réseau de la manière suivante :

- Administration de la sécurité : l'utilisation d' IPv4 adresses séquentielles réduit les frais de gestion de votre pare-feu. Vous pouvez ajouter un préfixe entier à une seule règle et l'associer à IPs partir du même préfixe au fur et à mesure de votre mise à l'échelle, ce qui vous permet d'économiser du temps et des efforts.
- Accès d'entreprise : vous pouvez simplifier l'espace d'adressage partagé avec vos clients en utilisant un bloc CIDR complet au lieu d'une longue liste d' IPv4 adresses publiques individuelles. Cela évite d'avoir à communiquer constamment les modifications d'adresse IP au fur et à mesure que votre application évolue sur AWS.
- Gestion IP simplifiée : L'utilisation d' IPv4 adresses séquentielles simplifie la gestion des adresses IP publiques pour votre équipe réseau centrale, car elle réduit le besoin de suivre le public individuel IPs et lui permet de se concentrer sur un nombre limité de préfixes IP.

Dans ce tutoriel, vous allez suivre les étapes nécessaires pour allouer des adresses IP Elastic séquentielles à partir d'un groupe IPAM. Vous allez créer un pool IPAM avec un bloc IPv4 CIDR public contigu fourni par Amazon, allouer des adresses IP élastiques à partir du pool et apprendre à surveiller les allocations de pool IPAM.

#### Note

- Des frais sont associés au provisionnement de blocs CIDR publics IPv4 appartenant à Amazon. Pour plus d'informations, consultez l'onglet [IPv4 Bloc contigu fourni par Amazon](#) sur la page de tarification d'Amazon [VPC](#).
- Ce tutoriel part du principe que vous souhaitez créer un IPAM [à l'aide d'IPAM avec un seul compte](#). Si vous souhaitez partager des IPv4 blocs publics contigus appartenant à Amazon sur plusieurs comptes, d'abord et ensuite. [Intégration d'IPAM aux comptes d'une organisation AWS](#) [Partage d'un groupe IPAM à l'aide d'AWS RAM](#) Si vous intégrez AWS Organizations, vous avez la possibilité de créer une [politique de contrôle des services](#) pour empêcher le déprovisionnement des IPv4 blocs contig affectés au pool.
- Vous ne pouvez pas [transférer](#) les adresses IP Elastic séquentielles allouées depuis un groupe IPAM vers d'autres comptes AWS . Au lieu de cela, IPAM vous permet de partager des pools IPAM entre différents AWS comptes en intégrant IPAM aux AWS Organizations (comme indiqué ci-dessus).

- Le nombre de blocs IPv4 CIDR publics appartenant à Amazon que vous pouvez provisionner et leur taille sont limités. Pour de plus amples informations, veuillez consulter [Quotas pour votre IPAM](#).

## Table des matières

- [Étape 1 : création d'un IPAM](#)
- [Étape 2 : création d'un groupe IPAM et provisionnement d'un CIDR](#)
- [Étape 3 : allocation d'une adresse IP Elastic à partir du groupe](#)
- [Étape 4 : associer l'adresse IP élastique à une EC2 instance](#)
- [Étape 5 : suivre et surveiller l'utilisation du groupe](#)
- [Nettoyage](#)

## Étape 1 : création d'un IPAM

Suivez les étapes de cette section pour créer un IPAM.

### AWS Management Console

#### Pour créer un IPAM

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans la console AWS de gestion, choisissez la AWS région 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 AWS région dans laquelle vous créez votre IPAM est sélectionnée comme l'une des régions opérationnelles par défaut.

Par exemple, si vous créez cet IPAM dans une AWS région **us-east-1** mais que vous souhaitez créer ultérieurement des pools IPAM régionaux qui le fournissent CIDRs **us-west-2**, sélectionnez **us-west-2** ici. VPCs 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 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.

Créez l'IPAM à l'aide de la commande [create-ipam](#) :

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

Exemple de réponse :

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

```
        "RegionName": "us-east-1"
    }
],
"State": "create-in-progress",
"Tags": [],
"DefaultResourceDiscoveryId": "ipam-res-disco-02cc5b34cc3f04f09",
"DefaultResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-06b3a4dccfc81f7c1",
"ResourceDiscoveryAssociationCount": 1,
"Tier": "advanced"
}
}
```

Vous en aurez besoin PublicDefaultScopeld à l'étape suivante. Pour plus d'informations sur les portées, consultez [Fonctionnement d'IPAM](#).

## Étape 2 : création d'un groupe IPAM et provisionnement d'un CIDR

Suivez les étapes de cette section pour créer un groupe IPAM à partir duquel vous allouerez les adresses IP Elastic.

### AWS Management Console

#### Création d'un groupe

1. Ouvrez la console IPAM à <https://console.aws.amazon.com/ipam/> l'adresse.
2. Dans le panneau de navigation, choisissez Pools (Groupes).
3. 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. Sous Famille d'adresses, sélectionnez IPv4.
8. Sous Planification des ressources, laissez sélectionné Planifier l'espace IP dans la portée.
9. Sous Paramètres régionaux, choisissez les paramètres régionaux du groupe. Le paramètre régional est la AWS région dans laquelle vous souhaitez que ce pool IPAM soit disponible

pour les allocations. Les options disponibles proviennent des Régions d'exploitation que vous avez sélectionnées lors de la création de votre IPAM.

10. Sous Service, sélectionnez EC2 (EIP/VPC). Le service que vous sélectionnez détermine le AWS service pour lequel le CIDR sera annoncé. Actuellement, la seule option est EC2 (EIP/VPC), ce qui signifie que le CIDRs montant alloué à partir de ce pool sera annoncé pour le EC2 service Amazon (pour les adresses IP élastiques).
11. Sous Source IP publique, sélectionnez appartenant à Amazon.
12. Sous CIDR à provisionner, choisissez Ajouter un CIDR public appartenant à Amazon. Choisissez une longueur de masque réseau comprise entre /29 (8 adresses IP) et /30 (4 adresses IP). Vous pouvez en ajouter jusqu'à 2 CIDRs par défaut. Pour plus d'informations sur l'augmentation des limites du public contigu fourni par Amazon, consultez. IPv4 CIDRs [Quotas pour votre IPAM](#)
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 du provisionnement dans l'CIDRsonglet de la page de détails du pool.

## Command line

### Création d'un groupe

1. Créez un pool IPAM à l'aide de la [create-ipam-pool](#)commande. Le paramètre régional est la Région AWS dans laquelle vous souhaitez que ce groupe IPAM soit disponible pour les allocations. Les options disponibles proviennent des Régions d'exploitation que vous avez sélectionnées lors de la création de votre IPAM.

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

Exemple de réponse avec état `create-in-progress` :

```
{
```

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

2. Vérifiez que le pool a été créé avec succès à l'aide de la [describe-ipam-pools](#) commande.

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

Exemple de réponse avec état `create-complete` :

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

3. Fournissez un CIDR au pool à l'aide de la [provision-ipam-pool-cidr](#) commande. Choisissez --netmask-length entre /29 (8 adresses IP) et /30 (4 adresses IP). Vous pouvez en ajouter jusqu'à 2 CIDRs par défaut. Pour plus d'informations sur l'augmentation des limites du public contigu fourni par Amazon, consultez. IPv4 CIDRs [Quotas pour votre IPAM](#)

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

Exemple de réponse avec état pending-provision :

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

```
    }  
}
```

4. Vérifiez que ce CIDR a été provisionné avant de continuer. Vous pouvez consulter l'état du provisionnement à l'aide de la [get-ipam-pool-cidrs](#) commande.

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

Exemple de réponse avec état provisioned :

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

## Étape 3 : allocation d'une adresse IP Elastic à partir du groupe

Suivez les étapes de cette section pour allouer une adresse IP Elastic à partir du groupe.

### AWS Management Console

Suivez les étapes décrites dans la [section Allouer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour attribuer l'adresse, mais notez ce qui suit :

- Assurez-vous que la AWS région dans laquelle vous vous trouvez dans la EC2 console correspond à l'option locale que vous avez choisie lors de la création du pool à l'étape 2.
- Lorsque vous choisissez le pool d'adresses, choisissez l'option Allouer à l'aide d'un pool IPv4 IPAM et choisissez le pool que vous avez créé à l'étape 1.

## Command line

Allouez une adresse depuis le groupe à l'aide de la commande [allocate-address](#). L'option `--region` utilisée doit correspondre à l'option `-local` que vous avez choisie lors de la création du groupe à l'étape 2. Incluez l'ID du groupe IPAM que vous avez créé à l'étape 2 dans `--ipam-pool-id`.

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

Exemple de réponse :

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

En option, vous pouvez également choisir un élément spécifique /32 dans votre groupe IPAM en utilisant l'option `--address`.

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

Exemple de réponse :

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

Pour plus d'informations, consultez la section [Allocation d'une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon.

## Étape 4 : associer l'adresse IP élastique à une EC2 instance

Suivez les étapes décrites dans cette section pour associer l'adresse IP élastique à une EC2 instance.

### AWS Management Console

Suivez les étapes décrites dans [Associer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour attribuer une adresse IP élastique à partir du pool IPAM, mais notez ce qui suit : lorsque vous utilisez l'option AWS Management Console, la AWS région à laquelle vous associez l'adresse IP élastique doit correspondre à l'option locale que vous avez choisie lors de la création du pool à l'étape 2.

### Command line

Utilisez la commande [associate-address](#) pour associer une adresse IP Elastic à une instance. L'option `--region` à laquelle vous associez l'adresse IP Elastic doit correspondre à l'option `--locale` que vous avez choisie lors de la création du groupe à l'étape 2.

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

Exemple de réponse :

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

Pour plus d'informations, consultez [Associer une adresse IP élastique à une instance ou à une interface réseau](#) dans le guide de EC2 l'utilisateur Amazon.

## Étape 5 : suivre et surveiller l'utilisation du groupe

Une fois que vous avez alloué des adresses IP Elastic à partir du groupe IPAM, vous pouvez suivre et surveiller les allocations du groupe IPAM.

## AWS Management Console

- Consultez l'onglet Allocations des détails du groupe IPAM dans la console IPAM. Toutes les adresses IP Elastic allouées à partir du groupe IPAM ont un type de ressource EIP.
- Utiliser [Public IP Insights](#) :
  - Sous Types d'adresses IP publiques, filtrez selon les adresses appartenant à Amazon EIPs. Cela indique le nombre total d' IPv4 adresses publiques allouées aux adresses IP Elastic appartenant à Amazon. Si vous filtrez en fonction de cette mesure et que vous faites défiler la page jusqu'aux adresses IP publiques, vous verrez les adresses IP Elastic que vous avez allouées.
  - Sous Utilisation de l'EIP, filtrez par propriété associée à Amazon EIPs ou Propriété non associée à Amazon. EIPs Cela indique le nombre total d'adresses IP élastiques que vous avez allouées à votre AWS compte et que vous avez associées ou non à une EC2 instance, à une interface réseau ou à une AWS ressource. Si vous filtrez en fonction de cette mesure et que vous accédez à Adresses IP publiques au bas de la page, vous verrez des détails sur les ressources filtrées.
  - Dans le cadre de l' IPs utilisation IPv4 contiguë appartenant à Amazon, surveillez l'utilisation séquentielle des IPv4 adresses publiques au fil du temps et les pools IPAM associés appartenant à Amazon. IPv4
- Utilisez Amazon CloudWatch pour suivre et surveiller les métriques relatives aux IPv4 blocs publics contigus fournis par Amazon qui ont été fournis à des pools IPAM. Pour les métriques disponibles spécifiques aux IPv4 blocs contigus, consultez la section Mesures IP publiques sous. [Métriques IPAM](#) En plus de consulter les statistiques, vous pouvez créer des alarmes sur Amazon CloudWatch pour vous avertir lorsque les seuils sont atteints. La création d'alarmes et la configuration de notifications avec Amazon CloudWatch n'entrent pas dans le cadre de ce didacticiel. Pour plus d'informations, consultez la section [Utilisation des CloudWatch alarmes Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

## Command line

- Affichez les allocations du pool IPAM à l'aide de la [get-ipam-pool-allocations](#) commande. Toutes les adresses IP Elastic allouées à partir du groupe IPAM ont un type de ressource EIP.

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

Exemple de réponse :

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

- Utilisez Amazon CloudWatch pour suivre et surveiller les métriques relatives aux IPv4 blocs publics contigus fournis par Amazon qui ont été fournis à des pools IPAM. Pour les métriques disponibles spécifiques aux IPv4 blocs contigus, consultez la section Mesures IP publiques sous. [Métriques IPAM](#) En plus de consulter les statistiques, vous pouvez créer des alarmes sur Amazon CloudWatch pour vous avertir lorsque les seuils sont atteints. La création d'alarmes et la configuration de notifications avec Amazon CloudWatch n'entrent pas dans le cadre de ce didacticiel. Pour plus d'informations, consultez la section [Utilisation des CloudWatch alarmes Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

Le tutoriel est maintenant terminé. Vous avez créé un pool IPAM avec un bloc IPv4 CIDR public contigu fourni par Amazon, alloué des adresses IP élastiques à partir du pool et appris à surveiller les allocations de pool IPAM. Passez à la section suivante pour supprimer les ressources que vous avez créées dans ce tutoriel.

## Nettoyage

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

### Étape 1 : dissocier une adresse IP Elastic

Suivez les étapes décrites dans [Dissocier une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour dissocier l'adresse IP élastique.

## Étape 2 : affectation de l'adresse IP Elastic

Suivez les étapes décrites dans la [section Libérer une adresse IP élastique](#) dans le guide de EC2 l'utilisateur Amazon pour libérer une adresse IP élastique depuis le IPv4 pool public.

## Étape 3 : déprovisionnement du CIDR à partir du groupe IPAM

Effectuez les étapes [Pour désapprovisionner un CIDR de groupe](#) pour déprovisionner le CIDR public appartenant à Amazon du groupe IPAM. Cette étape est obligatoire pour la suppression du groupe. Le IPv4 bloc contigu fourni par Amazon vous sera facturé jusqu'à ce que cette étape soit terminée.

## Étape 4 : supprimer le groupe IPAM

Suivez les étapes décrites dans [Suppression d'un groupe](#) pour supprimer le groupe IPAM.

## Étape 5 : supprimer l'IPAM

Suivez les étapes décrites dans [Suppression d'un IPAM](#) pour supprimer l'IPAM.

Le nettoyage du tutoriel est terminé.

# Gestion des identités et des accès dans IPAM

AWS utilise des identifiants de sécurité pour vous identifier et vous donner accès à vos AWS ressources. Vous pouvez utiliser les fonctionnalités de Gestion des identités et des accès AWS (IAM) pour permettre à d'autres utilisateurs, services et applications d'utiliser vos AWS ressources dans leur intégralité ou de manière limitée, sans partager vos informations d'identification de sécurité.

Cette section décrit les rôles AWS liés aux services créés spécifiquement pour IPAM et les politiques gérées associées aux rôles liés aux services 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 un VPC, consultez la section [Identity and access management for Amazon VPC](#) dans le Guide d'utilisation d'Amazon VPC.

## Table des matières

- [Rôles liés à un service pour IPAM](#)
- [AWS politiques gérées pour IPAM](#)
- [Exemple de stratégie](#)

## Rôles liés à un service pour IPAM

L'IPAM utilise des rôles de Gestion des identités et des accès AWS (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM. Les rôles liés à un service sont prédéfinis par l'IPAM et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service simplifie la configuration de l'IPAM du fait que vous n'avez pas besoin d'ajouter manuellement les autorisations requises. L'IPAM définit les autorisations de ses rôles liés à un service. De plus, sauf indication contraire, seul l'IPAM peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

## Autorisations de rôles liés 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 [AWS politiques gérées pour IPAM](#).

Une [politique d'approbation 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 [Intégration d'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 la section [Editing a service-linked role description](#) dans le Guide d'utilisation d'IAM.

## Modifier le 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 à l'aide 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.

## AWS politiques gérées pour IPAM

Si vous utilisez IPAM avec un seul AWS compte et que vous créez un IPAM, la politique AWSIPAMServiceRolePolicygérée 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 AWSIPAMServiceRolePolicygérée est automatiquement créée dans votre compte IAM et dans chacun des comptes membres de vos 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 :

- Surveillance CIDRs associée aux ressources réseau de tous les membres de votre AWS organisation.
  - Stockez les statistiques relatives à l'IPAM sur Amazon CloudWatch, telles que l'espace d'adresses IP disponible dans vos pools IPAM et le nombre de ressources CIDRs conformes aux règles d'allocation.
  - Modifier et lire des listes de préfixes gérées.

L'exemple suivant affiche les détails de la stratégie gérée créée.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAMDiscoveryDescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
```

```
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:ModifyManagedPrefixList",
        "globalaccelerator>ListAccelerators",
        "globalaccelerator>ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations>ListAccounts",
        "organizations>ListDelegatedAdministrators",
        "organizations>ListChildren",
        "organizations>ListParents",
        "organizations:DescribeOrganizationalUnit"
    ],
    "Resource": "*"
},
{
    "Sid": "CloudWatchMetricsPublishActions",
    "Effect": "Allow",
    "Action": "cloudwatch:PutMetricData",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": "AWS/IPAM"
        }
    }
}
]
```

La première déclaration de l'exemple précédent permet à l'IPAM de surveiller l' CIDRs utilisation par votre AWS compte unique ou par les membres de votre AWS organisation.

La deuxième instruction de l'exemple précédent utilise la clé de `cloudwatch:PutMetricData` condition pour permettre à IPAM de stocker les métriques IPAM dans votre espace de noms AWS/ IPAM [Amazon CloudWatch](#). Ces métriques sont utilisées par le AWS Management Console pour afficher des données sur les allocations dans vos pools et étendues IPAM. Pour de plus amples informations, veuillez consulter [Contrôle de l'utilisation des CIDR à l'aide du tableau de bord IPAM](#).

## Mises à jour de la politique AWS gérée

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour IPAM depuis que ce service a commencé à suivre ces modifications.

Modifier	Description	Date
AWSIPAMServiceRolePolicy	Actions ajoutées à la politique AWSIPAMService RolePolicy gérée (ec2:ModifyManagedPrefixList,ec2:DescribeManagedPrefixLists, et ec2:GetManagedPrefixListEntries) pour permettre à IPAM de modifier et de lire les listes de préfixes gérées.	31 octobre 2025
AWSIPAMServiceRolePolicy	Actions ajoutées à la politique AWSIPAMService RolePolicy gérée (organizations>ListChildren, organizations>ListParents, et organizations>DescribeOrganizationalUnit) pour permettre à IPAM d'obtenir les détails des unités organisationnelles (OUs) dans les AWS Organisations afin que les clients puissent utiliser IPAM	21 novembre 2024

Modifier	Description	Date
	au niveau de l'unité d'organisation.	
AWSIPAMServiceRolePolicy	Action ajoutée à la politique AWSIPAMService RolePolicy gérée (ec2:GetIpamDiscoveredPublicAddresses ) pour permettre à IPAM d'obtenir des adresses IP publiques lors de la découverte des ressources.	13 novembre 2023
AWSIPAMServiceRolePolicy	Actions ajoutées à la politique AWSIPAMService RolePolicy gérée (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 des ressources.	1er novembre 2023

Modifier	Description	Date
AWSIPAMServiceRolePolicy	Deux actions ont été ajoutées à la politique AWSIPAMService RolePolicy gérée (ec2:GetIpamDiscoveredAccounts et ec2:GetIpamDiscoveredResources) pour permettre à IPAM de surveiller les AWS comptes et les ressources CIDRs lors de la découverte des ressources.	25 janvier 2023
IPAM a commencé à suivre les modifications	L'IPAM a commencé à suivre les modifications apportées à ses politiques AWS gérées.	2 décembre 2021

## Exemple de stratégie

L'exemple de politique présenté dans cette section contient toutes les actions Gestion des identités et des accès AWS (IAM) pertinentes pour une utilisation complète de l'IPAM. Selon la façon dont vous utilisez IPAM, il se peut que vous n'ayez pas besoin d'inclure toutes les actions IAM. Pour une expérience complète d'utilisation de la console IPAM, vous devrez peut-être inclure des actions IAM supplémentaires pour des services tels que AWS Organizations, AWS Resource Access Manager (AWS RAM) et Amazon CloudWatch.

JSON

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

```
        "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.

Name	Par défaut	Ajustable
Blocs CIDR publics contigus fournis par Amazon IPv4	2	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Longueur du masque réseau de blocs CIDR public IPv4 contigu fourni par Amazon	/29	La taille acceptable est comprise entre /29 et /30. Pour demander une augmentation, contactez le AWS Support Center comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Longueur du masque réseau de blocs IPv6 CIDR fourni par Amazon	/52	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du

Name	Par défaut	Ajustable
		Références générales AWS.
Blocs IPv6 CIDR fournis par Amazon par pool régional	1	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Numéros de système autonomes (ASNs) que vous pouvez apporter à l'IPAM	5	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
CIDRs par piscine	50	<a href="#">Oui</a>
Cibles activées conformément à la politique IPAM	100	Oui. Pour demander un ajustement du quota, contactez le AWS Support Center comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Administrateurs IPAM par organisation	1	Non
IPAMs par région	1	<a href="#">Non</a>

Name	Par défaut	Ajustable
Politiques IPAM par IPAM	10	Oui. Pour demander un ajustement du quota, contactez le AWS Support Center comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Règles d'allocation des politiques IPAM par paire ressource-locale*	10	Oui. Pour demander un ajustement du quota, contactez le AWS Support Center comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
<a href="#">Exclusions d'unités organisationnelles par découverte de ressources</a>	10	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Profondeur de groupe (nombre de groupes dans les groupes)	10	<a href="#">Oui</a>
Groupes par portée	50	<a href="#">Oui</a>
Résolveurs de listes de préfixes par IPAM	10	<a href="#">Oui</a>

Name	Par défaut	Ajustable
Cibles de résolveur de liste de préfixes par résolveur de liste de préfixes	50	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Règles par résolveur de liste de préfixes	100	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Entrées CIDR par version du résolveur de listes de préfixes	1 000	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Associations de découvertes de ressources par IPAM	5	<a href="#">Oui</a>
Découvertes de ressources par région	1	<a href="#">Non</a>

Name	Par défaut	Ajustable
<a href="#">Métriques d'utilisation des ressources</a>	50	Oui. Contactez le Centre de AWS support comme indiqué dans la section <a href="#">Quotas de AWS service</a> du Références générales AWS.
Portées par IPAM	5	<a href="#">Oui</a> . 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.

\* Paire ressource-locale : Lorsque vous définissez des règles d'allocation, vous devez spécifier à la fois un type de ressource (une AWS ressource, par exemple EIPs ALBs, ou des clusters RDS) et un paramètre régional (la AWS région ou la zone locale où la règle s'applique). Les règles d'allocation sont limitées à cette combinaison de type de ressource et de paramètres régionaux. Par exemple, si vous définissez une politique pour us-east-1, vous pouvez définir jusqu'à 10 règles pour cette paire ressource-locale spécifique\*.

# Tarification d'IPAM

Amazon VPC IP Address Manager (IPAM) est un service qui vous aide à gérer votre espace d'adresses IP sur l'ensemble de vos AWS ressources et de vos réseaux sur site. L'IPAM fournit un moyen centralisé de planifier, de surveiller et de contrôler les adresses IP utilisées par vos ressources AWS et celles utilisées sur site.

Cette section explique comment afficher les informations relatives à la tarification et à vos coûts IPAM actuels.

## Table des matières

- [Afficher les informations sur la tarification](#)
- [Consultez vos coûts et votre utilisation actuels à l'aide de AWS Cost Explorer](#)

## 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 la <https://console.aws.amazon.com/cost-management/maison>.
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 USE1- IPAddress Manager-IP-Hours (Hrs) et que us-east-1 est votre région d'origine IPAM, vous verrez le nombre d'heures IP actives facturées par l'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 une adresse IP active pendant 18 heures, 3 adresses IP dans 3 régions différentes, chacune active pendant 6 heures, ou toute combinaison de ces adresses qui totalisent 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

Bien que le site de documentation technique d'AWS soit une ressource complète, il existe de nombreux autres endroits pour trouver des informations sur les services AWS. Les blogs, les livres blancs, les études de cas et les forums communautaires d'AWS peuvent fournir des informations précieuses, des exemples concrets ainsi que des points de vue alternatifs au-delà des détails techniques officiels. L'exploration de ces diverses sources peut vous permettre de mieux comprendre les offres AWS.

Les ressources connexes suivantes peuvent vous aider à utiliser le Gestionnaire d'adresses IP d'Amazon VPC :

- [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.
- [Visualiser la gestion et la planification des adresses IP d'entreprise avec la carte CIDR](#) : un blog AWS qui explique comment visualiser l'ensemble de votre environnement IPv4 et IPv6 à l'aide de la CIDR IPAM dans la console IPAM.

# Historique de document pour IPAM

Le tableau suivant décrit les versions d'IPAM.

Fonctionnalité	Description	Date de parution
<a href="#"><u>Utilisez votre propre adresse IP pour CloudFront utiliser IPAM</u></a>	Utilisez IPAM pour gérer votre BYOIP CIDRs pour les services AWS internationaux, en commençant CloudFront par les services anycast.	21 novembre 2025
<a href="#"><u>Définir une stratégie IPv4 d'allocation publique avec les politiques de l'IPAM</u></a>	Vous pouvez désormais utiliser les politiques IPAM pour définir des règles qui mappent les AWS services à des pools IPAM spécifiques, ce qui permet de définir une stratégie d' IPv4 allocation publique.	19 novembre 2025
<a href="#"><u>Intégrer l'IPAM à l'infrastructure Infoblox</u></a>	Vous pouvez désormais intégrer l'IPAM à l'infrastructure Infoblox, ce qui vous permet de gérer les adresses AWS IP par le biais de vos flux de travail Infoblox existants tout en bénéficiant de fonctionnalités cloud natives. AWS Cette intégration est disponible pour les zones privées et nécessite le niveau avancé d'IPAM.	7 novembre 2025
<a href="#"><u>Automatisation des mises à jour des listes de préfixes</u></a>	Vous pouvez désormais utiliser les résolveurs de listes de préfixes IPAM pour automatiser les mises à jour des listes de préfixes en fonction du pool IPAM. CIDRs	31 octobre 2025
<a href="#"><u>Gestion des alarmes depuis la console IPAM</u></a>	Vous pouvez désormais créer et gérer des CloudWatch alarmes Amazon directement depuis la console IPAM. Les alarmes liées à l'IPAM apparaîtront sous forme de barres d'avertissement et d'indicateurs visuels en cas d'état INSUFFICIENT_DATA ou ALARME.	21 août 2025

Fonctionnalité	Description	Date de parution
<a href="#"><u>Activation de la répartition des coûts</u></a>	Lorsque vous activez la répartition des coûts, vous répartissez les <a href="#"><u>frais des adresses IP actives</u></a> entre les comptes utilisant les adresses IP plutôt qu'auprès du propriétaire de l'IPAM. Cette fonction s'avère utile pour les grandes entreprises dans lesquelles l'administrateur IPAM délégué gère les adresses IP de manière centralisée à l'aide de l'IPAM et où chaque compte est responsable de sa propre utilisation, éliminant ainsi le besoin de calculs de facturation manuels.	1er mai 2025
<a href="#"><u>Exclure les unités organisationnelles d'IPAM</u></a>	Si votre IPAM est intégré à AWS Organizations, vous pouvez désormais exclure des unités organisationnelles de l'IPAM. IPAM ne générera pas les adresses IP des comptes dans le cadre des exclusions d'unités organisationnelles.	21 novembre 2024
<a href="#"><u>AWS mises à jour de politiques gérées</u></a> - Mise à jour d'une politique existante	AWSIPAMServiceRolePolicy Mise à jour existante.	21 novembre 2024
<a href="#"><u>Allouer des adresses IP Elastic séquentielles à partir d'un groupe IPAM</u></a>	IPAM vous permet désormais de fournir des IPv4 blocs publics appartenant à Amazon aux pools IPAM et d'allouer des adresses IP élastiques séquentielles de ces pools aux ressources. AWS Les adresses IP Elastic séquentielles vous permettent de simplifier vos besoins en matière de mise en réseau et de listes d'autorisations de sécurité.	28 août 2024

Fonctionnalité	Description	Date de parution
<a href="#"><u>IPv6 GUA privé et ULAs</u></a>	<p>Vous pouvez désormais fournir des plages IPv6 GUA et ULA privées à un pool IPAM dans un périmètre privé. Les IPv6 adresses privées ne sont disponibles que dans IPAM. Pour plus d'informations sur l' IPv6 adressage privé, consultez la section <a href="#"><u>IPv6 Adresses privées</u></a> dans le guide de l'utilisateur Amazon VPC.</p>	8 août 2024
<a href="#"><u>Niveaux gratuits et avancés de l'IPAM</u></a>	<p>Vous pouvez désormais choisir entre le niveau gratuit et le niveau avancé pour votre IPAM.</p>	17 novembre 2023
<a href="#"><u>Public IP Insights</u></a>	<p>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 <a href="#"><u>informations relatives aux adresses IP publiques sur Amazon CloudWatch</u></a>.</p>	17 novembre 2023
<a href="#"><u>Planifier l'espace d'adresse IP VPC pour les allocations IP de sous-réseau</u></a>	<p>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.</p>	17 novembre 2023
<a href="#"><u>Apportez votre propre ASN (BYOASN)</u></a>	<p>Vous pouvez désormais apporter votre propre numéro de système autonome (ASN) à AWS.</p>	17 novembre 2023
<a href="#"><u>AWS mises à jour de politiques gérées</u></a> - Mise à jour d'une politique existante	<p>AWSIPAMServiceRolePolicy Mise à jour existante.</p>	17 novembre 2023

Fonctionnalité	Description	Date de parution
<a href="#"><u>AWS mises à jour de politiques gérées</u></a> - Mise à jour d'une politique existante	AWSIPAMServiceRolePolicy Mise à jour existante.	1er novembre 2023
<a href="#"><u>Métriques d'utilisation des ressources</u></a>	L'IPAM publie désormais sur Amazon des métriques d'utilisation des adresses IP pour les ressources surveillées par l'IPAM. CloudWatch	2 août 2023
<a href="#"><u>Public IP Insights</u></a>	Public IP Insights affiche toutes les IPv4 adresses publiques utilisées par les services de cette région dans votre compte. Vous pouvez utiliser ces informations pour identifier l'utilisation des IPv4 adresses publiques et consulter les recommandations pour libérer les adresses IP élastiques non utilisées.	28 juillet 2023
<a href="#"><u>AWS mises à jour de politiques gérées</u></a> - Mise à jour d'une politique existante	AWSIPAMServiceRolePolicy Mise à jour existante.	25 janvier 2023
<a href="#"><u>Intégration d'IPAM à des comptes extérieurs à votre organisation</u></a>	Vous pouvez désormais gérer les adresses IP extérieures à votre organisation à partir d'un seul compte IPAM et partager des pools IPAM avec les comptes d'autres Organisations AWS .	25 janvier 2023
Bloc CIDR IPv6 contigu fourni par Amazon pour les pools IPAM	Lorsque vous créez un pool IPAM dans le périmètre public, vous pouvez désormais fournir un bloc CIDR IPv6 contigu fourni par Amazon au pool. Pour de plus amples informations, veuillez consulter <a href="#"><u>Créez des groupes d'adresses IPv6 dans votre IPAM</u></a> .	25 janvier 2023
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.