IP Address Manager

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: IP Address Manager

Table of Contents

O que é o IPAM? ... 1
Como funciona o IPAM ... 2
Conceitos básicos do IPAM ... 4
Acessar o IPAM ... 4
Configurar as opções de integração para o IPAM ... 5
Integrar o IPAM a contas em uma organização da AWS Organizations ... 6
Integrar o IPAM a contas fora de sua organização ... 9
Usar o IPAM com uma única conta ... 11
Criar um IPAM ... 12
Planejar o provisionamento de endereços IP ... 15
Exemplo de planos de grupo do IPAM ... 16
Criar grupos de IPv4 ... 19
Criar grupos de IPv6 ... 29
Alocar CIDRs ... 37
Ciar uma VPC que usa um CIDR de um grupo do IPAM ... 38
Alocar manualmente um CIDR a um grupo para reservar o espaço de endereços IP ... 39
Gerenciar o espaço de endereços IP no IPAM ... 41
Automatizar atualizações da lista de prefixos com o IPAM ... 42
O problema que isso resolve ... 42
Como funciona ... 42
Quando usar ... 43
Pré-requisitos ... 43
Etapas de configuração ... 43
Alterar o estado de monitoramento dos CIDRs da VPC ... 49
Criar escopos adicionais ... 50
Excluir um IPAM ... 52
Excluir um grupo ... 54
Excluir um escopo ... 55
Desprovisionar CIDRs de um grupo ... 56
Editar um grupo do IPAM ... 57
Habilitar a distribuição de custos ... 58
Integrar o VPC IPAM à infraestrutura da Infoblox ... 59
Visão geral do processo de integração ... 59
Quando usar essa integração ... 60

Pré-requisitos ... 43
Perfil do IAM para Infoblox ... 60
Configurar a integração da Infoblox no IPAM da VPC ... 61
Próximas etapas ... 62
Habilitar o provisionamento de CIDRs de GUA IPv6 privado ... 62
Impor o uso do IPAM para a criação de VPCs com SCPs ... 64
Aplicar o IPAM ao criar VPCs ... 65
Aplique um grupo do IPAM ao criar VPCs ... 65
Aplique o IPAM para todas, exceto uma determinada lista de UOs ... 66
Excluir unidades organizacionais do IPAM ... 67
Como funcionam as exclusões de UO ... 68
Adicionar ou remover exclusões de UO ... 69
Criar um nível de IPAM ... 75
Modificar regiões operacionais do IPAM ... 77
Provisionar CIDRs para um grupo ... 78
Mover CIDRs da VPC entre escopos ... 80
Como definir a estratégia de alocação de IPv4 ... 81
Liberar uma alocação ... 86
Compartilhar um grupo do IPAM usando o AWS RAM ... 88
Trabalhar com descobertas de recursos ... 91
Criar uma descoberta de recursos ... 92
Visualizar detalhes da descoberta de recursos ... 93
Compartilhar uma descoberta de recursos ... 95
Associar uma descoberta de recursos a um IPAM ... 98
Desassociar uma descoberta de recursos ... 99
Excluir uma descoberta de recursos ... 100
Rastrear uso de endereços IP no IPAM ... 102
Monitorar o uso do CIDR com o painel do IPAM ... 102
Monitorar o uso do CIDR por recurso ... 106
Monitorar o IPAM com o Amazon CloudWatch ... 110
Gerenciar alarmes ... 111
Métricas de escopo e grupo ... 112
Métricas de utilização de recursos ... 116
Ver histórico de endereços IP ... 122
Visualizar insights de IPs públicos ... 126
Tutoriais ... 131

Conceitos básicos do IPAM usando a AWS CLI 131
Pré-requisitos 43
Criar um IPAM 132
Obtenção do ID do escopo do IPAM 132
Criar um grupo de IPv4 de nível superior 133
Criação de um grupo de endereços IPv4 regional 134
Criar um grupo de desenvolvimento de IPv4 135
Criação de uma VPC usando um bloco CIDR do grupo do IPAM 136
Verificação da alocação no grupo do IPAM 136
Solução de problemas 136
Limpar recursos 137
Próximas etapas 139
Criar um IPAM e grupos usando o console 139
Pré-requisitos 43
Como o AWS Organizations se integra ao IPAM 140
Etapa 1: delegar um administrador do IPAM 141
Etapa 2: criar um IPAM 143
Etapa 3: criar um grupo do IPAM de nível superior 145
Etapa 4: criar grupos regionais do IPAM 150
Etapa 5: criar um grupo de desenvolvimento pré-produção 154
Etapa 6: compartilhar o grupo do IPAM 158
Etapa 7: criar uma VPC com um CIDR alocado em um grupo do IPAM 164
Etapa 8: limpeza 167
Criar um IPAM e grupos usando a AWS CLI 169
Etapa 1: habilitar o IPAM na sua organização 170
Etapa 2: criar um IPAM 170
Etapa 3: criar um grupo de endereços IPv4 172
Etapa 4: provisionar um CIDR para o grupo de nível superior 174
Etapa 5. Criar um grupo regional com o CIDR originado do grupo de nível superior 175
Etapa 6: provisionar um CIDR para o grupo regional 177
Etapa 7. Criar um compartilhamento do RAM para habilitar atribuições de IP nas contas 179
Etapa 8. Crie uma VPC 179
Etapa 9. Limpeza 180
Visualizar o histórico de endereços IP com a AWS CLI 181
Visão geral 181
Cenários 182

Traga o seu ASN para o IPAM 190
Pré-requisitos de integração para seu ASN 191
Etapas do tutorial 191
Trazer seus endereços IP para o IPAM 195
Verificar o controle do domínio 196
BYOIP com o console e a CLI da AWS 203
BYOIP apenas com a AWS CLI 231
Traga seu próprio IP para o CloudFront usando o IPAM 278
Transferir um CIDR IPv4 BYOIP para o IPAM 282
Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM 283
Etapa 2: obter o ID de escopo público do IPAM 284
Etapa 3: criar um grupo do IPAM 285
Etapa 4: compartilhar o grupo do IPAM usando o AWS RAM 287
Etapa 5: transferir um CIDR IPv4 BYOIP existente para o IPAM 289
Etapa 6: visualizar o CIDR no IPAM 292
Etapa 7: limpeza 292
Planeje o espaço de endereço IP da VPC para alocações IP de sub-rede 295
Etapa 1: criar uma VPC 297
Etapa 2: Criar um grupo de planejamento de recursos 298
Etapa 3: Criar grupos de sub-redes 298
Etapa 4: Criar sub-redes 299
Etapa 5: limpeza 300
Alocar endereços IP elásticos sequenciais de um grupo do IPAM 301
Etapa 1: criar um IPAM 302
Etapa 2: criar um grupo do IPAM e provisionar um CIDR 305
Etapa 3: alocar um endereço IP elástico do grupo 309
Etapa 4: associar o endereço IP elástico a uma instância do EC2 310
Etapa 5: rastrear e monitorar o uso do grupo 311
Limpeza 313
Identificar e acessar o gerenciamento no IPAM 314
Funções vinculadas ao serviço do IPAM 314
Permissões de perfil vinculado ao serviço 315
Criar a função vinculada ao serviço 315
Editar a função vinculada ao serviço 316
Excluir a função vinculada ao serviço 316
Políticas do IPAM gerenciadas 317

Atualiza a política gerenciada pela AWS 319
Exemplo de política 321
Cotas 324
Preços 329
Visualizar informações sobre preços 329
Veja seus custos e uso atuais usando o AWS Cost Explorer 329
Informações relacionadas 331
Histórico do documento 332

O que é o IPAM?

O IP Address Manager da Amazon VPC (IPAM) é um recurso da VPC que facilita o planejamento, o rastreamento e o monitoramento de endereços IP de suas workloads da AWS. Você pode usar os fluxos de trabalho automatizados do IPAM para gerenciar endereços IP com mais eficiência.

Você pode usar IPAM para fazer o seguinte:

- Organizar o espaço de endereços IP em domínios de roteamento e segurança
- Monitorar o espaço de endereços IP em uso e monitorar os recursos que estão usando esse espaço em relação às regras de negócios
- Exibir o histórico de atribuições de endereços IP em sua organização
- Alocar CIDRs automaticamente para VPCs usando regras de negócios específicas
- Solucionar problemas de conectividade de rede
- Habilitar o compartilhamento entre regiões e entre contas de seus endereços Bring Your Own IP (BYOIP, Traga seu próprio IP)
- Provisionar blocos CIDR IPv6 contíguos fornecidos pela Amazon para grupos para criação de VPC

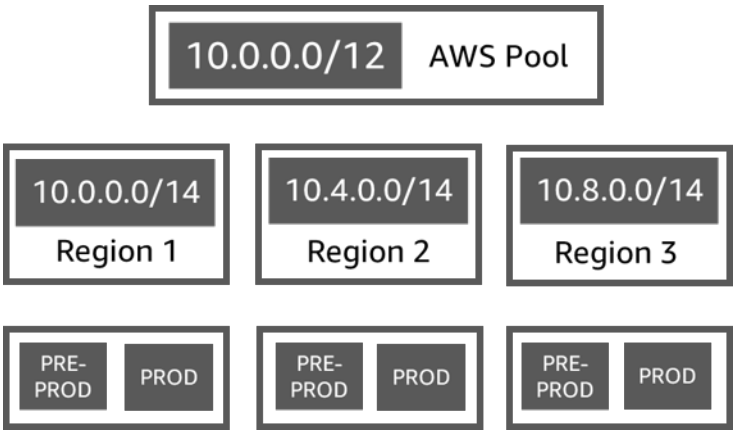
Este guia consiste nas seguintes seções:

- Como funciona o IPAM: conceitos e terminologia do IPAM
- Conceitos básicos do IPAM: etapas para habilitar o gerenciamento de endereços IP em toda a empresa com o AWS Organizations, criar um IPAM e planejar o uso de endereços IP.
- Gerenciar o espaço de endereços IP no IPAM: etapas para gerenciar seu IPAM, escopos, grupos e alocações.
- Rastrear uso de endereços IP no IPAM: etapas para monitorar e rastrear o uso de endereços IP com o IPAM.
- Tutoriais para o IP Address Manager da Amazon VPC: tutoriais detalhados para criar um IPAM e grupos, alocando CIDRs da VPC, e trazer seus próprios CIDRs de endereço IP público ao IPAM.

Como funciona o IPAM

Este tópico explica alguns dos conceitos-chave para ajudar a começar a usar o IPAM.

O diagrama a seguir mostra uma hierarquia de grupos do IPAM para várias Regiões da AWS em um grupo do IPAM de nível superior. Cada grupo regional da AWS tem dois grupos de desenvolvimento do IPAM dentro dele, um para pré-produção e outro de recursos de produção. Para obter mais informações sobre os conceitos do IPAM, consulte as descrições abaixo do diagrama.



Para usar o IP Address Manager da Amazon VPC, primeiro você cria um IPAM.

Ao criar o IPAM, você escolhe a região da AWS em que ele será criado. Ao criar um IPAM, o IPAM da AWS VPC cria automaticamente dois escopos para ele. Os escopos, juntamente com grupos e alocações, são componentes-chave do seu IPAM.

- Um escopo é o contêiner de nível mais alto dentro do IPAM. Quando você cria um IPAM, um escopo público padrão e um escopo privado padrão são criados automaticamente. Cada escopo representa o espaço IP de uma única rede. O escopo privado se destina a todos os endereços IP que não podem ser anunciados para a Internet. O escopo público normalmente é destinado a todos os endereços IP que podem ser anunciados da AWS para a Internet. Observe que, ao provisionar endereços BYOIPv6 para um pool do IPAM, você pode configurar os endereços para não serem anunciados publicamente, embora estejam no escopo público. Os escopos permitem que você reutilize endereços IP em várias redes não conectadas sem causar sobreposição ou conflito de endereços IP. Dentro de um escopo, você cria grupos do IPAM.
- Um grupo é uma coleção de intervalos de endereços IP contíguos (ou CIDRs). Os grupos do IPAM permitem que você organize seus endereços IP de acordo com suas necessidades de roteamento e segurança. Você pode ter vários grupos em um grupo de nível superior. Por exemplo, se você tiver necessidades separadas de roteamento e segurança para aplicações de desenvolvimento

e produção, poderá criar um grupo para cada uma. Nos grupos do IPAM, você aloca CIDRs para recursos da AWS.

- Uma alocação é uma atribuição CIDR de um grupo do IPAM para outro recurso ou grupo do IPAM. Quando você cria uma VPC e escolhe um grupo do IPAM para o CIDR da VPC, o CIDR é alocado do CIDR provisionado para o grupo do IPAM. Você pode monitorar e gerenciar a alocação com o IPAM.

O IPAM pode gerenciar e monitorar espaço IPv6 público e privado. Para obter mais informações sobre o endereçamento IPv6, consulte Endereços IPv6 no Manual do usuário da Amazon VPC.

Para começar e criar um IPAM, consulte Conceitos básicos do IPAM.

Conceitos básicos do IPAM

Siga as etapas nesta seção para começar a usar o IPAM. Esta seção tem como objetivo ajudar você a começar rapidamente com o IPAM, mas você pode descobrir que o que pode ser alcançado com as etapas desta seção não atende às suas necessidades. Para obter mais informações sobre as diferentes formas de usar o IPAM, consulte Planejar o provisionamento de endereços IP e Tutoriais para o IP Address Manager da Amazon VPC.

Nesta seção, você começará acessando o IPAM e decidindo se deseja delegar uma conta do IPAM. Ao final desta seção, você terá criado um IPAM, criado vários grupos de endereços IP e alocado um CIDR em um grupo para uma VPC.

Tarefas

- Acessar o IPAM
- Configurar as opções de integração para o IPAM
- Criar um IPAM
- Planejar o provisionamento de endereços IP
- Alocar CIDRs de um grupo do IPAM

Acessar o IPAM

Como acontece com outros serviços da AWS, você pode criar, acessar e gerenciar seu IPAM usando os seguintes métodos:

- Console de Gerenciamento da AWS: fornece uma interface da Web que pode ser usada para criar e gerenciar seu IPAM. Consulte https://console.aws.amazon.com/ipam/.
- AWS Command Line Interface (AWS CLI): fornece comandos para um amplo conjunto de serviços da AWS, incluindo a Amazon VPC. A AWS CLI é compatível com Windows, macOS e Linux. Para obter a AWS CLI, consulte AWS Command Line Interface.
- AWS SDKs: fornecem APIs específicas da linguagem. Os AWS SDKs cuidam de muitos dos detalhes da conexão, como calcular assinaturas, lidar com tentativas de solicitação e lidar com erros. Para obter mais informações, consulte AWS SDKs.
- API de consulta: fornece ações de API de baixo nível que são chamadas usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta de acessar o IPAM. No entanto, ela exige que a aplicação trate detalhes de baixo nível, como gerar o hash para assinar a solicitação e tratar

erros. Para obter mais informações, consulte Ações do IPAM da Amazon na Referência da API do Amazon EC2.

Este guia se concentra principalmente em usar Console de Gerenciamento da AWS para criar, acessar e gerenciar seu IPAM. Em cada descrição de como concluir um processo no console, incluímos links para a Referência de comando AWS CLI para que você possa fazer a mesma tarefa usando a AWS CLI.

Se você é um usuário iniciante do IPAM, revise Como funciona o IPAM para saber mais sobre a função do IPAM na Amazon VPC e, em seguida, continue com as instruções em Configurar as opções de integração para o IPAM.

Configurar as opções de integração para o IPAM

Esta seção descreve as opções de como você pode integrar o IPAM com o AWS Organizations, outras contas da AWS ou usá-lo com uma única conta da AWS.

Antes de começar a usar o IPAM, você deve escolher uma das opções nesta seção para permitir que o IPAM monitore CIDRs associados aos recursos de rede do EC2 e armazene métricas:

- Para habilitar a integração do IPAM ao AWS Organizations a fim de habilitar o serviço IPAM do Amazon VPC a gerenciar e monitorar recursos de rede criados por todas as contas-membro do AWS Organizations, consulte Integrar o IPAM a contas em uma organização da AWS Organizations.
- Após fazer a integração com o AWS Organizations, para integrar o IPAM com contas fora da sua organização, consulte Integrar o IPAM a contas fora de sua organização.
- Para usar uma única conta da AWS com o IPAM e habilitar o serviço IPAM da Amazon VPC para gerenciar e monitorar os recursos de rede que você cria com a conta única, consulte Usar o IPAM com uma única conta.

Se você não escolher uma dessas opções, ainda poderá criar recursos IPAM, como grupos, mas não verá métricas em seu painel e não poderá monitorar o status dos recursos.

Conteúdo

- Integrar o IPAM a contas em uma organização da AWS Organizations
- Integrar o IPAM a contas fora de sua organização

- Usar o IPAM com uma única conta

Integrar o IPAM a contas em uma organização da AWS Organizations

Opcionalmente, você pode seguir os passos nesta seção para integrar o IPAM ao AWS Organizations e delegar uma conta de membro, como a conta do IPAM.

A conta do IPAM é responsável por criar um IPAM e usá-lo para gerenciar e monitorar o uso de endereços IP.

Integrar o IPAM ao AWS Organizations e delegar um administrador do IPAM apresentam os seguintes benefícios:

- Compartilhar seus grupos do IPAM com sua organização: quando você delega uma conta do IPAM, o IPAM habilita outra contas de membros do AWS Organizations na organização para alocar CIDRs de grupos do IPAM que são compartilhados usando o AWS Resource Access Manager (RAM). Para obter mais informações sobre como configurar uma organização, consulte O que são AWS Organizations? no Guia do usuário do AWS Organizations.
- monitorar o uso de endereços IP em sua organização: quando você delega uma conta do IPAM, você concede permissão ao IPAM para monitorar o uso de IPs em todas as suas contas. Como resultado, o IPAM importa automaticamente CIDRs que são usados por VPCs existentes em outras contas de membros do AWS Organizations.

Se você não delegar uma conta de membro do AWS Organizations como uma conta do IPAM, o IPAM monitorará os recursos somente na conta da AWS que você usa para criar o IPAM.

> **Note**
>
> Ao integrar ao AWS Organizations:
>
> - É necessário habilitar a integração com o AWS Organizations usando o IPAM no Console de Gerenciamento da AWS ou o comando da AWS CLI enable-ipam-organization-admin-account. Isso garante que a função vinculada ao serviço `AWSServiceRoleForIPAM` seja criada. Se você habilitar o acesso confiável com o AWS Organizations usando o Console do AWS Organizations ou o comando register-delegated-administrator da AWS CLI, a função vinculada a serviços `AWSServiceRoleForIPAM` não foi criada e você não pode gerenciar ou monitorar recursos dentro de sua organização.

- A conta do IPAM deve ser uma conta de membro do AWS Organizations. Não é possível utilizar a conta de gerenciamento do AWS Organizations como a conta do IPAM. Para verificar se seu IPAM já está integrado ao AWS Organizations, use as etapas abaixo e visualize os detalhes da integração nas configurações da organização.
- O IPAM cobra por cada endereço IP ativo que ele monitora nas contas de membros da sua organização. Para obter mais informações sobre a definição de preço, consulte Preço do IPAM.
- Você deve ter uma conta no AWS Organizations e uma conta de gerenciamento configuradas com uma ou mais contas de membro. Para obter mais informações sobre os tipos de conta, consulte Terminologia e conceitos no Guia do usuário do AWS Organizations. Para obter mais informações sobre a configuração de uma organização, consulte Conceitos básicos do AWS Organizations.
- A conta IPAM deve ter usar um perfil do IAM com uma política do IAM anexada a ele que permita a ação `iam:CreateServiceLinkedRole`. Ao criar o IPAM, você cria automaticamente a função vinculada ao serviço AWSServiceRoleForIPAM.
- A conta de usuário associada à conta de gerenciamento do AWS Organizations deve usar um perfil do IAM que tenha as seguintes ações da política do IAM anexadas:
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`
  - `iam:CreateServiceLinkedRole`

  Para obter mais informações sobre como criar perfis do IAM, consulte Criar uma função para delegar permissões a um usuário do IAM no Manual do usuário do IAM.
- A conta de usuário associada à conta de gerenciamento do AWS Organizations deve usar um perfil do IAM que tenha as seguintes ações da política do IAM anexadas para listar os administradores delegados do AWS Orgs: `organizations:ListDelegatedAdministrators`

AWS Management Console

Para selecionar uma conta do IPAM

1. Faça login na conta de gerenciamento do AWS Organizations e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No Console de Gerenciamento da AWS, escolha a Região da AWS em que você deseja trabalhar com o IPAM.
3. No painel de navegação, selecione Organization settings (Configurações da organização).
4. A opção Delegar apenas estará disponível se você estiver conectado ao console como a conta de gerenciamento do AWS Organizations. Selecione Delegar.
5. Insira o ID da conta da AWS para uma conta do IPAM. O administrador do IPAM deve ser uma conta membro do AWS Organizations.
6. Escolha Salvar alterações.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

- Para delegar uma conta de administrador do IPAM usando a AWS CLI, use o seguinte comando: enable-ipam-organization-admin-account

Ao delegar uma conta de membro do Organizations como uma conta do IPAM, o IPAM cria automaticamente uma função do IAM vinculada ao serviço em todas as contas de membro em sua organização. O IPAM monitora o uso de endereços IP nessas contas assumindo a função do IAM vinculada ao serviço em cada conta de membro, descobrindo os recursos e respectivos CIDRs e integrando-os ao IPAM. Os recursos em todas as contas de membro poderão ser detectados pelo IPAM, independentemente de sua Unidade Organizacional. Se houver contas de membro que criaram uma VPC, por exemplo, você verá a VPC e o respectivo CIDR na seção “Resources” (Recursos) do console do IPAM.

> **Important**
>
> A função da conta de gerenciamento do AWS Organizations que delegou o administrador do IPAM está concluída agora. Para continuar usando o IPAM, a conta de administrador do IPAM deve fazer login no IPAM da Amazon VPC e criar um IPAM.

Integrar o IPAM a contas fora de sua organização

Esta seção descreve como integrar o IPAM com contas da AWS fora de sua organização. Para executar as etapas desta seção, você já deve ter concluído as etapas em Integrar o IPAM a contas em uma organização da AWS Organizations e delegado uma conta do IPAM.

A integração do IPAM com contas da AWS fora da sua organização permite que você faça o seguinte:

- Gerencie endereços IP fora da sua organização a partir de uma única conta do IPAM.
- Compartilhe grupos do IPAM com serviços de terceiros hospedados por outras contas da AWS em outros AWS Organizations.

Após integrar o IPAM com contas da AWS fora da sua organização, você pode compartilhar um grupo de IPAM diretamente com as contas desejadas de outras organizações.

Conteúdo

- Considerações e limitações
- Visão geral do processo

Considerações e limitações

Esta seção apresenta considerações e limitações para integrar o IPAM com contas fora da sua organização:

- Quando você compartilha uma descoberta de recursos com outra conta, os únicos dados trocados são os dados de monitoramento do endereço IP e do status da conta. Você pode visualizar esses dados antes de compartilhá-los usando os comandos da CLI get-ipam-discovered-resource-cidrs e get-ipam-discovered-accounts ou as APIs GetIpamDiscoveredResourceCidrs e GetIpamDiscoveredAccounts. Nenhum dado da organização (como os nomes das unidades

organizacionais em sua organização) é compartilhado para descobertas de recursos que monitoram recursos em uma organização.

- Quando você cria uma descoberta de recursos, a descoberta de recursos monitora todos os recursos visíveis na conta do proprietário. Se a conta do proprietário for uma conta da AWS de serviço de terceiros que cria recursos para vários de seus próprios clientes, esses recursos serão descobertos pela descoberta do recurso. Se a conta da AWS de serviço de terceiros compartilhar a descoberta de recursos com uma conta da AWS de usuário final, o usuário final terá visibilidade dos recursos dos outros clientes do serviço terceirizado da AWS. Por esse motivo, o serviço terceirizado da AWS deve ter cuidado ao criar e compartilhar descobertas de recursos ou usar uma conta da AWS distinta para cada cliente.

Visão geral do processo

Esta seção explica como integrar o IPAM com contas da AWS fora de sua organização. Ela se refere aos tópicos abordados em outras seções deste guia. Mantenha esta página visível e abra os tópicos vinculados abaixo em uma nova janela para que você possa retornar a esta página a fim de obter orientação.

Quando você integra o IPAM com contas da AWS fora da sua organização, há 4 contas da AWS envolvidas no processo:

- Proprietário da organização primária: a conta de gerenciamento do AWS Organizations da organização 1.
- Conta do IPAM da organização primária: a conta de administrador delegado do IPAM para a organização 1.
- Proprietário da organização secundária: a conta de gerenciamento do AWS Organizations da organização 2.
- Conta de administrador da organização secundária: a conta de administrador delegado do IPAM para a organização 2.

Etapas

1. O proprietário da organização primária delega um membro de sua organização como a conta do IPAM da organização primária (consulte Integrar o IPAM a contas em uma organização da AWS Organizations).
2. A conta do IPAM da organização primária cria um IPAM (consulte Criar um IPAM).

3. O proprietário da organização secundária delega um membro de sua organização como a conta de administrador da organização secundária (consulte Integrar o IPAM a contas em uma organização da AWS Organizations).
4. A conta de administrador da organização secundária cria uma descoberta de recursos e a compartilha com a conta do IPAM da organização primária usando o AWS RAM (consulte Criar uma descoberta de recursos para integração com outro IPAM e Compartilhar uma descoberta de recursos com outra conta da AWS). A descoberta de recursos deve ser criada na mesma região de origem da organização primária do IPAM.
5. A conta do IPAM da organização primária aceita o convite de compartilhamento de recursos usandoAWS RAM (consulte Aceitação e rejeição de convites para compartilhamento de recursos no Guia do usuário do AWS RAM).
6. A conta do IPAM da organização primária associa a descoberta de recursos ao IPAM (consulte Associar uma descoberta de recursos a um IPAM).
7. Agora, a conta do IPAM da organização primária pode monitorar e/ou gerenciar os recursos do IPAM criados pelas contas na organização secundária.
8. (Opcional) A conta do IPAM da organização primária compartilha grupos do IPAM com contas de membros na organização secundária (consulte Compartilhar um grupo do IPAM usando o AWS RAM).
9. (Opcional) Se a conta do IPAM da organização primária quiser parar de descobrir recursos na organização secundária, ela poderá desassociar a descoberta de recursos do IPAM (consulte Desassociar uma descoberta de recursos).
10. (Opcional) Se a conta de administrador da organização secundária quiser parar de participar do IPAM da organização primária, poderá cancelar o compartilhamento da descoberta de recursos compartilhados (consulte Atualizar um compartilhamento de recurso no AWS RAM no Guia do usuário do AWS RAM) ou excluir a descoberta de recursos (consulte Excluir uma descoberta de recursos).

Usar o IPAM com uma única conta

Se escolher não Integrar o IPAM a contas em uma organização da AWS Organizations, você poderá usar o IPAM com uma única conta da AWS.

Quando você cria um IPAM na seção seguinte, um perfil vinculado ao serviço é criado automaticamente para o serviço do IPAM da Amazon VPC no AWS Identity and Access Management (IAM).

Os perfis vinculados ao serviço são um tipo de perfil do IAM que permite que serviços da AWS acessem outros serviços da AWS em seu nome. Eles simplificam o processo de gerenciamento de permissões criando e gerenciando automaticamente as permissões necessárias para que os serviços específicos da AWS executem as ações necessárias, simplificando a configuração e a administração desses serviços.

O IPAM usa a função vinculada ao serviço para monitorar e armazenar os CIDRs associados aos recursos de rede do EC2. Para obter mais informações sobre a função vinculada ao serviço e como o IPAM a utiliza, consulte Funções vinculadas ao serviço do IPAM.

> **Important**
>
> Se usar o IPAM com uma única conta da AWS, você deve garantir que a conta da AWS que você usa para criar o IPAM usa um perfil do IAM com uma política do IAM anexada a ele que permita a ação `iam:CreateServiceLinkedRole`. Ao criar o IPAM, você cria automaticamente a função vinculada ao serviço AWSServiceRoleForIPAM. Para obter mais informações sobre como gerenciar uma política do IAM, consulte Edição de políticas do IAM no Guia do usuário do IAM.

Assim que a única conta da AWS tiver permissão para criar a função vinculada ao serviço do IPAM, acesse Criar um IPAM.

Criar um IPAM

Siga as etapas nesta seção para criar um IPAM. Se você delegou um administrador do IPAM, essas etapas devem ser concluídas pela conta do IPAM.

> **Important**
>
> Ao criar um IPAM, será solicitada a permissão para que o IPAM replique dados de contas de origem em uma conta de delegado do IPAM. Para integrar o IPAM ao AWS Organizations, o IPAM precisa de sua permissão para replicar detalhes de uso de recursos e IP em todas as contas (das contas de membro à conta de membro do IPAM delegada) e em todas as regiões da AWS (de regiões operacionais até a região de origem do seu IPAM). Para usuários do IPAM de conta única, o IPAM precisa de sua permissão para replicar detalhes de uso de recursos e IPs entre as regiões operacionais e a região inicial do seu IPAM.

Ao criar o IPAM, você escolhe as regiões da AWS em que o IPAM terá permissão para gerenciar CIDRs de endereços IP. Essas regiões da AWS são chamadas regiões operacionais. O IPAM descobre e monitora recursos somente nas regiões da AWS que você seleciona como regiões operacionais. O IPAM não armazena dados fora das regiões operacionais selecionadas.

O exemplo de hierarquia a seguir mostra como as regiões da AWS que você atribui ao criar o IPAM afetarão as regiões que estarão disponíveis para grupos criados posteriormente.

- IPAM operando na Região da AWS 1 e na Região da AWS 2
  - Escopo privado
    - Grupo do IPAM de nível superior
      - Grupo do IPAM regional na Região da AWS 2
        - Grupo de desenvolvimento
          - Alocação para uma VPC na Região da AWS 2

É possível criar apenas um IPAM. Para obter mais informações sobre o aumento de cotas relacionadas ao IPAM, consulte Cotas para o IPAM.

AWS Management Console

Para criar um IPAM

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No Console de Gerenciamento da AWS, escolha a Região da AWS em que você deseja criar o IPAM. Crie o IPAM em sua principal região de operações.
3. Na página inicial do serviço, selecione Create IPAM (Criar IPAM).
4. Selecione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir que o IP Address Manager da Amazon VPC replique dados das contas de origem para a conta delegada do IPAM). Se você não selecionar essa opção, não poderá criar um IPAM.
5. Escolha um nível IPAM. Para obter mais informações sobre os recursos disponíveis em cada nível e os custos associados aos níveis, consulte a guia IPAM na página de preços do Amazon VPC.
6. Em Operating regions (Regiões operacionais), selecione as regiões da AWS nas quais esse IPAM pode gerenciar e descobrir recursos. A região da AWS na qual você está criando seu IPAM é selecionada como uma das regiões operacionais por padrão. Por exemplo, se estiver

criando esse IPAM na região da AWS `us-east-1`, mas você deseja criar grupos do IPAM regionais posteriormente que forneçam CIDRs para VPCs em `us-west-2`, selecione `us-west-2` aqui. Se você esquecer uma região operacional, poderá retornar posteriormente e editar suas configurações de IPAM.

> **Note**
>
> Se estiver criando um IPAM no Nível Gratuito, pode escolher várias regiões de operação para o seu IPAM, mas a única funcionalidade disponível em todas as regiões de operação será a Insights de IP público. Não será possível utilizar outras funcionalidades do Nível Gratuito, como BYOIP, em regiões de operação do IPAM. Essas funcionalidades só podem ser utilizadas na Região de origem do IPAM. Para utilizar todos os recursos do IPAM em todas as Regiões de operação, é necessário criar um IPAM no nível avançado.

7. Escolha se você deseja habilitar CIDRs GUA IPv6 privados. Para obter mais informações sobre essa opção, consulte Habilitar o provisionamento de CIDRs de GUA IPv6 privado.
8. Escolha se você deseja ativar o Modo de medição. Para obter mais informações sobre essa opção, consulte Habilitar a distribuição de custos.
9. Escolha Create IPAM (Criar IPAM).

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar, modificar e exibir detalhes relacionados ao seu IPAM:

1. Criar o IPAM: create-ipam
2. Visualizar o IPAM que você criou: describe-ipams
3. Exiba os escopos que são criados automaticamente: describe-ipam-scopes
4. Modificar um IPAM existente: modify-ipam

Quando você tiver concluído essas etapas, o IPAM terá feito o seguinte:

- Criado seu IPAM. Você pode ver o IPAM e as regiões operacionais atualmente selecionadas escolhendo IPAMs no painel de navegação esquerdo do console.
- Criado um escopo privado e um público. Você pode visualizar os escopos escolhendo Scopes (Escopos) no painel de navegação. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.

Planejar o provisionamento de endereços IP

Siga as etapas nesta seção para planejar o provisionamento de endereços IP usando grupos do IPAM. Se você configurou uma conta do IPAM, essas etapas devem ser concluídas por essa conta. O processo de criação de grupos é diferente para os grupos no escopo público e no escopo privado. Esta seção inclui as etapas da criação de um grupo regional no escopo privado. Para obter tutoriais sobre BYOIP e BYOASN, consulte Tutoriais.

> **Important**
>
> Para usar grupos do IPAM em contas da AWS, você deve integrar o IPAM ao AWS Organizations ou alguns recursos podem não funcionar corretamente. Para ter mais informações, consulte Integrar o IPAM a contas em uma organização da AWS Organizations.

Um grupo do IPAM é uma coleção de intervalos de endereços IP contíguos (ou CIDRs). Os grupos permitem que você organize seus endereços IP de acordo com suas necessidades de roteamento e segurança. Você pode criar grupos para regiões da AWS fora da sua região do IPAM. Por exemplo, se você tiver necessidades separadas de roteamento e segurança para aplicações de desenvolvimento e produção, poderá criar um grupo para cada uma.

Na primeira etapa desta seção, você criará um grupo de nível superior. Em seguida, você criará um grupo regional dentro do grupo de nível superior. Dentro do grupo regional, você pode criar grupos adicionais conforme necessário, como grupos de ambiente de produção e desenvolvimento. Por padrão, você pode criar grupos de até 10 de profundidade. Para obter informações sobre cotas do IPAM, consulte Cotas para o IPAM.

> **Note**
>
> Os termos provisionar e alocar são usados em todo este guia do usuário e no console do IPAM. Provisionar é usado quando você adiciona um CIDR a um grupo do IPAM. Alocar é usado quando você associa um CIDR de um grupo do IPAM a um recurso.

O exemplo a seguir mostra a hierarquia da estrutura de grupos que você criará concluindo as etapas nesta seção.

- IPAM operando na Região da AWS 1 e na Região da AWS 2
  - Escopo privado
    - Grupo de nível superior
      - Grupo regional na Região da AWS 1
        - Grupo de desenvolvimento
          - Alocação para uma VPC

Essa estrutura serve como um exemplo de como você pode querer usar o IPAM, mas você pode usar o IPAM para atender às necessidades de sua organização. Para obter mais informações sobre as práticas recomendadas, consulte as Amazon VPC IP Address Manager Best Practices (Práticas recomendadas do Amazon VPC IP Address Manager).

Se você estiver criando um único grupo do IPAM, conclua as etapas em Criar um grupo de IPv4 de nível superior e depois vá para Alocar CIDRs de um grupo do IPAM.

Conteúdo

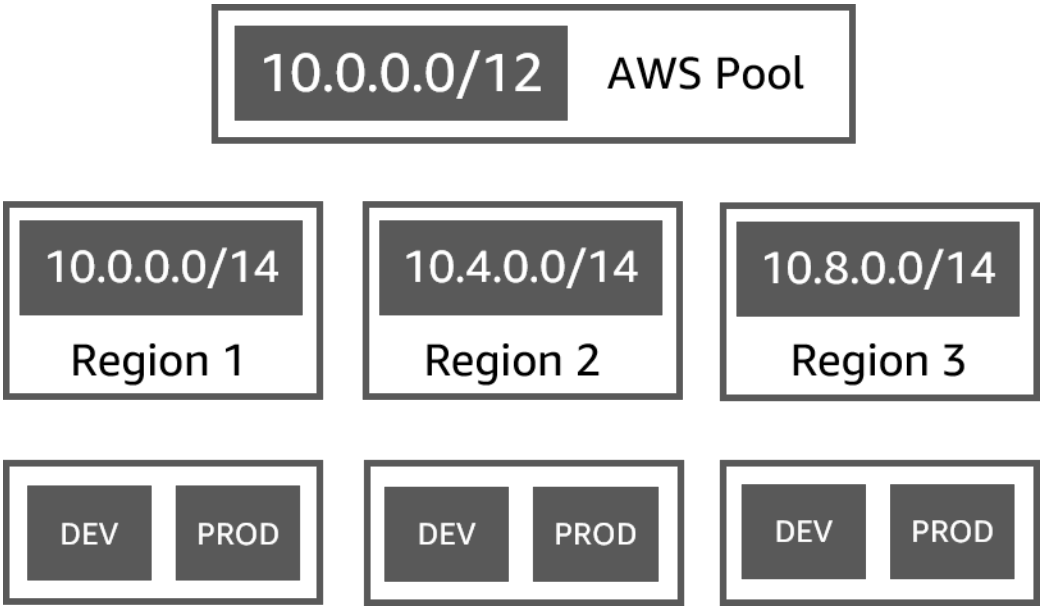
- Exemplo de planos de grupo do IPAM
- Criar grupos de IPv4
- Criar grupos de endereços IPv6 no IPAM

Exemplo de planos de grupo do IPAM

Você pode usar o IPAM para atender às necessidades da sua organização. Esta seção fornece exemplos de como você pode organizar seus endereços IP.

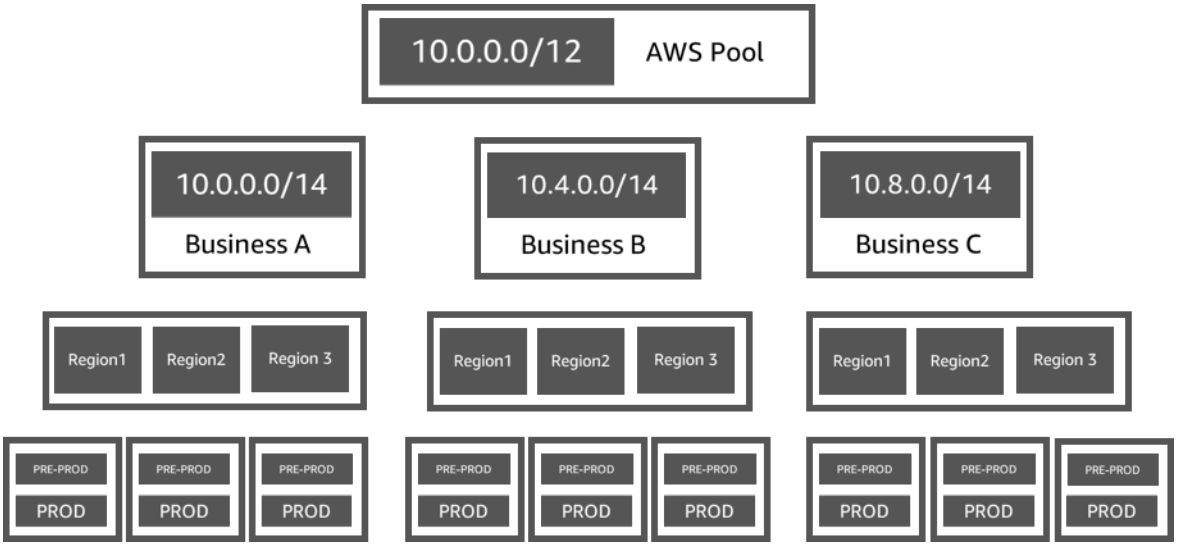
Grupos de IPv4 em várias regiões da AWS

O exemplo a seguir mostra uma hierarquia de grupos do IPAM para várias regiões da AWS em um grupo de nível superior. Cada grupo regional AWS contém dois agrupamentos de desenvolvimento do IPAM, um para recursos de desenvolvimento e outro para recursos de produção.



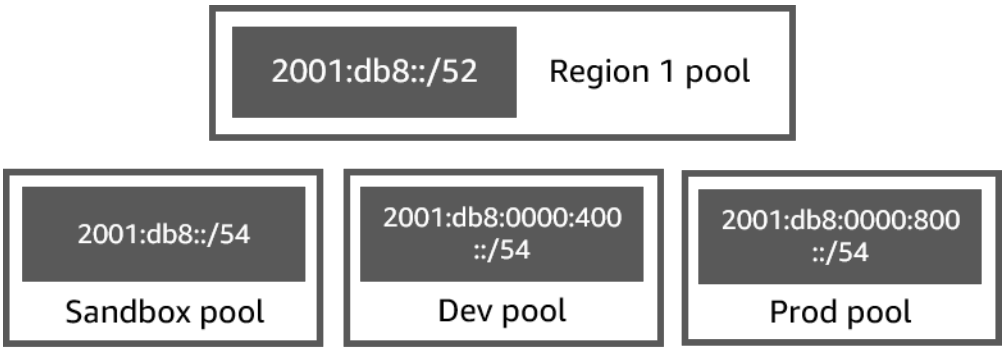
Grupos de IPv4 para várias linhas de negócios

O exemplo a seguir mostra uma hierarquia de grupos do IPAM para várias linhas de negócios em um grupo de nível superior. Cada grupo de cada linha de negócios contém três grupos regionais da AWS. Cada grupo regional da tem dois grupos de desenvolvimento do IPAM dentro dele, um para recursos pré-produção e outro de recursos de produção.



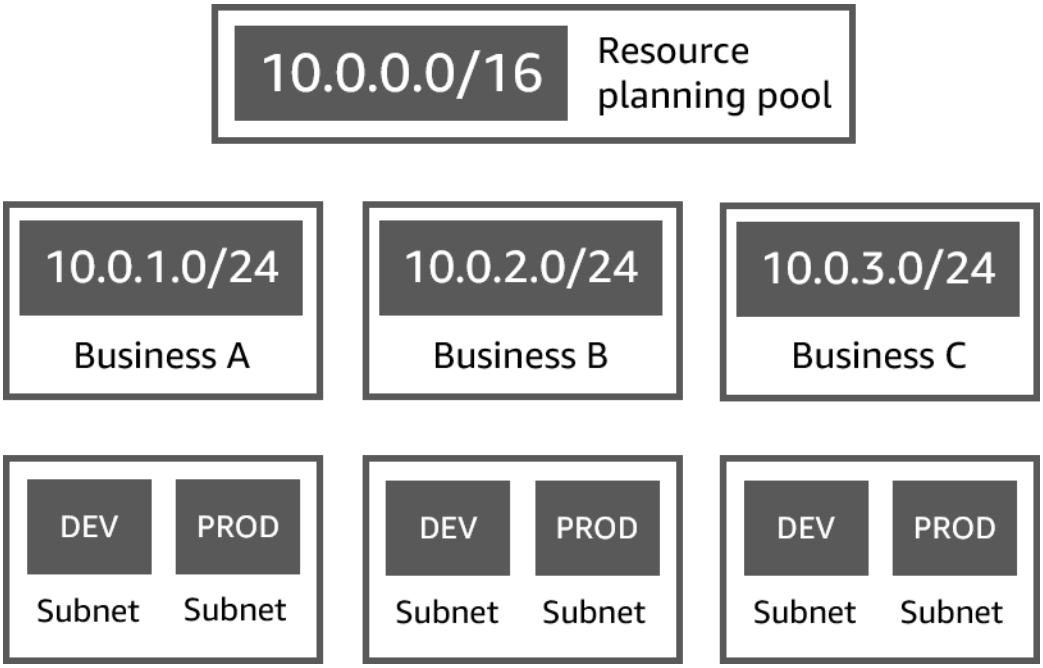
Grupos de IPv6 em uma região da AWS

O exemplo a seguir mostra uma hierarquia de grupos de IPv6 do IPAM para várias linhas de negócios em um grupo regional. Cada grupo regional tem três grupos do IPAM, um grupo para recursos de sandbox, um grupo para recursos de desenvolvimento e outro grupo de recursos de produção.



Grupos de sub-rede para diversas unidades de negócios

O exemplo a seguir ilustra uma estrutura hierárquica de agrupamento de planejamento de recursos para diversas unidades de negócios e grupos de sub-rede de dev/prod. Para obter informações adicionais sobre o planejamento do espaço de endereços de IP da sub-rede utilizando o IPAM, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.



Criar grupos de IPv4

Siga as etapas nesta seção para criar uma hierarquia de grupo de IPv4 do IPAM.

O exemplo a seguir mostra a hierarquia da estrutura do grupo que você pode criar seguindo as instruções contidas neste guia. Nesta seção, você está criando uma hierarquia de grupo de IPv4 do IPAM:

- IPAM operando na Região da AWS 1 e na Região da AWS 2
  - Escopo privado
    - Grupo de nível superior (10.0.0.0/8)
      - Grupo regional na região da AWS 2 (10.0.0.0/16)
        - Grupo de desenvolvimento (10.0.0.0/24)
          - Alocação para uma VPC (10.0.0.0/25)

No exemplo anterior, os CIDRs usados são apenas exemplos. Eles ilustram que cada grupo dentro do grupo de nível superior é provisionado com uma parte do CIDR de nível superior.

Conteúdo

- Criar um grupo de IPv4 de nível superior
- Criar um grupo regional de IPv4
- Criar um grupo de desenvolvimento de IPv4

Criar um grupo de IPv4 de nível superior

Siga as etapas nesta seção para criar um grupo de IPv4 do IPAM de nível superior. Ao criar o grupo, você provisiona um CIDR para esse grupo usar. Em seguida, você atribui esse espaço a uma alocação. Uma alocação é uma atribuição CIDR de um grupo do IPAM para outro grupo do IPAM ou para um recurso.

O exemplo a seguir mostra a hierarquia da estrutura do grupo que você pode criar seguindo as instruções contidas neste guia. Nesta etapa, você está criando o grupo do IPAM de nível superior:

- IPAM operando na Região da AWS 1 e na Região da AWS 2
  - Escopo privado
    - Grupo de nível superior (10.0.0.0/8)

- Grupo regional na região da AWS 1 (10.0.0.0/16)
  - Grupo de desenvolvimento para VPCs não associadas à produção (10.0.0.0/24)
    - Alocação para uma VPC (10.0.0.0/25)

No exemplo anterior, os CIDRs usados são apenas exemplos. Eles ilustram que cada grupo dentro do grupo de nível superior é provisionado com uma parte do CIDR de nível superior.

Ao criar um grupo do IPAM, você pode configurar regras para as alocações feitas dentro do grupo do IPAM.

As regras de alocação permitem configurar o seguinte:

- Se o IPAM deve importar CIDRs automaticamente para o grupo do IPAM se encontrá-los dentro do intervalo de CIDRs desse grupo
- O comprimento da máscara de rede necessário para alocações dentro do grupo
- As etiquetas necessárias para recursos dentro do grupo
- O local necessário para recursos dentro do grupo. O local é a Região da AWS onde um grupo do IPAM está disponível para alocações.

As regras de alocação determinam se os recursos estão em conformidade ou não. Para obter informações adicionais sobre conformidade, consulte Monitorar o uso do CIDR por recurso.

> **Important**
>
> Há uma regra implícita adicional que não é exibida nas regras de alocação. Se o recurso estiver em um grupo do IPAM que seja um recurso compartilhado no AWS Resource Access Manager (RAM), o proprietário do recurso deve ser configurado como entidade principal no AWS RAM. Para obter mais informações sobre compartilhamento de grupos com o RAM, consulte Compartilhar um grupo do IPAM usando o AWS RAM.

O exemplo a seguir mostra como usar regras de alocação para controlar o acesso a um grupo do IPAM:

Example

Quando você cria seus grupos com base nas necessidades de roteamento e segurança, talvez você queira permitir que apenas determinados recursos usem um grupo. Nesses casos, você pode definir uma regra de alocação informando que qualquer recurso que queira um CIDR desse grupo deve ter uma etiqueta que corresponda aos requisitos de etiquetas da regra de alocação. Por exemplo, você pode definir uma regra de alocação informando que somente VPCs com a etiqueta prod podem obter CIDRs de um grupo do IPAM. Também é possível definir uma regra informando que os CIDRs alocados a partir desse grupo não podem ser maiores que /24. Nesse caso, ao criar um recurso com um CIDR maior que /24 usando este grupo, você infringirá uma regra de alocação do grupo e a criação apresentará falhas. Os recursos existentes com um CIDR maior que /24 são sinalizados como não conformes.

Important

Este tópico aborda como criar um grupo de IPv4 de nível superior com um intervalo de endereços IP fornecido pela AWS. Há pré-requisitos se você quiser trazer seu próprio intervalo de endereços IPv4 para a AWS (BYOIP). Para obter mais informações, consulte Tutorial: trazer seus endereços IP para o IPAM.

AWS Management Console

Para criar um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Selecione Criar.
4. Em Escopo do IPAM, escolha o escopo privado que você quer usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.

   Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Os grupos no escopo privado devem ser grupos de IPv4. Os grupos no escopo público podem ser grupos de IPv4 ou IPv6. O escopo público é destinado a todo o espaço público.
5. (Opcional) Adicionar uma Name tag (Etiqueta de nome) e uma descrição para o grupo.
6. Em Tipo de origem, escolha Escopo do IPAM.
7. Em Address family (Família de endereços), escolha IPv4.

8. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
9. Para Locale (Localidade), escolha None (Nenhum). Você definirá a localidade no grupo Regional.

   A localidade é a Região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. Por exemplo, um CIDR pode ser alocado apenas para uma VPC de um grupo do IPAM que compartilhe uma localidade com a Região da VPC. Observe que, ao escolher uma localidade para um grupo, não será possível modificá-la. Se a região de origem do IPAM não estiver disponível devido a uma interrupção e o grupo tiver um local diferente da região de origem do IPAM, o grupo ainda poderá ser usado para alocar endereços IP.
10. (Opcional) Você pode criar um grupo sem um CIDR, mas não poderá usar o grupo para alocações até que tenha provisionado um CIDR para ele. Para provisionar um CIDR, escolha Adicionar novo CIDR. Insira um CIDR IPv4 para provisionar para o grupo. Há pré-requisitos se você quiser trazer seu próprio intervalo de endereços IP IPv4 ou IPv6 para a AWS. Para obter mais informações, consulte Tutorial: trazer seus endereços IP para o IPAM.
11. Escolha regras de alocação opcionais para este grupo:

    - Importar recursos descobertos automaticamente: essa opção não está disponível se Locale (Localidade) estiver definida como None (Nenhum). Se selecionado, o IPAM busca continuamente por recursos no intervalo de CIDRs desse grupo e os importa automaticamente para seu IPAM. Observe o seguinte:
      - Os CIDRs que serão alocados para esses recursos ainda não devem ser alocados para outros recursos para que a importação seja bem-sucedida.
      - O IPAM importará um CIDR, independentemente de sua conformidade com as regras de alocação do grupo, para que um recurso possa ser importado e posteriormente marcado como não compatível.
      - Se o IPAM descobrir vários CIDRs que se sobrepõem, importará apenas o maior deles.
      - Se o IPAM descobrir vários CIDRs com CIDRs correspondentes, importará aleatoriamente apenas um deles.

> **Warning**
>
> - Depois de criar um IPAM, ao criar uma VPC, escolha a opção de bloco CIDR alocado pelo IPAM. Caso contrário, o CIDR escolhido para sua VPC pode se sobrepor a uma alocação de CIDR do IPAM.
> - Se você já tiver uma VPC alocada em um grupo do IPAM, uma VPC com um CIDR sobreposto não poderá ser importada automaticamente. Por exemplo, se você tiver uma VPC com CIDR 10.0.0.0/26 alocada em um grupo do IPAM, uma VPC com CIDR 10.0.0.0/23 (que abrangeria a CIDR 10.0.0.0/26) não poderá ser importada.
> - Demora algum tempo para que as alocações de CIDR de VPCs existentes sejam importadas automaticamente para o IPAM.

- Comprimento mínimo da máscara de rede: o comprimento mínimo da máscara de rede necessário para que as alocações CIDR nesse grupo do IPAM sejam compatíveis e o bloco CIDR de maior tamanho que pode ser alocado a partir do grupo. O comprimento mínimo da máscara de rede deve ser menor que o comprimento máximo da máscara de rede. Os possíveis comprimentos de máscara de rede para endereços IPv4 são de 0 a 32. Os possíveis comprimentos de máscara de rede para endereços IPv6 são de 0 a 128.
- Comprimento padrão da máscara de rede: um comprimento de máscara de rede padrão para alocações adicionadas a esse grupo. Por exemplo, se o CIDR provisionado para esse grupo for **`10.0.0.0/8`** e você inserir **`16`** aqui, todas as novas alocações nesse grupo serão padronizadas para um comprimento de máscara de rede de /16.
- Comprimento máximo da máscara de rede: o comprimento máximo da máscara de rede que será necessário para alocações de CIDR nesse grupo. Esse valor dita o bloco CIDR de menor tamanho que poderá ser alocado a partir do grupo.
- Requisitos de marcação: as tags necessárias para que os recursos aloquem espaço do grupo. Se os recursos tiverem suas tags alteradas depois de terem alocado espaço ou se as regras de marcação de alocação forem alteradas no grupo, o recurso poderá ser marcado como não compatível.
- Localidade: a localidade que será necessária para recursos que usam CIDRs desse grupo. Recursos importados automaticamente que não tiverem essa localidade serão marcados como não compatíveis. Os recursos que não são importados automaticamente para o grupo não terão permissão para alocar espaço do grupo, a menos que estejam nessa localidade.

> **Note**
>
> As regras de alocação se aplicam somente aos recursos gerenciados dentro desse pool. As regras não se aplicam a recursos em pools dentro de um pool.

12. (Opcional) Escolha Tags (Etiquetas) para o grupo.
13. Selecione Criar.
14. Consulte Criar um grupo regional de IPv4.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar ou editar um grupo de nível superior no IPAM:

1. Criar um grupo: create-ipam-pool.
2. Editar o grupo depois de criá-lo para modificar as regras de alocação: modify-ipam-pool.

Criar um grupo regional de IPv4

Siga as etapas desta seção para criar um grupo regional dentro do grupo regional de nível superior. Se você precisar apenas de um grupo de nível superior e não precisar de grupos regionais e de desenvolvimento adicionais, avance para Alocar CIDRs de um grupo do IPAM.

> **Note**
>
> O processo de criação de grupos é diferente para os grupos no escopo público e no escopo privado. Esta seção inclui as etapas da criação de um grupo regional no escopo privado. Para obter tutoriais sobre BYOIP e BYOASN, consulte Tutoriais.

O exemplo a seguir mostra a hierarquia da estrutura do grupo que você cria seguindo as instruções neste guia. Nesta etapa, você está criando o grupo do IPAM regional:

- IPAM operando na Região da AWS 1 e na Região da AWS 2

- Escopo privado
  - Grupo de nível superior (10.0.0.0/8)
    - Grupo regional na região da AWS 1 (10.0.0.0/16)
      - Grupo de desenvolvimento para VPCs não associadas à produção (10.0.0.0/24)
        - Alocação para uma VPC (10.0.0.0/25)

No exemplo anterior, os CIDRs usados são apenas exemplos. Eles ilustram que cada grupo dentro do grupo de nível superior é provisionado com uma parte do CIDR de nível superior.

AWS Management Console

Para criar um grupo regional dentro de um grupo de nível superior

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Selecione Criar.
4. Em Escopo do IPAM, selecione o mesmo escopo usado durante a criação do grupo de nível superior. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
5. (Opcional) Adicionar uma Name tag (Etiqueta de nome) e uma descrição para o grupo.
6. Em Tipo de origem, escolha Grupo do IPAM. Em seguida, escolha o grupo de nível superior que você criou na seção anterior.
7. Caso esteja criando esse grupo no escopo público, você verá uma opção para Família de endereços. Escolha IPv4.
8. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
9. Escolha o local para o grupo. A escolha de uma localidade garante que não haja dependências inter-regionais entre seu grupo e os recursos alocados a partir dele. As opções disponíveis são provenientes das regiões operacionais que você escolheu ao criar seu IPAM.

   A localidade é a Região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. Por exemplo, um CIDR pode ser alocado apenas para uma VPC de um grupo do IPAM que compartilhe uma localidade com a Região da VPC. Observe que, ao escolher uma localidade para um grupo, não será possível modificá-la. Se a região de origem do IPAM não

estiver disponível devido a uma interrupção e o grupo tiver um local diferente da região de origem do IPAM, o grupo ainda poderá ser usado para alocar endereços IP.

> **Note**
>
> Ao criar um grupo no Nível Gratuito, sua escolha de localidade está restrita à região de origem do seu IPAM. Para desfrutar de todos os recursos do IPAM em todas as localidades, é necessário fazer upgrade para o Nível Avançado.

10. Caso esteja criando esse grupo no escopo público, você verá uma opção para Serviço. Escolha EC2 (EIP/VPC). O serviço selecionado determina o serviço da AWS no qual o CIDR poderá ser publicado. Atualmente, a única opção é EC2 (EIP/VPC), o que significa que os CIDRs alocados a partir desse grupo poderão ser anunciados para o serviço Amazon EC2 (para endereços IP elásticos) e para o serviço Amazon VPC (para CIDRs associados a VPCs).
11. (Opcional) Escolha um CIDR para provisionar para o grupo. Você pode criar um grupo sem um CIDR, mas não poderá usar o grupo para alocações até que você tenha provisionado um CIDR para ele. Você pode adicionar CIDRs a um grupo a qualquer momento editando o grupo.
12. Aqui, você tem as mesmas opções de regra de alocação que na criação do grupo de nível superior. Consulte Criar um grupo de IPv4 de nível superior para obter uma explicação das opções que estão disponíveis ao criar grupos. As regras de alocação para o grupo regional não são herdadas do grupo de nível superior. Se você não aplicar nenhuma regra aqui, nenhuma regra de alocação será definida para o grupo.
13. (Opcional) Escolha Tags (Etiquetas) para o grupo.
14. Ao terminar de configurar o grupo, escolha Create pool (Criar grupo).
15. Consulte Criar um grupo de desenvolvimento de IPv4.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar um grupo regional no IPAM:

1. Obter o ID do escopo no qual deseja criar o grupo: describe-ipam-scopes
2. Obter o ID do grupo no qual deseja criar o grupo: describe-ipam-pools

3. Criar o grupo: create-ipam-pool.
4. Visualizar o novo grupo: describe-ipam-pools

Repita essas etapas para criar grupos adicionais dentro do grupo de nível superior, conforme necessário.

Criar um grupo de desenvolvimento de IPv4

Siga as etapas desta seção para criar um grupo de desenvolvimento dentro do grupo regional. Se você precisar apenas de um grupo regional e de nível superior e não precisar de grupos de desenvolvimento, avance para Alocar CIDRs de um grupo do IPAM.

O exemplo a seguir mostra a hierarquia da estrutura do grupo que você pode criar seguindo as instruções contidas neste guia. Nesta etapa, você está criando um grupo do IPAM de desenvolvimento:

- IPAM operando na Região da AWS 1 e na Região da AWS 2
  - Escopo privado
    - Grupo de nível superior (10.0.0.0/8)
      - Grupo regional na região da AWS 1 (10.0.0.0/16)
        - Grupo de desenvolvimento para VPCs não associadas à produção (10.0.0.0/24)
          - Alocação para uma VPC (10.0.1.0/25)

No exemplo anterior, os CIDRs usados são apenas exemplos. Eles ilustram que cada grupo dentro do grupo de nível superior é provisionado com uma parte do CIDR de nível superior.

AWS Management Console

Para criar um grupo de desenvolvimento em um grupo regional

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Selecione Criar.
4. Em Escopo do IPAM, escolha o mesmo escopo usado quando você cria grupos regionais e de nível superior. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.

5. (Opcional) Adicionar uma Name tag (Etiqueta de nome) e uma descrição para o grupo.
6. Em Tipo de origem, escolha Grupo do IPAM. Em seguida, selecione o grupo regional.
7. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
8. (Opcional) Escolha um CIDR para provisionar para o grupo. Você só pode provisionar um CIDR que foi provisionado para o grupo de nível superior. Você pode criar um grupo sem um CIDR, mas não poderá usar o grupo para alocações até que você tenha provisionado um CIDR para ele. Você pode adicionar CIDRs a um grupo a qualquer momento editando o grupo.
9. Aqui, você tem as mesmas opções de regra de alocação que na criação do grupo de nível superior e regional. Consulte Criar um grupo de IPv4 de nível superior para obter uma explicação das opções que estão disponíveis ao criar grupos. As regras de alocação para o grupo não são herdadas do grupo acima dele na hierarquia. Se você não aplicar nenhuma regra aqui, nenhuma regra de alocação será definida para o grupo.
10. (Opcional) Escolha Tags (Etiquetas) para o grupo.
11. Ao terminar de configurar o grupo, escolha Create pool (Criar grupo).
12. Consulte Alocar CIDRs de um grupo do IPAM.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar um grupo regional no IPAM:

1. Obter o ID do escopo no qual deseja criar o grupo: describe-ipam-scopes
2. Obter o ID do grupo no qual deseja criar o grupo: describe-ipam-pools
3. Criar o grupo: create-ipam-pool.
4. Visualizar o novo grupo: describe-ipam-pools

Repita essas etapas para criar grupos de desenvolvimento adicionais dentro do grupo regional, conforme necessário.

Criar grupos de endereços IPv6 no IPAM

A AWS disponibiliza conectividade com o endereço IPv6 em diversos serviços, como o EC2, a VPC e o S3, possibilitando o uso do espaço de endereços ampliado e dos recursos de segurança aprimorados do endereço IPv6. O IPv6 foi projetado para resolver essa limitação fundamental do IPv4. Com a mudança para um espaço de endereços de 128 bits, o endereço IPv6 proporciona um grande número de endereços IP exclusivos. Essa expansão massiva de endereços permite a proliferação contínua de tecnologias conectadas, desde smartphones e dispositivos de IoT até uma infraestrutura em nuvem.

Além disso, você pode usar o IPAM para garantir que está utilizando CIDRs com o endereço IPv6 contíguos para a criação de VPCs. Os CIDRs alocados de forma contígua se tratam de CIDRs que são alocados sequencialmente. Esses CIDRs possibilitam simplificar as regras de segurança e de rede. Além disso, os CIDRs com o endereço IPv6 podem ser agregados em uma única entrada em componentes de rede e de segurança, como listas de controle de acesso, tabelas de rotas, grupos de segurança e firewalls.

Siga as etapas nesta seção para criar uma hierarquia de grupo de IPv6 do IPAM. Ao criar o grupo, você pode provisionar um CIDR para esse grupo usar. O grupo atribui espaço dentro desse CIDR às alocações dentro do grupo. Uma alocação é uma atribuição CIDR de um grupo do IPAM para outro recurso ou grupo do IPAM.

> **Note**
>
> O endereçamento IPv6 tanto público quanto privado está disponível na AWS. A AWS considera endereços IP públicos os que são anunciados na Internet pela AWS, enquanto os endereços IP privados não são e não podem ser anunciados na Internet pela AWS. Se você quiser que suas redes privadas sejam compatíveis com IPv6 e não tiver intenção de rotear o tráfego desses endereços para a Internet, crie um grupo de iPv6 em um escopo privado. Para obter mais informações sobre o endereçamento IPv6, consulte Endereços IPv6 no Manual do usuário da Amazon VPC.

O exemplo a seguir mostra a hierarquia da estrutura do grupo que você pode criar seguindo as instruções contidas neste guia. Nesta seção, você está criando uma hierarquia de grupos de IPv6 do IPAM:

- IPAM operando na Região da AWS 1 e na Região da AWS 2

- Escopo
  - Grupo regional na região 1 da AWS (2001:db8::/52)
    - Grupo de desenvolvimento (2001:db8::/54)
      - Alocação para uma VPC (2001:db8::/56)

No exemplo anterior, os CIDRs usados são apenas exemplos. Eles ilustram que o grupo Desenvolvimento dentro do grupo Regional é provisionado com uma parte do CIDR do grupo Regional.

Conteúdo

- Criar um grupo regional de endereços IPv6 em seu IPAM
- Criar um grupo de desenvolvimento de endereços IPv6 no IPAM

Criar um grupo regional de endereços IPv6 em seu IPAM

Siga as etapas nesta seção para criar um grupo regional de IPv6 do IPAM. Quando você provisiona um bloco CIDR IPv6 fornecido pela Amazon para um grupo, ele deve ser provisionado para um grupo com uma localidade (região da AWS) selecionada. Ao criar o grupo, é possível provisionar um CIDR para o grupo usar ou adicioná-lo posteriormente. Em seguida, você atribui esse espaço a uma alocação. Uma alocação é uma atribuição CIDR de um grupo do IPAM para outro grupo do IPAM ou para um recurso.

O exemplo a seguir mostra a hierarquia da estrutura do grupo que você pode criar seguindo as instruções contidas neste guia. Nesta etapa, você está criando o grupo regional de IPv6 do IPAM regional:

- IPAM operando na Região da AWS 1 e na Região da AWS 2
  - Escopo
    - Grupo regional na região 1 da AWS (2001:db8::/52)
      - Grupo de desenvolvimento (2001:db8::/54)
        - Alocação para uma VPC (2001:db8::/56)

No exemplo anterior, os CIDRs usados são apenas exemplos. Eles ilustram que cada grupo no grupo regional de IPv6 é provisionado com uma parte do CIDR regional de IPv6.

Ao criar um grupo do IPAM, você pode configurar regras para as alocações feitas dentro do grupo do IPAM.

As regras de alocação permitem configurar o seguinte:

- O comprimento da máscara de rede necessário para alocações dentro do grupo
- As etiquetas necessárias para recursos dentro do grupo
- O local necessário para recursos dentro do grupo. O local é a Região da AWS onde um grupo do IPAM está disponível para alocações.

As regras de alocação determinam se os recursos estão em conformidade ou não. Para obter informações adicionais sobre conformidade, consulte Monitorar o uso do CIDR por recurso.

> **Note**
>
> Há uma regra implícita adicional que não é exibida nas regras de alocação. Se o recurso estiver em um grupo do IPAM que seja um recurso compartilhado no AWS Resource Access Manager (RAM), o proprietário do recurso deve ser configurado como entidade principal no AWS RAM. Para obter mais informações sobre compartilhamento de grupos com o RAM, consulte Compartilhar um grupo do IPAM usando o AWS RAM.

O exemplo a seguir mostra como usar regras de alocação para controlar o acesso a um grupo do IPAM:

Example

Quando você cria seus grupos com base nas necessidades de roteamento e segurança, talvez você queira permitir que apenas determinados recursos usem um grupo. Nesses casos, você pode definir uma regra de alocação informando que qualquer recurso que queira um CIDR desse grupo deve ter uma etiqueta que corresponda aos requisitos de etiquetas da regra de alocação. Por exemplo, você pode definir uma regra de alocação informando que somente VPCs com a etiqueta prod podem obter CIDRs de um grupo do IPAM.

> **Note**
>
> - Este tópico trata de como criar um grupo de IPv6 regional com um intervalo de endereços IPv6 fornecido pela AWS ou um intervalo de endereços IPv6 privados. Se você quiser

trazer seus próprios intervalos de endereços IP IPv4 ou IPv6 para a AWS (BYOIP), haverá pré-requisitos. Para obter mais informações, consulte Tutorial: trazer seus endereços IP para o IPAM.

- Se você estiver criando um grupo de IPv6 em um escopo privado, poderá usar um intervalo de GUAs ou ULAs IPv6 privados. Para usar um intervalo de GUAs privados, você precisa primeiro habilitar a opção no IPAM (consulte Habilitar o provisionamento de CIDRs de GUA IPv6 privado).

AWS Management Console

Para criar um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Selecione Criar.
4. Em Escopo do IPAM, escolha um escopo privado ou público. Se você quiser que suas redes privadas sejam compatíveis com IPv6 e não tiver intenção de rotear o tráfego desses endereços para a Internet, escolha um escopo privado. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.

   Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado.
5. (Opcional) Adicionar uma Name tag (Etiqueta de nome) e uma descrição para o grupo.
6. Em Tipo de origem, escolha Escopo do IPAM.
7. Em Família de endereços, selecione IPv6. Se você estiver criando esse grupo no escopo público, todos os CIDRs desse grupo poderão ser anunciados publicamente.
8. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
9. Escolha o Local do grupo. Se você quiser provisionar um bloco CIDR IPv6 fornecido pela Amazon para um grupo, ele deverá ser provisionado para um grupo com uma localidade (região da AWS) selecionada. A escolha de uma localidade garante que não haja dependências inter-regionais entre seu grupo e os recursos alocados a partir dele. As opções disponíveis são provenientes das regiões operacionais que você escolheu para o IPAM ao criá-lo. Você pode acrescentar regiões operacionais adicionais a qualquer momento.

A localidade é a Região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. Por exemplo, um CIDR pode ser alocado apenas para uma VPC de um grupo do IPAM que compartilhe uma localidade com a Região da VPC. Observe que, ao escolher uma localidade para um grupo, não será possível modificá-la. Se a região de origem do IPAM não estiver disponível devido a uma interrupção e o grupo tiver um local diferente da região de origem do IPAM, o grupo ainda poderá ser usado para alocar endereços IP.

> **Note**
>
> Ao criar um grupo no Nível Gratuito, sua escolha de localidade está restrita à região de origem do seu IPAM. Para desfrutar de todos os recursos do IPAM em todas as localidades, é necessário fazer upgrade para o Nível Avançado.

10. (Opcional) Se você estiver criando um grupo de IPv6 no escopo público, em Serviço, escolha EC2 (EIP/VPC). O serviço selecionado determina o serviço da AWS no qual o CIDR poderá ser publicado. Atualmente, a única opção é EC2 (EIP/VPC), o que significa que os CIDRs alocados a partir desse grupo poderão ser anunciados para o serviço Amazon EC2 (para endereços IP elásticos) e para o serviço Amazon VPC (para CIDRs associados a VPCs).
11. (Opcional) Se você estiver criando um grupo de IPv6 no escopo público, na opção Origem do IP público, escolha Pertencente à Amazon para AWS fornecer um intervalo de endereços IPv6 para esse grupo. Conforme destacado na parte superior desta página, este tópico aborda como criar um grupo regional de IPv6 com um intervalo de endereços IP fornecido pela AWS. Há pré-requisitos se você quiser trazer seu próprio intervalo de endereços IPv4 ou IPv6 para a AWS (BYOIP). Para obter mais informações, consulte Tutorial: trazer seus endereços IP para o IPAM.
12. (Opcional) É possível criar um grupo sem um CIDR, mas não poderá usar o grupo para alocações até que tenha provisionado um CIDR para ele. Para provisionar um CIDR, use um dos seguintes procedimentos:

    - Se você estiver criando um grupo de IPv6 no escopo público com Origem de IP público pertencente à Amazon, para provisionar um CIDR, em CIDRs para provisionar, escolha Adicionar CIDR pertencente à Amazon e escolha o tamanho da máscara de rede entre /40 e /52 para o CIDR. Ao escolher um comprimento de máscara de rede no menu suspenso, você vê o comprimento da máscara de rede, bem como o número de /56 CIDRs que a máscara de rede representa. Por padrão, é possível adicionar um bloco CIDR IPv6

fornecido pela Amazon com um grupo regional. Para obter informações sobre como aumentar o limite padrão, consulte Cotas para o IPAM.

- Se você estiver criando um grupo de IPv6 em um escopo privado, poderá usar um intervalo de GUAs ou ULAs IPv6 privados:
  - Para obter detalhes importantes sobre IPv6 privado, consulte Endereços IPv6 privados no Manual do usuário da Amazon VPC.
  - Para usar um intervalo de ULAs IPv6 privados, em CIDRs para provisionar, escolha Adicionar CIDR de ULA por máscara de rede e escolha um tamanho de máscara de rede ou escolha Inserir CIDRs IPv6 privado e insira um intervalo de ULAs. Um espaço de ULAs IPv6 válido é todo espaço abaixo de fd00::/8 que não coincide com o intervalo reservado fd00: :/16 da Amazon.
  - Para usar um intervalo de GUAs IPv6 privados, você precisa primeiro habilitar a opção no IPAM (consulte Habilitar o provisionamento de CIDRs de GUA IPv6 privado). Depois de habilitar os CIDRs de GUA IPv6 privado, insira um GUA IPv6 em Inserir CIDR IPv6 privado.

13. Escolha regras de alocação opcionais para este grupo:

- Comprimento mínimo da máscara de rede: o comprimento mínimo da máscara de rede necessário para que as alocações CIDR nesse grupo do IPAM sejam compatíveis e o bloco CIDR de maior tamanho que pode ser alocado a partir do grupo. O comprimento mínimo da máscara de rede deve ser menor que o comprimento máximo da máscara de rede. Os possíveis comprimentos de máscara de rede para endereços IPv6 são de 0 a 128.
- Comprimento padrão da máscara de rede: um comprimento de máscara de rede padrão para alocações adicionadas a esse grupo. Por exemplo, se o CIDR provisionado para esse grupo for `2001:db8::/52` e você inserir 56 aqui, todas as novas alocações nesse grupo serão padronizadas para um comprimento de máscara de rede de /56.
- Comprimento máximo da máscara de rede: o comprimento máximo da máscara de rede que será necessário para alocações de CIDR nesse grupo. Esse valor dita o bloco CIDR de menor tamanho que poderá ser alocado a partir do grupo. Por exemplo, se você inserir /56 aqui, o menor comprimento de máscara de rede que pode ser alocado para CIDRs desse grupo é /56.
- Requisitos de marcação: as tags necessárias para que os recursos aloquem espaço do grupo. Se os recursos tiverem suas tags alteradas depois de terem alocado espaço ou

se as regras de marcação de alocação forem alteradas no grupo, o recurso poderá ser marcado como não compatível.

- Localidade: a localidade que será necessária para recursos que usam CIDRs desse grupo. Recursos importados automaticamente que não tiverem essa localidade serão marcados como não compatíveis. Os recursos que não são importados automaticamente para o grupo não terão permissão para alocar espaço do grupo, a menos que estejam nessa localidade.

14. (Opcional) Escolha Tags (Etiquetas) para o grupo.
15. Selecione Criar.
16. Consulte Criar um grupo de desenvolvimento de endereços IPv6 no IPAM.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar ou editar um grupo regional de IPv6 no IPAM:

1. Se você quiser habilitar o provisionamento de CIDRs de GUA IPv6 privado, modifique o IPAM com modify-ipam e inclua a opção `enable-private-gua`. Para obter mais informações, consulte Habilitar o provisionamento de CIDRs de GUA IPv6 privado.
2. Criar um grupo com create-ipam-pool.
3. Provisionar um CIDR para o grupo: provision-ipam-pool-cidr.
4. Editar o grupo depois de criá-lo para modificar as regras de alocação: modify-ipam-pool.

Criar um grupo de desenvolvimento de endereços IPv6 no IPAM

Siga as etapas desta seção para criar um grupo de desenvolvimento dentro do grupo regional de IPv6. Se precisar apenas de um grupo regional e não precisar de grupos de desenvolvimento, avance para Alocar CIDRs de um grupo do IPAM.

O exemplo a seguir mostra a hierarquia da estrutura do grupo que você pode criar seguindo as instruções contidas neste guia. Nesta etapa, você está criando um grupo do IPAM de desenvolvimento:

- IPAM operando na Região da AWS 1 e na Região da AWS 2
  - Escopo

- Grupo regional na região 1 da AWS (2001:db8::/52)
  - Grupo de desenvolvimento (2001:db8::/54)
    - Alocação para uma VPC (2001:db8::/56)

No exemplo anterior, os CIDRs usados são apenas exemplos. Eles ilustram que cada grupo dentro do grupo de nível superior é provisionado com uma parte do CIDR de nível superior.

AWS Management Console

Para criar um grupo de desenvolvimento em um grupo regional de IPv6

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Selecione Criar.
4. Em Escopo do IPAM, escolha um escopo. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
5. (Opcional) Adicionar uma Name tag (Etiqueta de nome) e uma descrição para o grupo.
6. Em Tipo de origem, escolha Grupo do IPAM. Em seguida, em Grupo de origem, escolha o grupo regional de IPv6.
7. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
8. (Opcional) Escolha um CIDR para provisionar para o grupo. Você só pode provisionar um CIDR que foi provisionado para o grupo de nível superior. Você pode criar um grupo sem um CIDR, mas não poderá usar o grupo para alocações até que você tenha provisionado um CIDR para ele. Você pode adicionar CIDRs a um grupo a qualquer momento editando o grupo.
9. Aqui, você tem as mesmas opções de regra de alocação que na criação do grupo regional de IPv6. Consulte Criar um grupo regional de endereços IPv6 em seu IPAM para obter uma explicação das opções que estão disponíveis ao criar grupos. As regras de alocação para o grupo não são herdadas do grupo acima dele na hierarquia. Se você não aplicar nenhuma regra aqui, nenhuma regra de alocação será definida para o grupo.
10. (Opcional) Escolha Tags (Etiquetas) para o grupo.
11. Ao terminar de configurar o grupo, escolha Create pool (Criar grupo).

12. Consulte Alocar CIDRs de um grupo do IPAM.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar um grupo regional de IPv6 no IPAM:

1. Obter o ID do escopo no qual deseja criar o grupo: describe-ipam-scopes
2. Obter o ID do grupo no qual deseja criar o grupo: describe-ipam-pools
3. Criar o grupo: create-ipam-pool.
4. Visualizar o novo grupo: describe-ipam-pools

Repita essas etapas para criar grupos de desenvolvimento adicionais dentro do grupo regional de IPv6, conforme necessário.

Alocar CIDRs de um grupo do IPAM

Um recurso importante do IPAM é a capacidade de alocar e gerenciar espaço de endereços IP. Ao criar uma VPC, você deve especificar um bloco CIDR de endereços IP, que define o intervalo de endereços IP disponíveis para essa VPC. O IPAM simplifica esse processo fornecendo uma visão global de todo o seu inventário de endereços IP, ajudando você a atribuir e reutilizar estrategicamente prefixos IP em várias VPCs.

Essa alocação de espaço de endereços é crucial para garantir que não haja intervalos de IP sobrepostos, o que pode causar conflitos de roteamento e problemas de conectividade. O IPAM também permite que você reserve espaço de endereços IP para futura expansão da VPC, evitando a necessidade de uma renumeração complexa posteriormente.

Siga as etapas nesta seção para alocar um CIDR de um grupo do IPAM para um recurso.

> **Note**
>
> Os termos provisionar e alocar são usados em todo este guia do usuário e no console do IPAM. Provisionar é usado quando você adiciona um CIDR a um grupo do IPAM. Alocar é usado quando você associa um CIDR de um grupo do IPAM a um recurso.

Você pode alocar CIDRs de um grupo do IPAM das seguintes formas:

- Usar um serviço da AWS integrado ao IPAM, como a Amazon VPC, e selecionar a opção para usar um grupo do IPAM para o CIDR. O IPAM cria automaticamente a alocação no grupo para você.
- Aloque um CIDR manualmente em um grupo do IPAM para reservá-lo para uso posterior com um serviço da AWS que esteja integrado ao IPAM, como a Amazon VPC.

Esta seção mostra as duas opções: como usar os serviços da AWS integrados ao IPAM para provisionar o CIDR de um grupo do IPAM e como reservar manualmente o espaço de endereços IP.

Conteúdo

- Ciar uma VPC que usa um CIDR de um grupo do IPAM
- Alocar manualmente um CIDR a um grupo para reservar o espaço de endereços IP

Ciar uma VPC que usa um CIDR de um grupo do IPAM

Com a Amazon Virtual Private Cloud (Amazon VPC), é possível iniciar recursos da AWS em uma rede virtual logicamente isolada que você mesmo define. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu data center, com os benefícios de usar a infraestrutura escalável da AWS.

Uma nuvem privada virtual (VPC) é uma rede virtual dedicada à sua conta da AWS. Ela é isolada de maneira lógica de outras redes virtuais na Nuvem da AWS. Você pode especificar um intervalo de endereços IP para a VPC, adicionar sub-redes, adicionar gateways e associar grupos de segurança.

Siga as etapas descritas em Crie uma VPC no Guia do usuário da Amazon VPC. Ao chegar à etapa de escolher um CIDR para a VPC, você terá a opção de usar um CIDR de um grupo do IPAM.

Se você escolher a opção de usar um grupo do IPAM ao criar a VPC, a AWS aloca um CIDR no grupo do IPAM. Você pode visualizar a alocação no IPAM escolhendo um grupo no painel de conteúdo do console do IPAM e exibindo a guia “Resources” (Recursos) do grupo.

> **Note**
>
> Para obter instruções completas usando a AWS CLI, incluindo a criação de uma VPC, consulte a seção Tutoriais para o IP Address Manager da Amazon VPC.

Alocar manualmente um CIDR a um grupo para reservar o espaço de endereços IP

Siga as etapas nesta seção para alocar manualmente um CIDR a um grupo. Você pode fazer isso para reservar um CIDR dentro de um grupo do IPAM para uso posterior. Você também pode reservar espaço em seu grupo do IPAM para representar uma rede on-premises. O IPAM gerenciará essa reserva para você e indicará se algum CIDR se sobrepõe ao seu espaço IP on-premises.

AWS Management Console

Para alocar manualmente um CIDR

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, o escopo privado padrão é selecionado. Se você não quiser usar o escopo privado padrão, no menu suspenso na parte superior do painel de conteúdo, escolha o escopo que deseja usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. No painel de conteúdo, escolha um grupo.
5. Escolha Actions (Ações) > Create custom allocation (Criar alocação personalizada).
6. Escolha se deseja adicionar um CIDR específico para alocar (p. ex., `10.0.0.0/24` para IPv4 ou `2001:db8::/52` para IPv6) ou adicionar um CIDR por tamanho escolhendo somente o comprimento da máscara de rede (p. ex., `/24` para IPv4 ou `/52` para IPv6).
7. Escolha Allocate.
8. Você pode visualizar a alocação no IPAM escolhendo Pools (Grupos) no painel de navegação, escolhendo um grupo e visualizando a guia Allocations (Alocações) do grupo.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para alocar manualmente um CIDR para um grupo:

1. Obter o ID do grupo do IPAM no qual deseja criar o a alocação: describe-ipam-pools
2. Criar a alocação: allocate-ipam-pool-cidr.

3. Visualizar a alocação: get-ipam-pool-allocations.

Para liberar um CIDR alocado manualmente, consulte Liberar uma alocação.

Gerenciar o espaço de endereços IP no IPAM

As tarefas nesta seção são opcionais. Observe que esta seção é um conjunto de procedimentos, todos relacionados ao trabalho com o IPAM. Os procedimentos são ordenados em ordem alfabética.

Se você quiser concluir as tarefas nesta seção e delegou uma conta do IPAM, as tarefas devem ser concluídas pelo administrador do IPAM.

Siga as etapas desta seção para gerenciar seu espaço de endereços IP no IPAM.

Conteúdo

- Automatizar atualizações da lista de prefixos com o IPAM
- Alterar o estado de monitoramento dos CIDRs da VPC
- Criar escopos adicionais
- Excluir um IPAM
- Excluir um grupo
- Excluir um escopo
- Desprovisionar CIDRs de um grupo
- Editar um grupo do IPAM
- Habilitar a distribuição de custos
- Integrar o VPC IPAM à infraestrutura da Infoblox
- Habilitar o provisionamento de CIDRs de GUA IPv6 privado
- Impor o uso do IPAM para a criação de VPCs com SCPs
- Excluir unidades organizacionais do IPAM
- Criar um nível de IPAM
- Modificar regiões operacionais do IPAM
- Provisionar CIDRs para um grupo
- Mover CIDRs da VPC entre escopos
- Definir a estratégia de alocação de IPv4 público com as políticas do IPAM
- Liberar uma alocação
- Compartilhar um grupo do IPAM usando o AWS RAM

- Trabalhar com descobertas de recursos

Automatizar atualizações da lista de prefixos com o IPAM

Uma lista de prefixos gerenciada é um conjunto de blocos CIDR que você pode referenciar nas regras do grupo de segurança e nas tabelas de roteamento, em vez de especificar endereços IP individuais. Por exemplo, em vez de criar regras de grupo de segurança separadas para `10.1.0.0/16`, `10.2.0.0/16` e `10.3.0.0/16`, você pode criar uma lista de prefixos contendo todos os três CIDRs e referenciá-la em uma única regra.

Existem dois tipos:

- Listas de prefixos gerenciadas pelo cliente: intervalos de IP que você define e gerencia
- Listas de prefixos gerenciadas pela AWS: intervalos de IP para serviços da AWS (como S3 ou CloudFront)

Esse recurso do IPAM automatiza o gerenciamento de listas de prefixos gerenciadas pelo cliente, mantendo suas entradas CIDR sincronizadas com as alterações na sua rede.

O problema que isso resolve

Sem automação, as equipes de rede gastam muito tempo atualizando manualmente as listas de prefixos quando a infraestrutura muda e mantendo listas de prefixos consistentes em todos os ambientes e regiões.

O IPAM resolve esse problema ao permitir que você crie regras que preenchem automaticamente listas de prefixos. Você pode usar duas abordagens: referenciar CIDRs de seus pools IPAM ou criar regras com base em seus recursos reais da AWS, como “incluir todas as VPCs com a etiqueta env=prod”, “incluir todas as sub-redes em us-east-1” ou “incluir todos os endereços IP elásticos pertencentes à conta 123456789”. Quando você adiciona ou remove esses recursos, o IPAM atualiza automaticamente a lista de prefixos com seus respectivos CIDRs.

Como funciona

Você cria regras que informam ao IPAM quais endereços IP devem ser incluídos em uma lista de prefixos. Por exemplo, “incluir todos os CIDRs de VPC com a etiqueta env=prod” Quando você adiciona ou remove VPCs de produção, o IPAM atualiza automaticamente a lista de prefixos.

Quando usar

- Grupos de segurança: crie uma regra “incluir todas as VPCs com a etiqueta env=prod” para que, quando você adicionar novas VPCs de produção, elas sejam automaticamente permitidas nas regras do seu grupo de segurança.
- Várias regiões: implante as mesmas regras de IPAM em várias regiões para manter listas de prefixos idênticas sem copiar manualmente as entradas CIDR.
- Infraestrutura dinâmica: quando você cria/exclui VPCs ou sub-redes, seus CIDRs são automaticamente adicionados/removidos das listas de prefixos sem atualizações manuais.

Pré-requisitos

Antes de começar, verifique se você tem:

- Um IPAM com Nível avançado habilitado
- Uma lista de prefixos gerenciados pelo cliente (ou crie uma durante a configuração)
- Permissões do IAM para operações de IPAM e lista de prefixos do EC2

Etapas de configuração

Etapa 1: Criar um resolvedor de lista de prefixos do IPAM

Defina quais CIDRs incluir na sua lista de prefixos, criando um resolvedor de lista de prefixos do IPAM.

AWS Management Console

Para criar um resolvedor de lista de prefixos do IPAM

1. Abra o console do IPAM.
2. No painel de navegação, selecione Resolvedores de lista de prefixos.
3. Selecione Criar resolvedor de lista de prefixos.
4. Na Etapa 1: Configurar detalhes do resolvedor, escolha o seguinte:
   - IPAM: uma instância do IPAM
   - Família de endereços: IPv4 ou IPv6

- Etiqueta de nome - opcional: um nome descritivo
- Descrição - opcional: uma descrição
- Etiquetas: etiquetas de recursos

5. Escolha Próximo.
6. Na Etapa 2: Configurar regras, escolha Adicionar regra. É possível adicionar até 99 regras.

> **Important**
>
> É possível criar um resolvedor de lista de prefixos sem nenhuma regra de seleção de CIDR, mas ele gerará versões vazias (sem CIDRs) até que você adicione regras.

7. Escolha um dos tipos de regras:

- CIDR estático: uma lista fixa de CIDRs que não mudam (como uma lista manual replicada entre regiões)
- CIDR do pool IPAM: CIDRs de pools IPAM específicos (como todos os CIDRs do seu pool de produção IPAM)

  Se escolher esta opção, selecione o seguinte:

  - Escopo do IPAM: selecione o escopo do IPAM para pesquisar recursos
  - Condições:
    - Propriedade
      - ID do pool IPAM: selecione um pool IPAM que contenha os recursos
      - CIDR (como 10.24.34.0/23)
    - Operação: Igual/Não é igual
    - Valor: o valor no qual corresponder à condição
- CIDR de recurso de escopo: CIDRs de recursos da AWS como VPCs, sub-redes e EIPs dentro de um escopo IPAM

  Se escolher esta opção, selecione o seguinte:

  - Escopo do IPAM: selecione o escopo do IPAM para pesquisar recursos
  - Tipo de recurso: selecione um recurso, como uma VPC ou uma sub-rede.
  - Condições:
    - Propriedade:

        - ID do recurso: o ID exclusivo de um recurso (como vpc-1234567890abcdef0)
        - Proprietário do recurso (como 111122223333)
        - Região do recurso (como us-east-1)
        - Tag de recurso (como chave: nome, valor: dev-vpc-1)
        - CIDR (como 10.24.34.0/23)
      - Operação: Igual/Não é igual
      - Valor: o valor no qual corresponder à condição
8. Escolha Próximo.
9. Escolha Validar e criar.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar um resolvedor de lista de prefixos do IPAM:

- Use o comando create-ipam-prefix-list-resolver e salve o ID do resolvedor retornado na etapa 2.

Etapa 2: Criar um destino de resolução para se conectar a uma lista de prefixos

Vincule seu resolvedor a uma lista de prefixos existente criando um destino de resolvedor. Use o ID do resolvedor retornado na Etapa 1.

AWS Management Console

Para criar um destino de resolução de lista de prefixos do IPAM

1. No console do IPAM, escolha Resolvedores de listas de prefixos.
2. Selecione o resolvedor criado na Etapa 1.
3. Na página de detalhes do resolvedor, selecione a guia Destinos.
4. Escolha Criar destino.
5. Configure o destino:

- Região: selecione a região em que a lista de prefixos gerenciados existe ou na qual você criará uma.
- Lista de prefixos: escolha uma lista de prefixos gerenciados existente ou crie uma nova

6. Em Versão desejada, selecione uma destas opções:

   - Sempre acompanhar a versão mais recente: escolha essa opção para atualizações automáticas quando quiser que as suas listas de prefixos permaneçam atualizadas com as alterações na infraestrutura sem intervenção manual.
   - Rastrear uma versão específica: escolha essa opção para obter estabilidade quando precisar de atualizações previsíveis e controladas e quiser aprovar manualmente as alterações nas suas listas de prefixos.

7. Escolha Criar destino.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar um destino de resolvedor de lista de prefixos do IPAM:

- Use o comando create-ipam-prefix-list-resolver-target com o ID do resolvedor da etapa 1 e seu ID da lista de prefixos existente.

O IPAM agora atualiza automaticamente sua lista de prefixos com base nas suas regras. A lista de prefixos será preenchida com CIDRs que corresponderem aos seus critérios.

Etapa 3: Monitorar versões e a sincronização

Como resultado da criação de um resolvedor de lista de prefixos e um destino, o resolvedor de lista de prefixos gera versões de CIDRs com base nas suas regras e, em seguida, o destino sincroniza esses CIDRs do resolvedor com uma lista de prefixos gerenciada específica. Cada versão é um snapshot do que os CIDRs corresponderam às suas regras naquele momento específico. O número da versão aumenta sempre que a lista de CIDRs é alterada devido a mudanças na infraestrutura.

Exemplo de versão:

Estado inicial (versão 1)

Ambiente de produção:

- vpc-prod-web (10.1.0.0/16) - com a etiqueta env=prod
- vpc-prod-db (10.2.0.0/16) - com a etiqueta env=prod

Regra de resolução: incluir todas as VPCs com a etiqueta env=prod

CIDRs da versão 1: 10.1.0.0/16, 10.2.0.0/16

Alteração na infraestrutura (Versão 2)

Nova VPC adicionada:

- vpc-prod-api (10.3.0.0/16) - com a etiqueta env=prod

O IPAM detecta automaticamente a alteração e cria uma nova versão.

CIDRs da versão 2: 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16

Esta seção explica como monitorar a criação de versões com o console da AWS ou a AWS CLI e o sucesso da sincronização com a AWS CLI.

Além disso, recomendamos que você defina alarmes do CloudWatch para métricas de falha, pois talvez seja necessário reavaliar e ajustar as regras de seleção de CIDR para permanecer dentro dos limites de versão e tamanho da lista de prefixos. Para obter uma lista das métricas do CloudWatch relacionadas às listas de prefixos do IPAM, consulte Métricas do resolvedor da lista de prefixos do IPAM.

AWS Management Console

Para visualizar as versões criadas e monitorar a sincronização de destino

1. No console do IPAM, escolha Resolvedores de listas de prefixos.
2. Selecione o resolvedor criado na Etapa 1.
3. Na página de detalhes do resolvedor, selecione a guia Versões. Aqui você verá todas as versões que foram criadas pelo resolvedor, juntamente com todos os CIDRs na versão.
4. Na página de detalhes do resolvedor, selecione a guia Monitoramento. Nesta visualização, Métricas do resolvedor da lista de prefixos do IPAM são apresentados em forma de gráfico:

- Criação com êxito da versão do resolvedor de lista de prefixos
- Falha na criação da versão do resolvedor de lista de prefixos

5. Na guia Monitoramento, também é possível configurar um alarme CloudWatch selecionando Criar alarme para a criação da versão do resolvedor da lista de prefixos. Você será direcionado para o console do CloudWatch com o alarme parcialmente configurado para a métrica. Para obter mais informações sobre como concluir a criação do alarme, consulte Criar um alarme CloudWatch com base em um limite estático no Guia do usuário do Amazon CloudWatch.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os comandos da AWS CLI a seguir para monitorar as versões e a sincronização:

1. Use o comando get-ipam-prefix-list-resolver-version-entries para ver a versão mais recente criada pelo resolvedor.
2. Use o comando describe-ipam-prefix-list-resolver-targets para monitorar o status de sincronização do destino do resolvedor.

O comando monitor mostra:

- state - estado atual da sincronização (create-complete, modify-complete, entre outros)
- lastSyncedVersion - última versão sincronizada com êxito
- desiredVersion - versão de destino para sincronizar
- stateMessage - detalhes do erro se a sincronização falhar

> **Important**
>
> Para oferecer suporte aos fluxos de trabalho de reversão, o IPAM reterá cópias das 10 versões anteriores do resolvedor da lista de prefixos para cada um de seus destinos; além disso, o IPAM excluirá as versões anteriores a esse limite se elas permanecerem sem referência por mais 7 dias.

Etapa 4: (Opcional) Habilitar e desabilitar a sincronização da lista de prefixos do IPAM

Se uma lista de prefixos gerenciada tiver sido configurada como um destino da lista de prefixos do IPAM e você quiser fazer alterações na lista de prefixos sem precisar de permissão para acessar o destino do resolvedor da lista de prefixos do IPAM, é possível modificar a lista de prefixos gerenciada e desativar a sincronização com o resolvedor da lista de prefixos do IPAM. Quando desabilitada, a lista de prefixos de CIDRs não é atualizada automaticamente e você pode fazer alterações nela. Quando habilitada, a lista de prefixos CIDRs é atualizada automaticamente com base nas regras de seleção CIDR do resolvedor associado.

Alterar o estado de monitoramento dos CIDRs da VPC

Siga as etapas nesta seção para alterar o estado de monitoramento do CIDR de uma VPC. Altere o CIDR de uma VPC de monitorado para ignorado se não quiser que o IPAM gerencie ou monitore a VPC e permita que o CIDR alocado a ela esteja disponível para uso. Se quiser que o IPAM gerencie e monitore o CIDR da VPC, altere o CIDR da VPC de ignorado para monitorado.

> **Note**
>
> - Você não pode ignorar CIDRs da VPC no escopo público.
> - Se um CIDR for ignorado, você ainda será cobrado pelos endereços IP ativos no CIDR. Para obter mais informações, consulte Preços do IPAM.
> - Se um CIDR for ignorado, você ainda poderá visualizar o histórico dos endereços IP no CIDR. Para obter mais informações, consulte Ver histórico de endereços IP.

Você pode alterar o estado de monitoramento do CIDR de um CIDR da VPC para monitorado ou ignorado:

- Monitored (Monitorado): o CIDR da VPC foi detectado pelo IPAM e está sendo monitorado quanto à sobreposição com outros CIDRs e conformidade com regras de alocação.
- Ignored (Ignorado): o CIDR da VPC foi escolhido para ficar isento do monitoramento. Os CIDRs da VPC ignorados não são avaliados quanto à sobreposição com outros CIDRs ou conformidade com as regras de alocação. Depois que um CIDR da VPC for escolhido para ser ignorado, qualquer espaço alocado a ele de um grupo do IPAM retornará ao grupo e o CIDR da VPC não será importado novamente por meio da importação automática (se a regra de alocação de importação automática estiver definida no grupo).

AWS Management Console

Como alterar o status de monitoramento de um CIDR alocado para uma VPC

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Resources (Recursos).
3. No menu suspenso na parte superior do painel de conteúdo, escolha o escopo privado que você quer usar.
4. No painel de conteúdo, escolha a VPC e exiba os detalhes dela.
5. Em CIDRs da VPC, selecione um dos CIDRs alocados para a VPC e escolha Ações > Marcar como ignorado ou Desmarcar como ignorado.
6. Selecione Mark as ignored (Marcar como ignorado) ou Unmark as ignored (Desmarcar como ignorado).

Command line

Use os seguintes comandos da AWS CLI para alterar o estado de monitoramento da CIDR de uma VPC:

1. Obter um ID de escopo: describe-ipam-scopes
2. Exibir o estado de monitoramento atual do CIDR da VPC: get-ipam-resource-cidrs
3. Alterar o estado do CIDR da VPC: modify-ipam-resource-cidr
4. Exibir o novo estado de monitoramento do CIDR da VPC: get-ipam-resource-cidrs

Criar escopos adicionais

Siga as etapas nesta seção para criar um escopo adicional.

Um escopo é o contêiner de nível mais alto dentro do IPAM. Quando você cria um IPAM, ele cria dois escopos padrão para você. Cada escopo representa o espaço IP de uma única rede. O escopo privado é destinado a todo o espaço privado. O escopo público é destinado a todo o espaço público. Os escopos permitem que você reutilize endereços IP em várias redes não conectadas sem causar sobreposição ou conflito de endereços IP.

Ao criar um IPAM, os escopos padrão (um privado e um público) são criados para você. É possível criar escopos privados adicionais. Não é possível criar escopos públicos adicionais.

Se você precisar de suporte para várias redes privadas desconectadas, é possível criar escopos privados adicionais. Escopos privados adicionais permitem criar grupos e gerenciar recursos que usam o mesmo espaço IP.

> **Important**
>
> Se o IPAM descobrir recursos com CIDRs IPv4 privado ou IPV6 privado, os CIDRs dos recursos serão importados para o escopo privado padrão e não aparecerão em nenhum escopo privado adicional que você criar. Você pode mover CIDRs do escopo privado padrão para outro escopo privado. Para mais informações, consulte Mover CIDRs da VPC entre escopos.

AWS Management Console

Para criar um escopo privado adicional

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Scopes (Escopos).
3. Escolha Create scope (Criar escopo).
4. Escolha o IPAM ao qual você deseja adicionar o escopo.
5. Adicione uma descrição para o escopo.
6. Escolha Create scope (Criar escopo).
7. Você pode visualizar o escopo no IPAM escolhendo Scopes (Escopos) no painel de navegação.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para criar um escopo privado adicional:

1. Visualizar escopos atuais: describe-ipam-scopes
2. Criar um novo escopo privado :create-ipam-scope
3. Visualizar escopos atuais para visualizar o novo escopo: describe-ipam-scopes

Excluir um IPAM

Você pode querer excluir um IPAM caso ele não seja mais necessário, caso precise reestruturar seu gerenciamento de endereços IP ou caso queira começar do zero com uma nova configuração de IPAM. A exclusão de um IPAM pode ajudar a simplificar o gerenciamento de endereços IP e a estar alinhado com as mudanças nos requisitos comerciais ou operacionais.

Siga as etapas nesta seção para excluir um IPAM. Para obter informações sobre como aumentar o número padrão de IPAMs que você pode ter em vez de excluir um IPAM existente, consulte Cotas para o IPAM.

> **Note**
>
> A exclusão de um IPAM remove todos os dados monitorados associados a ele, incluindo os dados históricos de CIDRs.

AWS Management Console

Para excluir um IPAM

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione IPAMs.
3. No painel de conteúdo, selecione seu IPAM.
4. Escolha Actions (Ações) > Delete (Excluir).
5. Execute um destes procedimentos:
   - Escolha Cascade delete (Exclusão em cascata) para excluir o IPAM, escopos privados, grupos em escopos privados e quaisquer alocações nos grupos em escopos privados. Você não pode excluir o IPAM com essa opção se houver um grupo no escopo público. Se você usar essa opção, o IPAM realizará faz o seguinte:
     - Desloca todos os CIDRs alocados a recursos da VPC (como VPCs) em grupos em escopos privados.

> **Note**
>
> Nenhum recurso da VPC é excluído devido à habilitação dessa opções. O CIDR associado ao recurso não será mais alocado de um grupo do IPAM, mas o CIDR em si permanecerá inalterado.

- Desaprovisiona todos os CIDRs IPv4 provisionados para grupos do IPAM em escopos privados.
- Exclui todos os grupos do IPAM em escopos privados.
- Exclui todos os escopos privados não padrão no IPAM.
- Exclui os escopos públicos e privados padrão e o IPAM.

- Se você não escolher a caixa de seleção Cascade delete (Exclusão em cascata), antes de poder excluir um IPAM, deverá fazer o seguinte:
  - Libere as alocações nos grupos do IPAM. Para obter mais informações, consulte Liberar uma alocação.
  - Desprovisione os CIDRs provisionados para grupos dentro do IPAM. Para obter mais informações, consulte Desprovisionar CIDRs de um grupo.
  - Exclua quaisquer escopos não padrão adicionais. Para obter mais informações, consulte Excluir um escopo.
  - Exclua seus grupos do IPAM. Para obter mais informações, consulte Excluir um grupo.

6. Insira **`delete`** e escolha Delete (Excluir).

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para excluir um IPAM:

1. Visualizar os IPAMs atuais: describe-ipams
2. Excluir um IPAM: delete-ipam
3. Visualizar os IPAMs atualizados: describe-ipams

Para criar um novo IPAM, consulte Criar um IPAM.

Excluir um grupo

Um grupo do IPAM na AWS representa um intervalo definido de endereços IP que podem ser alocados e gerenciados em uma organização ou ambiente da AWS específicos. Os grupos são usados para organizar o espaço de endereços IP, permitir o gerenciamento automatizado de endereços IP e aplicar políticas de governança de endereços IP em toda a sua infraestrutura de nuvem.

Você pode querer excluir um grupo do IPAM para remover um espaço de endereço IP não utilizado ou desnecessário e recuperá-lo para outros fins. Não é possível excluir um grupo de endereços IP se houver alocações nele. Primeiro é necessário liberar as alocações e Desprovisionar CIDRs de um grupo antes que o grupo possa ser excluído.

Siga as etapas nesta seção para excluir um grupo do IPAM.

AWS Management Console

Para excluir um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. No menu suspenso na parte superior do painel de conteúdo, escolha o escopo que você quer usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. No painel de conteúdo, selecione o grupo com o CIDR que você deseja excluir.
5. Escolha Actions (Ações) > Delete pool (Excluir grupo).
6. Insira **`delete`** e escolha Delete (Excluir).

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para excluir um grupo:

1. Visualizar grupos e obter um ID de grupo do IPAM: describe-ipam-pools
2. Excluir um grupo: delete-ipam-pool
3. Visualizar seus grupos: describe-ipam-pools

Para criar um novo grupo, consulte Criar um grupo de IPv4 de nível superior.

Excluir um escopo

Você pode querer excluir um escopo do IPAM caso ele não atenda mais à finalidade pretendida, como quando você reestrutura a rede, consolida regiões ou ajusta a alocação de endereços IP. A exclusão de escopos não utilizados pode ajudar a otimizar sua configuração do IPAM e o gerenciamento de endereços IP na AWS.

> **Note**
>
> É possível excluir um escopo se uma das seguintes situações for verdadeira:
>
> - O escopo é um escopo padrão. Quando você cria um IPAM, dois escopos padrão (um público e um privado) são criados automaticamente e não podem ser excluídos. Para ver se um escopo é padrão, veja o Scope type (Tipo de escopo) nos detalhes do escopo.
> - Há um ou mais grupos no escopo. Primeiro é necessário Excluir um grupo antes que o escopo possa ser excluído.

AWS Management Console

Para excluir um escopo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Scopes (Escopos).
3. No painel de conteúdo, escolha o escopo que você quer excluir.
4. Escolha Actions (Ações) > Delete scope (Excluir escopo).
5. Insira **`delete`** e escolha Delete (Excluir).

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para excluir um escopo:

1. Visualizar escopos: describe-ipam-scopes

2. Excluir um escopo: delete-ipam-scope
3. Visualizar escopos atualizados: describe-ipam-scopes

Para criar um novo escopo, consulte Criar escopos adicionais. Para excluir o IPAM, consulte Excluir um IPAM.

Desprovisionar CIDRs de um grupo

Você pode querer desprovisionar um CIDR do grupo para liberar espaço de endereços IP, simplificar o gerenciamento de endereços IP, preparar-se para mudanças na rede ou atender aos requisitos de conformidade. O desprovisionamento de um CIDR do grupo permite um melhor controle e otimização de suas alocações de endereços IP no IPAM, ao mesmo tempo em que garante que o espaço de IP não utilizado seja recuperado e disponibilizado para uso futuro. Não será possível desprovisionar o CIDR se houver alocações no grupo. Para remover alocações, consulte the section called “Liberar uma alocação”.

Siga as etapas nesta seção para desprovisionar CIDRs de um grupo do IPAM. Ao desprovisionar todos os CIDRs do grupo, o grupo não poderá mais ser usado para alocações. Primeiro, é necessário provisionar um novo CIDR para o grupo antes de poder usar o grupo para alocações.

AWS Management Console

Para desprovisionar o CIDR de um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. No menu suspenso na parte superior do painel de conteúdo, escolha o escopo que você quer usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. No painel de conteúdo, escolha o grupo com o CIDR que você deseja desprovisionar.
5. Escolha a guia CIDRs.
6. Selecione um ou mais CIDRs e escolha Deprovision CIDRs (Desprovisionar CIDRs).
7. Escolha Deprovision CIDR (Desprovisionar CIDR).

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para desprovisionar o CIDR de um grupo:

1. Obter um ID de grupo do IPAM: describe-ipam-pools
2. Visualizar seus CIDRs atuais do grupo: get-ipam-pool-cidrs
3. Desprovisionar CIDRs: deprovision-ipam-pool-cidr
4. Visualizar seus CIDRs atualizados: get-ipam-pool-cidrs

Para provisionar um novo CIDR para o grupo, consulte Desprovisionar CIDRs de um grupo. Se quiser excluir o grupo, consulte Excluir um grupo.

Editar um grupo do IPAM

Você pode querer editar um grupo para executar uma das seguintes ações:

- Alterar as regras de alocação do grupo. Para obter mais informações sobre etiquetas de alocação de custos, consulte Criar um grupo de IPv4 de nível superior.
- Modificar o nome, a descrição ou outros metadados do grupo para melhorar a organização e visibilidade no IPAM.
- Alterar as opções do grupo, como importação automática de recursos descobertos, para otimizar o gerenciamento automatizado de endereços IP do IPAM.

Siga as etapas nesta seção para editar um grupo do IPAM.

AWS Management Console

Para editar um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, o escopo privado padrão é selecionado. Se você não quiser usar o escopo privado padrão, no menu suspenso na parte superior do painel de conteúdo, escolha o escopo que deseja usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM
4. No painel de conteúdo, selecione o grupo com o CIDR que você deseja editar.
5. Selecione Actions (Ações) > Edit (Editar).

6. Faça as alterações que você precisa nos grupos. Para obter mais informações sobre as opções de configuração do grupo, consulte Criar um grupo de IPv4 de nível superior.
7. Selecione Atualizar.

Command line

Use os seguintes comandos da AWS CLI para editar um grupo:

1. Obter um ID de grupo do IPAM: describe-ipam-pools
2. Modificar o grupo: modify-ipam-pool

Habilitar a distribuição de custos

Ao habilitar a distribuição de custos, você distribui as cobranças por endereços IP ativos para as contas que usam os endereços IP, e não para o proprietário do IPAM. Isso é útil para grandes organizações em que o administrador delegado do IPAM gerencia os endereços IP centralmente usando o IPAM e cada conta é responsável por seu próprio uso, eliminando a necessidade de cálculos de cobrança manuais.

A opção de distribuição de custos está disponível quando você cria um IPAM ou modifica um IPAM no Modo de medição, onde:

- Proprietário do IPAM (padrão): a conta da AWS proprietária do IPAM é cobrada por todos os endereços IP ativos gerenciados no IPAM.
- Proprietário do recurso: a conta da AWS que possui o endereço IP é cobrada pelo endereço IP ativo.

Requisitos

- Seu IPAM deve estar integrado ao AWS Organizations.
- O IPAM deve ter sido criado pelo administrador delegado do IPAM em sua organização da AWS.
- A região de origem do IPAM deve ser uma região habilitada por padrão. Não pode ser uma região de adesão.

Como a cobrança funciona

- Embora você possa distribuir cobranças de endereço IP dentro de uma organização, todas as cobranças do IPAM são consolidadas na conta pagante da organização por meio do faturamento consolidado do AWS Organizations.
- Quando a distribuição de custos está habilitada, as contas dos membros da organização ainda podem visualizar o uso e as cobranças individuais do IPAM nas faturas da conta.
- O ARN do IPAM aparecerá nas faturas de contas individuais quando a distribuição de custos estiver habilitada, o que permitirá que os proprietários de recursos rastreiem o uso do IP ativo do IPAM. Se você usar o Exportações de dados da AWS, as cobranças do IPAM aparecerão com o ARN do IPAM associado nas faturas de contas consolidadas e individuais.
- Somente contas dentro da organização do administrador delegado podem receber cobranças pelos recursos que possuem. Os custos dos endereços IP fora da organização são cobrados do proprietário do IPAM.

Restrições de tempo

- Você tem 24 horas para desistir após ativar a distribuição de custos. Depois de 24 horas, não será possível alterar a configuração por 7 dias. Após 7 dias, você poderá desabilitar a distribuição de custos.

Integrar o VPC IPAM à infraestrutura da Infoblox

A integração entre o IPAM da Amazon VPC e a Infoblox conecta seu Gerenciador de endereços IP (IPAM) da AWS VPC com a Infoblox, permitindo que você gerencie endereços IP da AWS por meio de seus fluxos de trabalho existentes da Infoblox enquanto obtém recursos nativos da nuvem da AWS.

Essa integração resolve um desafio corporativo comum: evitar sistemas duplicados de gerenciamento de IP. Em vez de aprender novas ferramentas e manter processos separados para redes on-premises e da AWS, você pode designar a Infoblox como a autoridade de gerenciamento dos escopos IPAM da VPC e continuar usando sua interface familiar da Infoblox para todas as operações de endereço IP.

Visão geral do processo de integração

As etapas a seguir fornecem uma visão geral do processo de integração completo:

1. Configurar escopo do IPAM (descrito neste documento): o administrador delegado do IPAM da Amazon VPC cria um novo escopo ou modifica um escopo existente para usar a Infoblox como sua autoridade externa.
2. Configurar a Infoblox (descrito fora deste documento): consulte Próximas etapas.
3. Criar um pool de alto nível: o administrador delegado do IPAM da Amazon VPC cria um pool no escopo vinculado à Infoblox. O pool começa sem nenhum CIDR atribuído.
4. Provisionar CIDR de uma autoridade externa: o administrador delegado do IPAM da Amazon VPC provisiona um CIDR para o pool. Você pode solicitar qualquer CIDR disponível (a Infoblox escolhe o intervalo permitido) ou solicitar um CIDR específico (a Infoblox aceita ou rejeita com base na disponibilidade). O IPAM se coordena automaticamente com a Infoblox para obter e provisionar o CIDR aprovado.
5. Continuar com as operações do IPAM padrão: crie VPCs e pools secundários a partir do CIDR alocado usando procedimentos padrão do IPAM da Amazon VPC.

Quando usar essa integração

Use essa integração se você já usa ou planeja usar a Infoblox para gerenciamento de rede on-premises e deseja estender suas práticas existentes de gerenciamento de IP para a AWS sem manter sistemas separados.

Pré-requisitos

Antes de configurar essa integração, verifique se você tem:

- Nível avançado do IPAM da VPC: habilitado na sua conta da AWS. Para mais informações, consulte Nível avançado do IPAM da VPC.
- Permissões do IAM necessárias: listadas abaixo
- Identificador de recurso da Infoblox: do seu administrador da Infoblox

Perfil do IAM para Infoblox

Crie um perfil do IAM para a entidade principal da Infoblox ou use um perfil existente. A função precisa dessas permissões:

- `ec2:DescribeIpamPools`

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

Para obter instruções sobre como adicionar essas permissões a um perfil do IAM, consulte Adicionar e remover permissões de identidade do IAM no Guia do usuário do IAM.

> **Note**
>
> A Infoblox pode exigir permissões para a descoberta do IPAM da VPC, além dessas permissões necessárias para habilitar essa integração.

Configurar a integração da Infoblox no IPAM da VPC

Você pode ativar a integração da Infoblox ao criar ou modificar escopos no console do IPAM da AWS VPC ou da AWS CLI.

> **Important**
>
> A integração com a Infoblox está disponível somente para escopos privados, não públicos.

Criação de um novo escopo com a integração da Infoblox

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha IPAM e, em seguida, selecione Escopos.
3. Escolha Create scope (Criar escopo).
4. Em Configurações de escopo, faça o seguinte:
   - O ID do IPAM é preenchido automaticamente.
   - (Opcional) Em Nome da etiqueta, insira um nome para o escopo.
   - (Opcional) Em Descrição, insira uma descrição para o escopo.
5. Em Autoridade do escopo, escolha IPAM da Infoblox.

6. Para Identificador de recurso da Infoblox, insira o identificador de recurso da Infoblox no formato `<version>.identity.account.<entity_realm>.<entity_id>`.
7. Verifique se você tem as permissões do IAM necessárias conforme exibido na caixa de informações.
8. Escolha Create scope (Criar escopo).

O comando relacionado da AWS CLI para isso é create-ipam-scope.

Modificar escopos existentes

Para alterar a autoridade do escopo do IPAM da Amazon VPC para o IPAM da Infoblox para um escopo existente, edite as configurações do escopo e siga as mesmas etapas de configuração do procedimento anterior.

O comando relacionado da AWS CLI para isso é modify-ipam-scope.

Próximas etapas

Isso completa a configuração do IPAM da Amazon VPC necessária para a integração. Após configurar a autoridade do escopo, você pode criar um pool do IPAM de nível superior dentro do escopo. Para obter mais informações, consulte Criar um grupo de IPv4 de nível superior.

A integração também requer a configuração de um pool de origem da Infoblox, a verificação do status do trabalho de descoberta, a configuração do escopo privado a ser gerenciado pela Infoblox, a habilitação do gerenciamento da Infoblox para o IPAM da Amazon VPC e a criação de pools a partir da integração da Infoblox ou diretamente do portal da Infoblox.

Para obter informações sobre o lado da Infoblox da integração, consulte o Guia do usuário de integração do IPAM da AWS na documentação da Infoblox.

Habilitar o provisionamento de CIDRs de GUA IPv6 privado

Se você quiser que suas redes privadas sejam compatíveis com IPv6 e não tiver intenção de rotear o tráfego desses endereços para a Internet, poderá provisionar um intervalo de ULAs ou GUAs IPv6 privados para um grupo do IPAM em um escopo privado.

Para obter detalhes importantes sobre IPv6 privado, consulte Endereços IPv6 privados no Manual do usuário da Amazon VPC.

Há dois tipos de endereços IPv6 privados:

- Intervalos de ULAs IPv6: endereços IPv6 conforme definição da RFC4193. Esses intervalos de endereços sempre começarão com “fc” ou “fd”, o que os torna facilmente identificáveis. Um espaço de ULAs IPv6 válido é todo espaço abaixo de fd00::/8 que não coincide com o intervalo reservado fd00: :/16 da Amazon.
- Intervalos de GUAs IPv6: endereços IPv6 conforme definição da RFC3587. A opção de usar intervalos de GUAs IPv6 como endereços IPv6 privados está desabilitada por padrão e deve ser habilitada para poder ser usada.

Para usar intervalos de ULAs IPv6, você escolhe a opção IPv6 ao provisionar um CIDR para um grupo do IPAM e insere o intervalo de ULAs IPv6. Porém, para usar seus próprios intervalos de GUAs IPv6 como endereços IPv6 privados, você deve primeiro concluir as etapas desta seção. A opção está desabilitada por padrão.

> **Note**
>
> - Quando você usa intervalos de GUAs IPv6 privado, exigimos que use seus próprios intervalos de GUAs IPv6.
> - O IPAM descobre recursos com endereços IPv6 ULA e GUA e monitora grupos em busca de espaços de endereços IPv6 ULA e GUA sobrepostos.
> - Se você quiser se conectar à Internet a partir de um recurso que tenha um endereço IPv6 privado, poderá fazê-lo, mas deverá rotear o tráfego por um recurso em outra sub-rede com um endereço IPv6 público para ter sucesso.
> - Se você tiver um intervalo de GUAs IPv6 privados alocado para uma VPC, não poderá usar um espaço de GUAs IPv6 públicos que coincida com espaço de GUAs que coincida com o espaço de GUAs iPv6 privados na mesma VPC.
> - A comunicação entre recursos com intervalos de ULAs e GUAs IPv6 privados é compatível (por exemplo, por Direct Connect, emparelhamento de VPC, gateway de trânsito ou conexões da VPN).
> - Um intervalo de IPv6 GUA privado não pode ser convertido em um intervalo de IPv6 GUA anunciado publicamente.

AWS Management Console

Para habilitar o provisionamento de CIDRs de GUA IPv6 privado

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione IPAMs.
3. Escolha seu IPAM e Ações > Editar.
4. Em CIDRs de GUA IPv6 privado, escolha Habilitar provisionamento de espaço de CIDR de GUA para grupos do IPAM com IPv6 privado.
5. Escolha Salvar alterações.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os comandos AWS CLI a seguir para habilitar o provisionamento de CIDRs de GUA IPv6 privado:

1. Visualizar os IPAMs atuais com describe-ipams
2. Modifique o IPAM com modify-ipam e inclua a opção para `enable-private-gua`.

Depois de habilitar a opção de provisionar CIDRs de GUA IPv6 privado, você pode provisionar um CIDR de GUA IPv6 privado para um grupo. Para obter mais informações, consulte Provisionar CIDRs para um grupo.

Impor o uso do IPAM para a criação de VPCs com SCPs

> **Note**
>
> Esta seção só se aplica a você se você tiver habilitado o IPAM para se integrar ao AWS Organizations. Para obter mais informações, consulte Integrar o IPAM a contas em uma organização da AWS Organizations.

Esta seção descreve como criar uma política de controle de serviço no AWS Organizations que exija que os integrantes da organização usem o IPAM quando criarem uma VPC. Políticas de controle

de serviço (SCPs) são um tipo de política organizacional que permite gerenciar permissões na organização. Para obter mais informações, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations.

Aplicar o IPAM ao criar VPCs

Siga as etapas desta seção para exigir que os integrantes da organização usem o IPAM quando criarem VPCs.

Para criar um SCP e restringir a criação de VPCs ao IPAM

1. Siga as etapas descritas em Create a service control policy no Guia do usuário do AWS Organizations e adicione o seguinte texto no editor JSON:

   JSON

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

2. Anexe a política a uma ou mais unidades organizacionais da organização. Para obter mais informações, consulte Attach policies e Detach policies no Guia do usuário do AWS Organizations.

Aplique um grupo do IPAM ao criar VPCs

Siga as etapas desta seção para exigir que os integrantes da organização usem um grupo específico do IPAM quando criarem VPCs.

Para criar um SCP e restringir a criação de VPCs a um grupo do IPAM

1. Siga as etapas descritas em Create a service control policy no Guia do usuário do AWS Organizations e adicione o seguinte texto no editor 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. Altere o valor de exemplo `ipam-pool-0123456789abcdefg` para o ID do grupo IPv4 ao qual você gostaria de restringir os usuários.
3. Anexe a política a uma ou mais unidades organizacionais da organização. Para obter mais informações, consulte Attach policies e Detach policies no Guia do usuário do AWS Organizations.

Aplique o IPAM para todas, exceto uma determinada lista de UOs

Siga as etapas desta seção para aplicar o IPAM para todas as UOs (unidades organizacionais), exceto uma determinada lista. A política descrita nesta seção requer que as unidades organizacionais (UOs) na organização, exceto as que você especificar em `aws:PrincipalOrgPaths`, usem o IPAM para criar e para ampliar as VPCs. As UOs listadas podem usar o IPAM ao criar VPCs ou especificar um intervalo de endereços IP manualmente.

Para criar uma SCP e aplicar o IPAM para todas, exceto uma determinada lista de UOs

1. Siga as etapas descritas em Create a service control policy no Guia do usuário do AWS Organizations e adicione o seguinte texto no editor 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. Remova os valores de exemplo (como `o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/`) e adicione os caminhos da entidade do AWS Organizations das UOs que você deseja ter a opção (mas não exigir) de usar o IPAM. Para obter mais informações sobre o caminho da entidade, consulte Compreender o caminho da entidade do AWS Organizations e aws:PrincipalOrgPaths no Guia do usuário do IAM.
3. Anexe a política à raiz da sua organização. Para obter mais informações, consulte Attach policies e Detach policies no Guia do usuário do AWS Organizations.

Excluir unidades organizacionais do IPAM

Se o IPAM for integrado ao AWS Organizations, você poderá excluir uma unidade organizacional (UO) do gerenciamento pelo IPAM. Quando você exclui uma UO, o IPAM não gerenciará os endereços IP nas contas dessa UO. Esse atributo oferece mais flexibilidade no uso do IPAM.

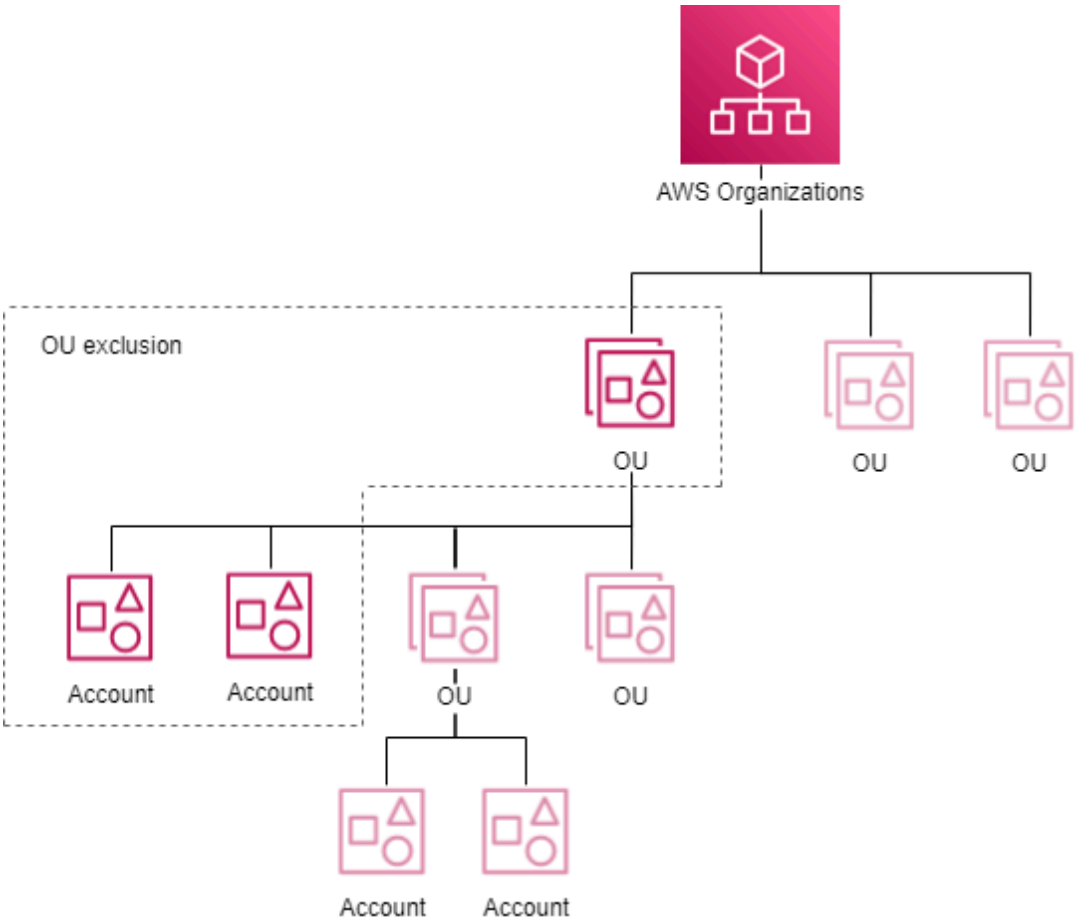
Você pode usar exclusões de UO das seguintes maneiras:

- Habilitar o IPAM para partes específicas da empresa: se tiver várias unidades de negócios ou subsidiárias no AWS Organizations, agora você poderá usar o IPAM apenas nas que precisarem dele.
- Manter as contas de sandbox separadas: você pode excluir as contas de sandbox do IPAM, concentrando-se apenas nas contas que realmente importam para o gerenciamento de endereços IP.

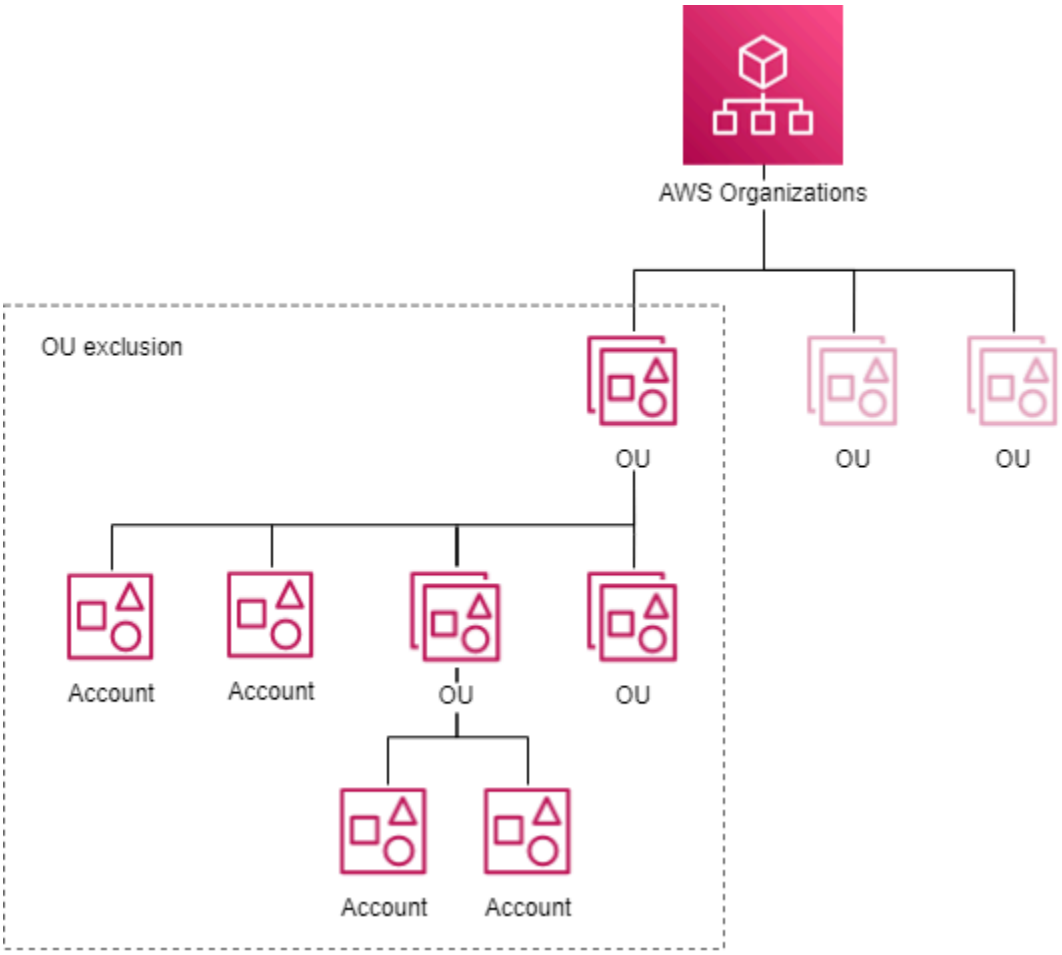
Como funcionam as exclusões de UO

Os diagramas desta seção demonstram dois casos de uso da adição de exclusões de UO no IPAM.

O primeiro diagrama mostra o impacto da adição de uma exclusão de unidade organizacional (UO) em uma UO superior apenas. Como resultado, o IPAM não gerenciará os endereços IP nas contas da UO superior. O IPAM gerenciará os endereços IP nas contas das outras UOs não incluídas na exclusão.



O segundo diagrama mostra o impacto da adição de uma exclusão de uma unidade organizacional (UO) superior e de todas as UOs subordinadas. Como resultado, o IPAM não gerenciará os endereços IP nas contas da UO superior nem nas contas das UOs subordinadas. O IPAM gerenciará os endereços IP nas contas das UOs fora da exclusão.



Adicionar ou remover exclusões de UO

Conclua as etapas desta seção para adicionar ou remover exclusões de UO.

> **Note**
>
> - A conta de administrador delegado do IPAM não é excluída, mesmo que esteja em uma UO que é excluída.
> - O IPAM deve ser integrado com o AWS Organizations para adicionar uma exclusão de UO seja adicionada. A organização deve conter UOs.
> - Você deve ser o administrador delegado do IPAM para visualizar, adicionar ou remover exclusões de UO.

- O IPAM leva algum tempo para descobrir unidades organizacionais recém-criadas.
- Existe uma cota padrão para o número de exclusões que você pode adicionar por descoberta de recursos. Para obter mais informações, consulte Exclusões de unidade organizacional por descoberta de recursos em Cotas para o IPAM.
- Se você compartilhar uma descoberta de recursos com outra conta, essa outra conta poderá ver as exclusões de UO, as quais contêm informações como o ID da organização, o ID da raiz e os IDs das unidades organizacionais da organização do proprietário da descoberta de recursos.

AWS Management Console

Para adicionar ou remover exclusões de UO

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Descobertas de recursos.
3. Escolha a descoberta de recursos padrão.
4. Escolha Edit.
5. Em Exclusões de unidades organizacionais, faça o seguinte:
   - Para adicionar uma exclusão de UO:
     - Se você quiser excluir a UO e todas as suas UOs subordinadas:
       - Localize a UO na tabela e marque a caixa de seleção correspondente. Todas as UOs subordinadas serão selecionadas automaticamente.
     - Se você quiser excluir apenas as contas da UO superior:
       - Localize a UO na tabela e marque a caixa de seleção correspondente. Todas as UOs subordinadas serão selecionadas automaticamente. Desmarque todas as UOs subordinadas.
     - Como alternativa, você pode usar a coluna Ações para selecionar apenas uma UO superior ou uma UO superior e suas subordinadas:
       - Selecionar todas as UOs subordinadas: inclua todas as UOs subordinadas na exclusão. Como resultado da escolha de uma UO, ela é adicionada na tela. Cada UO contém o ID e o caminho da entidade da exclusão de UO.

- Selecionar apenas essa UO: inclua somente essa UO na exclusão. Como resultado da escolha de uma UO, ela é adicionada na tela. Cada UO contém o ID e o caminho da entidade da exclusão de UO.
- Copiar caminho de entidade da UO: copie o caminho da entidade da organização para usar conforme necessário.

- Se você já souber o caminho da entidade do AWS Organizations ou desejar criá-lo:
  - Escolha Inserir exclusão da unidade organizacional e insira o caminho da entidade da exclusão de UO. Crie o caminho para as UOs usando os IDs do AWS Organizations separados por uma `/`. Inclua todas as UOs subordinadas terminando o caminho com `/*`.
    - Exemplo 1
      - Caminho para uma UO subordinada: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscccccc/ou-jkl0-awsddddd/`
      - Neste exemplo, `o-a1b2c3d4e5` é o ID da organização, `r-f6g7h8i9j0example` é o ID da raiz, `ou-ghi0-awscccccc` é o ID de uma UO e `ou-jkl0-awsddddd` é o ID de uma UO subordinada.
      - O IPAM não gerenciará os endereços IP nas contas da UO subordinada.
    - Exemplo 2
      - Caminho no qual todas as UOs subordinadas serão incluídas na exclusão: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awscccccc/*`
      - Neste exemplo, o IPAM não gerenciará os endereços IP nas contas da UO (`ou-ghi0-awscccccc`) nem nas contas das UOs subordinadas a ela.
- Para remover uma exclusão de UO:
  - Escolha o X ao lado de uma UO que já foi adicionada. A `/*` depois do ID da UO indica que é se trata de uma UO superior e que as UOs subordinadas estão incluídas da exclusão de UO.

6. Escolha Salvar alterações.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

1. Visualize os detalhes da descoberta de recursos para obter o ID da descoberta de recursos padrão para a próxima etapa com describe-ipam-resource-discoveries.

   Entrada:

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

   Resultado:

```
{

    "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. Adicione ou remova uma exclusão de unidade organizacional de uma descoberta de recursos com modify-ipam-resource-discovery e as opções `--add-organizational-unit-exclusions` ou `--remove-organizational-unit-exclusions`. Você precisará inserir um caminho de entidade do AWS Organizations. Crie o caminho para as UOs usando os IDs do AWS Organizations separados por uma `/`. Inclua todas as UOs subordinadas terminando o caminho com `/*`. Não é possível incluir o mesmo caminho de entidade mais de uma vez nos parâmetros de adição ou remoção.

   - Exemplo 1
     - Caminho para uma UO subordinada: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
     - Neste exemplo, `o-a1b2c3d4e5` é o ID da organização, `r-f6g7h8i9j0example` é o ID da raiz, `ou-ghi0-awsccccc` é o ID de uma UO e `ou-jkl0-awsddddd` é o ID de uma UO subordinada.
     - O IPAM não gerenciará os endereços IP nas contas da UO subordinada.
   - Exemplo 2
     - Caminho no qual todas as UOs subordinadas serão incluídas na exclusão: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
     - Neste exemplo, o IPAM não gerenciará os endereços IP nas contas da UO (`ou-ghi0-awsccccc`) nem nas contas das UOs subordinadas a ela.

> **Note**
>
> O conjunto resultante de exclusões não deve "se sobrepor", o que significa que duas ou mais exclusões de UO não devem excluir a mesma UO.
> Exemplo de caminhos de entidade não sobrepostos:
>
> - Caminho 1 = "o-1/r-1/ou-1/"
> - Caminho 2 = "o-1/r-1/ou-1/ou-2/"
>
> Esses caminhos não se sobrepõem porque Caminho 1 exclui somente as contas sob ou-1 e Caminho 2 exclui somente as contas sob ou-2.
> Exemplo de caminhos de entidade sobrepostos:
>
> - Caminho 1 = "o-1/r-1/ou-1/*"
> - Caminho 2 = "o-1/r-1/ou-1/ou-2/"
>
> Esses caminhos se sobrepõem porque Caminho 1 representa tanto "o-1/r-1/ou-1/" quanto "o-1/r-1/ou-1/ou-2/" e "o-1/r-1/ou-1/ou-2/" se sobrepõe a Caminho 2.

Entrada:

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

Resultado:

```
{
    "IpamResourceDiscovery": {
        "OwnerId": "111122223333",
        "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",
```

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

Criar um nível de IPAM

O IPAM oferece dois níveis: nível gratuito e nível avançado. A mudança para o nível avançado do Gerenciador de endereços IP da Amazon VPC fornece um controle mais granular do gerenciamento de endereços IP. Isso pode ser benéfico à medida que a complexidade da rede aumenta, permitindo que você otimize e gerencie melhor seu espaço de endereços IP. Para obter mais informações sobre os recursos disponíveis no nível gratuito e os custos associados ao nível avançado, consulte a guia IPAM na página de preços do Amazon VPC.

Note

Antes de mudar do nível avançado para o nível gratuito, você deve:

- Excluir grupos de escopo privado.
- Excluir âmbitos de aplicação privados não predefinidos.
- Excluir grupos com localidades diferentes da região de origem do IPAM.
- Excluir associações de descoberta de recursos não padrão.
- Excluir alocações de grupo para contas que não são proprietárias do IPAM.

AWS Management Console

Para modificar o nível IPAM

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione IPAMs.
3. No painel de conteúdo, selecione seu IPAM.
4. Selecione Actions (Ações) > Edit (Editar).

> **Note**
>
> Se você estiver no nível gratuito, verá Sua estimativa de contagem total de IPs ativos do IPAM é....
> A contagem total de IPs ativos representa o número de endereços IP ativos no seu IPAM pelos quais seria cobrada uma taxa se você migrasse do nível gratuito para o nível avançado. Um endereço IP ativo é definido como um endereço IP ou um prefixo associado a uma interface de rede elástica (ENI) anexada a um recurso, como uma instância do EC2.
>
> - Essa métrica só está disponível para os clientes do nível gratuito.
> - Se seu IPAM estiver integrado ao AWS Organizations, a contagem de IPs ativos cobrirá todas as contas da organização.
> - Você não pode ver um detalhamento do número de endereços IP ativos por tipo de IP (público/privado) ou classe (IPv4/IPv6).
> - O IPAM só conta os IPs de ENIs pertencentes a contas monitoradas. O número pode não ser exato para sub-redes compartilhadas. Os endereços IP serão excluídos se o proprietário da sub-rede ou da ENI não for coberto pelo IPAM.

5. Escolha o nível do IPAM que você deseja usar para o IPAM.
6. Escolha Salvar alterações.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Utilize os seguintes comandos AWS CLI para visualizar e modificar um nível do IPAM:

1. Visualizar os IPAMs atuais: describe-ipams
2. Modifique o nível do IPAM: modify-ipam
3. Visualizar os IPAMs atualizados: describe-ipams

Modificar regiões operacionais do IPAM

As regiões operacionais são as regiões da AWS em que o IPAM terá permissão para gerenciar CIDRs de endereços IP. O IPAM apenas descobre e monitora recursos somente nas regiões da AWS que você seleciona como regiões operacionais.

Adicionar uma região operacional a um IPAM permite gerenciar o espaço de endereços IP em várias regiões da AWS. Essa adição pode melhorar a utilização de endereços IP, permite a segmentação regional e é compatível com uma infraestrutura distribuída geograficamente. A expansão do escopo regional do IPAM oferece maior flexibilidade e controle sobre o gerenciamento geral de endereços IP.

AWS Management Console

Para modificar as regiões operacionais do IPAM

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione IPAMs.
3. No painel de conteúdo, selecione seu IPAM.
4. Selecione Actions (Ações) > Edit (Editar).
5. Em Configurações do IPAM, escolha as regiões operacionais que você deseja usar para o IPAM.
6. Escolha Salvar alterações.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Utilize os seguintes comandos AWS CLI para visualizar e modificar um nível do IPAM:

1. Visualizar os IPAMs atuais: describe-ipams

2. Adicionar ou remover regiões operacionais do IPAM: modify-ipam
3. Visualizar os IPAMs atualizados: describe-ipams

Provisionar CIDRs para um grupo

Siga as etapas nesta seção para provisionar CIDRs para um grupo. Se você já provisionou um CIDR quando criou o grupo, talvez seja necessário provisionar CIDRs adicionais se um grupo estiver perto da alocação completa. Para monitorar o uso do grupo, consulte Monitorar o uso do CIDR com o painel do IPAM.

> **Note**
>
> Os termos provisionar e alocar são usados em todo este guia do usuário e no console do IPAM. Provisionar é usado quando você adiciona um CIDR a um grupo do IPAM. Alocar é usado quando você associa um CIDR de um grupo do IPAM a uma VPC ou endereço IP elástico.

AWS Management Console

Para provisionar CIDRs para um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, o escopo privado padrão é selecionado. Se você não quiser usar o escopo privado padrão, no menu suspenso na parte superior do painel de conteúdo, escolha o escopo que deseja usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. No painel de conteúdo, escolha o grupo em que você quer adicionar um CIDR.
5. Escolha Actions (Ações) >Provision CIDRs (Provisionar CIDRs).
6. Execute um destes procedimentos:

   - Se você estiver provisionando um CIDR para um grupo no escopo público, insira a máscara de rede.
   - Se você estiver provisionando um CIDR para um grupo de IPv4 no escopo privado, insira o CIDR.

- Se você estiver provisionando um CIDR para um grupo de IPv6 no escopo privado, observe o seguinte:
  - Para obter detalhes importantes sobre IPv6 privado, consulte Endereços IPv6 privados no Manual do usuário da Amazon VPC.
  - Para usar um intervalo de ULAs IPv6 privados, em CIDRs para provisionar, escolha Adicionar CIDR de ULA por máscara de rede e escolha um tamanho de máscara de rede ou escolha Inserir CIDRs IPv6 privado e insira um intervalo de ULAs. Os intervalos válidos de ULAs IPv6 privados são de /9 a /60, a partir de fd80::/9.
  - Para usar um intervalo de GUAs IPv6 privados, você precisa primeiro habilitar a opção no IPAM (consulte Habilitar o provisionamento de CIDRs de GUA IPv6 privado). Depois de habilitar os CIDRs de GUA IPv6 privado, insira um GUA IPv6 em Inserir CIDR IPv6 privado.

> **Note**
>
> - Por padrão, é possível adicionar um bloco CIDR IPv6 fornecido pela Amazon com um grupo regional. Para obter informações sobre como aumentar o limite padrão, consulte Cotas para o IPAM.
> - O CIDR que você deseja provisionar deve estar disponível no escopo.
> - Se você estiver provisionando CIDRs para um grupo dentro de um grupo, o espaço CIDR que você deseja provisionar deverá estar disponível no grupo.

7. Escolha Provisionar.
8. Você pode visualizar o CIDR no IPAM escolhendo Pools (Grupos) no painel de navegação, escolhendo um grupo e visualizando a guia “CIDRs” do grupo.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para provisionar CIDRs para um grupo:

1. Obter o ID de grupo do IPAM: describe-ipam-pools
2. Obter os CIDRs que são provisionados para o grupo: get-ipam-pool-cidrs

3. Provisionar um novo CIDR para o grupo: provision-ipam-pool-cidr
4. Obter os CIDRs que são provisionados para o grupo e visualizar o novo CIDR: get-ipam-pool-cidrs

Mover CIDRs da VPC entre escopos

Mover os CIDRs entre escopos permite que você otimize a alocação de endereços IP, organize por região, separe os problemas, imponha a conformidade e se adapte às mudanças na infraestrutura. Essa flexibilidade ajuda a gerenciar seu espaço de endereços IP de forma eficiente à medida que as workloads se desenvolvem.

Siga as etapas nesta seção para mover o CIDR da VPC de um escopo para outro.

Important

- Você só pode mover CIDRs da VPC. Quando você move um CIDR da VPC, os CIDRs de sub-rede da VPC também são movidos automaticamente.
- Você só pode mover CIDRs da VPC de um escopo privado para outro. Não é possível mover CIDRs da VPC de um escopo público para um escopo privado ou de um escopo privado para um escopo público.
- A mesma conta da AWS deve ter ambos os escopos.
- Se um CIDR da VPC estiver alocado a partir de um grupo em um escopo privado, a solicitação de movimentação terá sucesso, mas o CIDR da VPC não será movido até que você libere a alocação de CIDR da VPC do grupo atual. Para saber mais sobre como liberar uma alocação, consulte Liberar uma alocação.

AWS Management Console

Para mover um CIDR alocado para uma VPC

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Resources (Recursos).
3. No menu suspenso na parte superior do painel de conteúdo, escolha o escopo que você quer usar.
4. No painel de conteúdo, escolha uma VPC e exiba os detalhes dela.

5. Em VPC CIDRs (CIDRs da VPC), selecione um dos CIDRs alocados ao recuso e escolha Actions (Ações) > Move CIDR to different scope (Mover CIDR para um escopo diferente).
6. Selecione o escopo para o qual você deseja mover o CIDR da VPC.
7. Escolha Move CIDR to different scope (Mover CIDR para um escopo diferente).

Command line

Use os seguintes comandos da AWS CLI para mover um CIDR da VPC:

1. Obter um CIDR da VPC no escopo atual: get-ipam-resource-cidrs
2. Mover um CIDR da VPC: modify-ipam-resource-cidr
3. Obter um CIDR da VPC no outro escopo: get-ipam-resource-cidrs

Definir a estratégia de alocação de IPv4 público com as políticas do IPAM

Uma política do IPAM é um conjunto de regras que define como os endereços IPv4 públicos dos pools do IPAM são alocados aos recursos da AWS. Cada regra associa um serviço da AWS aos grupos do IPAM que o serviço usará para acessar endereços IP. Uma única política pode ter várias regras e ser aplicada a várias regiões da AWS. Se o grupo do IPAM ficar sem endereços, os serviços retornarão aos endereços IP fornecidos pela Amazon. Uma política pode ser uma conta da AWS individual ou uma entidade dentro das AWS Organizations. Se você trouxer seu próprio IP (BYOIP), isso ajudará a reduzir seus custos com IPv4 público da AWS.

Quando usar as políticas do IPAM

Use as políticas do IPAM para:

- Reduzir os custos com IPv4 públicos usando endereços BYOIP
- Controlar centralmente quais pools de IP seus recursos da AWS usam
- Garantir uma alocação consistente de IP em toda a sua organização

Como funciona

Quando você cria um recurso da AWS que precisa de um endereço IP público em uma conta com políticas do IPAM aplicadas:

- O IPAM verifica suas regras de política em ordem.
- Se uma regra corresponder ao tipo de recurso, o IPAM aloca um IP do pool especificado.
- Se o pool estiver vazio e o estouro estiver habilitado, a Amazon fornecerá um endereço IP.
- Se nenhuma regra corresponder, o comportamento padrão será aplicado.

Serviços e recursos compatíveis

Você pode criar políticas do IPAM para definir como os endereços IPv4 públicos dos pools do IPAM são alocados aos seguintes serviços e recursos da AWS:

- Endereços IP elásticos (EIPs – Elastic IP addresses)
- Application Load Balancers (ALBs)
- Amazon Relational Database Service (RDS)
- Gateways NAT regionais

> **Important**
>
> Se você escolher um pool do IPAM ou ID de alocação do EIP específico ao criar um recurso da AWS, isso substituirá a política do IPAM.

Pré-requisitos

- Um IPAM na conta de administrador delegado com o nível avançado habilitado
- Um pool do IPAM público com endereços IPv4
- Permissões do IAM para operações de IPAM e EC2

Terminologia

Política do IPAM

Uma política do IPAM é um conjunto de regras que define como os endereços IPv4 públicos dos pools do IPAM são alocados aos recursos da AWS. Cada regra associa um serviço da AWS aos grupos do IPAM que o serviço usará para acessar endereços IP. Uma única política pode ter várias regras e ser aplicada a várias regiões da AWS. Se o grupo do IPAM ficar sem endereços, os serviços retornarão aos endereços IP fornecidos pela Amazon. Uma política pode ser uma

conta da AWS individual ou uma entidade dentro das AWS Organizations. Uma política pode ser uma conta da AWS individual ou uma entidade dentro das AWS Organizations.

Regras de alocação

As configurações opcionais dentro de uma política do IPAM que mapeiam os tipos de recursos da AWS a pools do IPAM específicos. Se nenhuma regra for definida, os tipos de recurso usarão como padrão os endereços IP fornecidos pela Amazon.

Target

Uma conta da AWS individual ou uma entidade dentro de uma organização da AWS à qual uma política do IPAM pode ser aplicada.

Etapa 1: criar uma política do IPAM

Usando o Console da AWS:

Para criar uma política do IAM usando o Console da AWS, siga estas etapas:

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação à esquerda, escolha Políticas.
3. Escolha Create policy (Criar política).
4. Insira um nome para a sua política (opcional).
5. Selecione o IPAM a ser associado a essa política.
6. (Opcional) Adicione tags.
7. Escolha Criar política.

Usar a AWS CLI:

Use o comando create-ipam-policy.

Etapa 2: adicionar regras de alocação

Depois de criar a política, você precisa adicionar regras de alocação que definam como os endereços IP são alocados:

Usando o Console da AWS:

Siga estas etapas para adicionar regras de alocação usando o Console da AWS:

1. No painel de navegação à esquerda, escolha Políticas.
2. Selecione a política criada na etapa anterior.
3. Na página de detalhes da sua política, escolha a guia Regras de alocação.
4. Escolha Criar regras de alocação.
5. Defina a Configuração do serviço:
   - Localidade: escolha a região da AWS (us-east-1) ou a zona local em que deseja que essa política seja aplicada.
   - Tipo de recurso: selecione o tipo de recurso ou serviço da AWS para essa política (endereços IP elásticos, instâncias do banco de dados do RDS, Application Load Balancers ou gateways NAT no modo de disponibilidade regional).
6. Defina a configuração das regras:
   - Pool do IPAM: selecione o pool do IPAM que fornecerá os endereços IP.
   - Analise os detalhes do pool (localidade, origem de IP público, espaço disponível e intervalos CIDR disponíveis).
7. (Opcional) Escolha Adicionar nova regra para adicionar mais regras.
8. Escolha Criar regra de alocação.

Usar a AWS CLI:

Use o comando modify-ipam-policy-allocation-rules.

Etapa 3: habilitar a política

Especifique quais contas devem usar essa política.

Usando o Console da AWS:

Siga estas etapas para habilitar a política usando o Console da AWS:

1. Na página de detalhes da sua política, escolha a guia Destinos.
2. Escolha Gerenciar destinos da política.
3. Execute um destes procedimentos:
   - Para o uso com uma única conta (IPAM não integrado com o AWS Organizations), escolha Habilitar para a sua conta.

- Para IPAM integrado com o AWS Organizations (quando você é o administrador delegado):
  - Na seção Estrutura organizacional, selecione as contas ou unidades organizacionais nas quais você deseja aplicar essa política.
  - Marque a caixa de seleção Habilitado para cada destino.
  - Escolha Salvar alterações.
  - Importante: habilitar essa política substituirá todas as políticas ativas do IPAM nas contas ou unidades organizacionais selecionadas.

Usar a AWS CLI:

Use o comando enable-ipam-policy com base na sua configuração:

Para o uso com uma única conta (IPAM não integrado com o AWS Organizations):

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

Para IPAM integrado com o AWS Organizations (quando você é o administrador delegado), defina uma política para segmentar uma conta no AWS Organization:

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

Para IPAM integrado com o AWS Organizations (quando você é o administrador delegado), defina uma política para segmentar uma unidade organizacional:

```
aws ec2 enable-ipam-policy \
    --ipam-policy-id ipam-policy-12345678 \
    --organization-target-id ou-123
```

Important

A ativação dessa política substituirá todas as políticas ativas do IPAM nas contas ou unidades organizacionais selecionadas.

Etapa 4: testar sua política

Crie um novo recurso do tipo que você configurou (como um EIP) em uma das contas de destino. O recurso usará automaticamente um endereço IP do seu pool do IPAM.

> **Important**
>
> Se você escolher um pool do IPAM ou ID de alocação do EIP específico ao criar um recurso da AWS, isso substituirá a política do IPAM.

Etapa 5: Monitorar o uso

Verifique seu pool do IPAM no console para ver os endereços IP sendo alocados aos seus recursos.

Liberar uma alocação

Se você estiver planejando excluir um grupo, talvez seja necessário liberar uma alocação de grupo. Uma alocação é uma atribuição CIDR de um grupo do IPAM para outro recurso ou grupo do IPAM.

Você não poderá excluir grupos se eles tiverem CIDRs provisionados e não poderá desprovisioná-los se os CIDRs forem alocados aos recursos.

> **Note**
>
> - Para liberar uma alocação manual, use as etapas desta seção ou chame a API ReleaseIpamPoolAllocation.
> - Para liberar uma alocação em um escopo privado, você deve ignorar ou excluir o CIDR do recurso. Para obter mais informações, consulte Alterar o estado de monitoramento dos CIDRs da VPC. Depois de algum tempo, o IPAM da Amazon VPC liberará automaticamente a alocação em seu nome.
>
>   Example
>
>   Exemplo
>
>   Se você tiver um CIDR de VPC em um escopo privado, para liberar a alocação, você deve ignorar ou excluir o CIDR da VPC. Depois de algum tempo, o IPAM da Amazon VPC liberará automaticamente a alocação do CIDR da VPC do grupo do IPAM.

- Para liberar uma alocação em um escopo público, você deve excluir o CIDR do recurso. Você não pode ignorar CIDRs de recursos públicos. Para obter mais informações, consulte Cleanup (Limpeza) em Traga seu próprio CIDR IPv4 público para o IPAM usando somente a AWS CLI ou Cleanup (Limpeza) em Traga seu próprio CIDR IPv6 para o IPAM usando somente a AWS CLI. Depois de algum tempo, o IPAM da Amazon VPC liberará automaticamente a alocação em seu nome.

Para que o IPAM da Amazon VPC libere alocações em seu nome, todas as permissões de conta devem ser configuradas corretamente para um uso de conta única ou uso de várias contas.

Ao liberar um CIDR gerenciado pelo IPAM, o IPAM da Amazon VPC o recicla de volta em um grupo do IPAM. Se você estiver usando o IPAM no nível avançado, o CIDR levará alguns minutos para ficar disponível para futuras alocações. Se você estiver usando o IPAM no nível gratuito, o CIDR levará até 48 horas para ficar disponível para futuras alocações. Para obter mais informações sobre grupos e alocações, consulte Como funciona o IPAM.

AWS Management Console

Para liberar uma alocação de grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. No menu suspenso na parte superior do painel de conteúdo, escolha o escopo que você quer usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. No painel de conteúdo, escolha o grupo no qual a alocação está.
5. Escolha a guia Allocations (Alocações).
6. Selecione uma ou mais alocações. Você pode identificar as alocações pelo Resource type (Tipo de recurso):

   - custom (personalizado): uma alocação personalizada.
   - vpc: uma alocação de VPC.
   - ipam-pool: uma alocação de grupo do IPAM.
   - ec2-public-ipv4-pool: uma alocação de grupo IPv4 público.
   - sub-rede: uma alocação de sub-rede.

7. Escolha Actions (Ações) > Release custom allocation (Liberar alocação personalizada).
8. Escolha Deallocate CIDR (Desalocar CIDR).

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para liberar uma alocação de grupo:

1. Obter um ID de grupo do IPAM: describe-ipam-pools
2. Visualizar suas alocações atuais no grupo: get-ipam-pool-allocations.
3. Liberar uma alocação: release-ipam-pool-allocation
4. Visualizar as alocações atualizadas: get-ipam-pool-allocations.

Para adicionar uma nova alocação, consulte Alocar CIDRs de um grupo do IPAM. Para excluir o grupo após liberar alocações, primeiro é necessário Desprovisionar CIDRs de um grupo.

Compartilhar um grupo do IPAM usando o AWS RAM

Siga as etapas nesta seção para compartilhar um grupo do IPAM usando o AWS Resource Access Manager (RAM). Quando você compartilha um grupo do IPAM com o RAM, as “entidades principais” podem alocar CIDRs do grupo para recursos da AWS, como VPCs, de suas respectivas contas. Uma entidade principal é um conceito no RAM que significa qualquer conta da AWS, perfil do IAM ou unidade organizacional no AWS Organizations. Para obter mais informações, consulte Compartilhamento dos seus recursos da AWS no Guia do usuário do AWS RAM.

> **Note**
>
> - Só é possível compartilhar um grupo do IPAM com o AWS RAM se você integrou o IPAM ao AWS Organizations. Para obter mais informações, consulte Integrar o IPAM a contas em uma organização da AWS Organizations. Não será possível compartilhar um grupo do IPAM com o AWS RAM se você for um usuário do IPAM com uma única conta.
> - É necessário habilitar o compartilhamento de recursos com o AWS Organizations no AWS RAM. Para obter mais informações, consulte Habilitar compartilhamento de recursos com o AWS Organizations no Guia do usuário do AWS RAM.

- O compartilhamento do RAM só está disponível na região da AWS inicial do IPAM. Você deve criar o compartilhamento na região da AWS em que o IPAM está, não na região do grupo do IPAM.
- A conta que cria e exclui compartilhamentos de recursos do grupo do IPAM deve ter as seguintes permissões na política do IAM anexada ao perfil do IAM:
  - `ec2:PutResourcePolicy`
  - `ec2:DeleteResourcePolicy`
- Você pode adicionar vários grupos do IPAM a um compartilhamento do RAM.
- Embora seja possível compartilhar grupos do IPAM com qualquer conta da AWS externa a uma organização da AWS, o IPAM monitorará somente os endereços IP em contas externas à organização se o proprietário da conta tiver realizado o processo de compartilhamento da descoberta de recursos com o administrador delegado do IPAM, conforme descrito em Integrar o IPAM a contas fora de sua organização.

AWS Management Console

Para compartilhar um grupo do IPAM usando o RAM

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, o escopo privado padrão é selecionado. Se você não quiser usar o escopo privado padrão, no menu suspenso na parte superior do painel de conteúdo, escolha o escopo que deseja usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. No painel de conteúdo, escolha o grupo que deseja compartilhar e escolha Actions (Ações) > View details (Visualizar os detalhes).
5. Em Resource sharing (Compartilhamento de recursos), escolha Create resource share (Criar compartilhamento de recursos). Como resultado, o console do AWSRAM é exibido. Você criará o grupo compartilhado no AWS RAM.
6. Escolha Create a resource share (Criar um compartilhamento de recursos).
7. Adicione um Name (Nome) para o recurso compartilhado.
8. Em Select resource type (Selecionar tipo de recurso), selecione grupos do IPAM e escolha um ou mais grupos do IPAM.

9. Escolha Próximo.
10. Escolha uma das permissões para o compartilhamento de recursos:
    - AWSRAMDefaultPermissionsIpamPool: escolha esta permissão para permitir que as entidades principais visualizem os CIDRs e as alocações no grupo do IPAM compartilhado e aloque/libere CIDRs no grupo.
    - AWSRAMPermissionIpamPoolByoipCidrImport: escolha esta permissão para que as entidades possam importar CIDRs de BYOIP para o grupo do IPAM compartilhado. Você precisará dessa permissão somente se tiver CIDRs de BYOIP existentes e quiser importá-los para o IPAM e compartilhá-los com as entidades principais. Para obter informações adicionais sobre CIDRs de BYOIP para IPAM, consulte Tutorial: transferir um CIDR IPv4 BYOIP para o IPAM.
11. Escolha as entidades principais que têm permissão para acessar esse recurso. Se as entidades principais importarem CIDRs de BYOIP existentes para esse grupo do IPAM compartilhado, adicione a conta de proprietário CIDR de BYOIP como entidade principal.
12. Revise as opções de compartilhamento de recursos e as entidades principais com as quais você compartilhará e escolha Create (Criar).

Command line

O(s) comando(s) nessa seção são vinculados à Referência de comando AWS CLI. Lá você encontrará descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para compartilhar um grupo do IPAM usando o RAM:

1. Obter o ARN do IPAM: describe-ipam-pools
2. Criar o compartilhamento de recursos: create-resource-share
3. Visualizar o compartilhamento de recursos: get-resource-shares

Como resultado da criação do compartilhamento de recursos no RAM, outras entidades principais já podem alocar CIDRs para recursos usando o grupo do IPAM. Para obter informações sobre recursos de monitoramento criados por entidades principais, consulte Monitorar o uso do CIDR por recurso. Para obter mais informações sobre como criar uma VPC e alocar um CIDR de um grupo do IPAM compartilhado, consulte Crie uma VPC no Guia do usuário da Amazon VPC.

Trabalhar com descobertas de recursos

A descoberta de recursos é um componente do IPAM que permite ao IPAM gerenciar e monitorar recursos que pertencem à conta proprietária da descoberta de recursos. Isso permite que o IPAM mantenha um inventário atualizado do uso de endereços IP em suas workloads, facilitando o gerenciamento e o planejamento de endereços IP.

Uma descoberta de recursos é criada por padrão quando você cria um IPAM. Você também pode criar uma descoberta de recursos independentemente de um IPAM e integrá-la a um IPAM de propriedade de outra conta ou organização. Se o proprietário da descoberta de recursos for o administrador delegado de uma organização, o IPAM monitorará os recursos de todos os membros da organização.

> **Note**
>
> Criar, compartilhar e associar descobertas de recursos faz parte do processo de integração do IPAM com contas fora de suas organizações (consulte Integrar o IPAM a contas fora de sua organização). Se você não estiver criando e integrando um IPAM com contas fora da sua organização, não é necessário criar, compartilhar ou associar descobertas de recursos.

Observe que esta seção é um conjunto de procedimentos, todos relacionados ao trabalho com descobertas de recursos.

Conteúdo

- Criar uma descoberta de recursos para integração com outro IPAM
- Visualizar detalhes da descoberta de recursos
- Compartilhar uma descoberta de recursos com outra conta da AWS
- Associar uma descoberta de recursos a um IPAM
- Desassociar uma descoberta de recursos
- Excluir uma descoberta de recursos

Criar uma descoberta de recursos para integração com outro IPAM

Esta seção descreve como criar uma descoberta de recursos. Uma descoberta de recursos é criada por padrão quando você cria um IPAM. A cota padrão para descobertas de recursos por região é 1. Para obter mais informações sobre cotas do IPAM, consulte Cotas para o IPAM.

> **Note**
>
> Criar, compartilhar e associar descobertas de recursos faz parte do processo de integração do IPAM com contas fora de suas organizações (consulte Integrar o IPAM a contas fora de sua organização). Se você não estiver criando e integrando um IPAM com contas fora da sua organização, não é necessário criar, compartilhar ou associar descobertas de recursos.

Se você estiver integrando um IPAM com contas fora de suas organizações, essa é uma etapa obrigatória que deve ser executada pela conta de administrador da organização secundária. Para obter mais informações sobre os perfis envolvidos no processo, consulte Visão geral do processo.

AWS Management Console

Para criar uma descoberta de recursos

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Descobertas de recursos.
3. Escolha Criar descoberta de recursos.
4. Selecione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir que o IP Address Manager da Amazon VPC replique dados das contas de origem para a conta delegada do IPAM). Se você não selecionar essa opção, não será possível criar uma descoberta de recursos.
5. (Opcional) Adicione uma tag de Nome à descoberta de recursos. Uma tag é um rótulo atribuído a um recurso do AWS. Cada tag consiste em uma chave e um valor opcional. Você pode usar etiquetas para pesquisar e filtrar seus recursos ou monitorar seus custos na AWS.
6. (Opcional) Adicione uma descrição.
7. Em Regiões operacionais, selecione as regiões da AWS nas quais os recursos serão descobertos. A região atual será definida automaticamente como uma das regiões operacionais. Se você estiver criando a descoberta de recursos para poder compartilhá-la com um IPAM na região operacional `us-east-1`, não se esqueça de selecionar `us-east-1`

aqui. Se você esquecer uma região operacional, poderá retornar posteriormente e editar suas configurações de descoberta de recursos.

> **Note**
>
> Na maioria dos casos, a descoberta de recursos deve ter as mesmas regiões operacionais do IPAM, caso contrário você só obterá a descoberta de recursos nessa região.

8. (Opcional) Escolha quaisquer Tags adicionais para o grupo.
9. Escolha Criar.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

- Criar uma descoberta de recursos: create-ipam-resource-discovery

Visualizar detalhes da descoberta de recursos

A visualização dos detalhes de uma descoberta de recursos no AWS IPAM pode fornecer insights valiosos, como:

- Identificar os recursos específicos da AWS que foram importados e suas alocações de endereços IP associados.
- Monitoramento do status e do progresso do processo de descoberta de recursos.
- Solução de problemas ou discrepâncias entre o IPAM e os recursos descobertos.
- Análise da utilização e das tendências de endereços IP.

Essas informações podem ajudar a otimizar o gerenciamento de endereços IP e garantir o alinhamento entre o IPAM e suas implantações reais de recursos.

AWS Management Console

Para ver os detalhes da descoberta de recursos

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Descobertas de recursos.
3. Escolha uma descoberta de recursos.
4. Em Detalhes da descoberta de recursos, visualize os detalhes relacionados à descoberta de recursos, como Padrão, que indica se a descoberta de recursos é o padrão. A descoberta de recursos padrão é a descoberta de recursos criada automaticamente quando você cria um IPAM.
5. Nas guias, veja os detalhes de uma descoberta de recursos:

   - Recursos descobertos: recursos monitorados por meio de uma descoberta de recursos. O IPAM monitora CIDRs dos seguintes tipos de recursos: VPCs, grupos de IPv4 públicos, sub-redes VPC e endereços IP elásticos.
     - Nome (ID do recurso): ID da descoberta de recursos.
     - IPs alocatos: o percentual do espaço de endereço IP em uso. Para converter o decimal em um percentual, multiplique o decimal por 100. Observe o seguinte:
       - Para recursos que sejam VPCs, esse valor é o percentual de espaço de endereços IP na VPC ocupado por CIDRs de sub-rede.
       - Para recursos que são sub-redes, se a sub-rede tiver um CIDR IPv4 provisionado para ela, esse valor será a porcentagem do espaço de endereços IPv4 da sub-rede que está em uso. Se a sub-rede tiver um CIDR IPv6 provisionado, a porcentagem de espaço de endereços IPv6 em uso não será representada. A porcentagem de espaço de endereços IPv6 em uso não pode ser calculada no momento.
       - Para recursos que sejam grupos de IPv4 públicos, trata-se do percentual de espaço de endereço IP no grupo que foi alocado para endereços IP elásticos (EIPs).
     - CIDR: CIDR do recurso.
     - Região: a região do recurso.
     - ID do proprietário: o ID do proprietário do recurso.
     - Horário de amostragem: o último horário bem-sucedido de descoberta de recursos.
   - Contas descobertas: as contas da AWS que estão sendo monitoradas por meio de uma descoberta de recursos. Se você tiver integrado o IPAM com o AWS Organizations, todas as contas na organização serão contas descobertas.

        - ID da conta: o ID da conta.
        - Região: a região da AWS da qual as informações da conta são retornadas.
        - Horário da última tentativa de descoberta: o horário da última tentativa de descoberta de recursos.
        - Horário da última descoberta bem-sucedida: a última vez bem-sucedida na descoberta de recursos.
        - Status: motivo da falha na descoberta de recursos.
    - Regiões operacionais: as regiões operacionais para a descoberta de recursos.
    - Compartilhamento de recursos: se a descoberta de recursos tiver sido compartilhada, o ARN do compartilhamento de recursos será listado.
        - ARN de compartilhamento de recursos: o ARN do compartilhamento de recursos.
        - Status: o status atual do compartilhamento de recursos. Os valores possíveis são:
            - Ativo: o compartilhamento de recursos está ativo e disponível para uso.
            - Excluído: o compartilhamento de recursos foi excluído e não está mais disponível para uso.
            - Pendente: um convite para aceitar o compartilhamento de recurso está aguardando uma resposta.
        - Criado em: quando o compartilhamento de recursos foi criado.
    - Tags: uma tag é um rótulo que você atribui a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional. Você pode usar etiquetas para pesquisar e filtrar seus recursos ou monitorar seus custos na AWS.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

- Visualizar os detalhes da descoberta de recursos: describe-ipam-resource-discoveries

Compartilhar uma descoberta de recursos com outra conta da AWS

Siga as etapas nesta seção para compartilhar uma descoberta de recursos usando o AWS Resource Access Manager. Para obter mais informações sobre o AWS RAM, consulte Compartilhar seus recursos da AWS no Guia do usuário do AWS RAM.

> **Note**
>
> Criar, compartilhar e associar descobertas de recursos faz parte do processo de integração do IPAM com contas fora de suas organizações (consulte Integrar o IPAM a contas fora de sua organização). Se você não estiver criando e integrando um IPAM com contas fora da sua organização, não é necessário criar, compartilhar ou associar descobertas de recursos.

Quando você cria um IPAM que monitora contas fora da sua organização, a conta de administrador da organização secundária compartilha a descoberta de recursos com a conta do IPAM da organização primária usando o AWS RAM. Primeiramente, você deve compartilhar uma descoberta de recursos com a conta do IPAM da organização primária antes que a conta do IPAM da organização primária possa associar a descoberta de recursos ao IPAM. Para obter mais informações sobre os perfis envolvidos no processo, consulte Visão geral do processo.

> **Note**
>
> - Ao criar um compartilhamento de recursos usando o AWS RAM para compartilhar uma descoberta de recursos, você deve criar o compartilhamento de recursos na região de origem da organização primária do IPAM.
> - A conta que cria e exclui um compartilhamento de recursos para uma descoberta de recursos deve ter as seguintes permissões em sua política do IAM:
>   - ec2:PutResourcePolicy
>   - ec2:DeleteResourcePolicy
> - Se você compartilhar uma descoberta de recursos com outra conta, essa conta poderá ver quaisquer exclusões de UO aplicáveis a ela, as quais contêm informações como ID da organização, ID da raiz e IDs das unidades organizacionais da organização do proprietário da descoberta de recursos.

Se você estiver integrando um IPAM com contas fora de suas organizações, essa é uma etapa obrigatória que deve ser executada pela conta de administrador da organização secundária.

AWS Management Console

Para compartilhar uma descoberta de recursos

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Descobertas de recursos.
3. Escolha a guia Compartilhamento de recursos.
4. Escolha Criar compartilhamento de recursos. O console do AWS RAM é aberto. Você criará o compartilhamento de recursos nele.
5. No console do AWS RAM, selecione Configurações.
6. Escolha Habilitar compartilhamento com AWS Organizations e, em seguida, escolha Salvar configurações.
7. Escolha Create a resource share (Criar um compartilhamento de recursos).
8. Adicione um Name (Nome) para o recurso compartilhado.
9. Em Selecionar tipo de recurso, selecione Descoberta de recursos IPAM e escolha a descoberta do recursos.
10. Escolha Próximo.
11. Em Associar permissões, você pode ver a permissão padrão que será habilitada para entidades principais que tenham acesso a esse compartilhamento de recursos:
    - AWSRAMPermissionIpamResourceDiscovery
    - Ações habilitadas por essa permissão:
      - ec2:AssociateIpamResourceDiscovery
      - ec2:GetIpamDiscoveredAccounts
      - EC2: Obtenha endereços públicos descobertos pelo IPAM
      - ec2:GetIpamDiscoveredResourceCidrs
12. Especifique as entidades principais que têm permissão para acessar o recurso compartilhado. Em Entidades principais, escolha a conta do IPAM da organização primária e escolha Adicionar.
13. Escolha Próximo.
14. Revise as opções de compartilhamento de recursos e as entidades principais com as quais você compartilhará. Em seguida, escolha Criar compartilhamento de recursos.
15. Depois que uma descoberta de recursos for compartilhada, ela deve ser aceita pela conta IPAM da organização primária e, em seguida, associada a um IPAM pela conta do IPAM da

organização primária. Para obter mais informações, consulte Associar uma descoberta de recursos a um IPAM.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

1. Criar o compartilhamento de recursos: create-resource-share
2. Visualizar o compartilhamento de recursos: get-resource-shares

Associar uma descoberta de recursos a um IPAM

Esta seção descreve como associar uma descoberta de recursos a um IPAM. Quando você associa uma descoberta de recursos a um IPAM, o IPAM monitora todos os CIDRs e contas de recursos descobertos na descoberta de recursos. Quando você cria um IPAM, uma descoberta de recursos padrão é criada para seu IPAM e associada automaticamente ao seu IPAM.

A cota padrão para associações de descoberta de recursos é de 5. Para obter mais informações (incluindo sobre como ajustar essa cota), consulte Cotas para o IPAM.

> **Note**
>
> Criar, compartilhar e associar descobertas de recursos faz parte do processo de integração do IPAM com contas fora de suas organizações (consulte Integrar o IPAM a contas fora de sua organização). Se você não estiver criando e integrando um IPAM com contas fora da sua organização, não é necessário criar, compartilhar ou associar descobertas de recursos.

Se você estiver integrando um IPAM com contas fora de suas organizações, essa é uma etapa obrigatória que deve ser executada pela conta do IPAM da organização primária. Para obter mais informações sobre os perfis envolvidos no processo, consulte Visão geral do processo.

AWS Management Console

Para associar uma descoberta de recursos

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.

2. No painel de navegação, selecione IPAMs.
3. Selecione Descobertas associadas e escolha Associar descobertas de recursos.
4. Em Descobertas de recursos do IPAM, escolha uma descoberta de recursos que tenha sido compartilhada com você pela conta de administrador da organização secundária.
5. Selecione Associar.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

- Associar uma descoberta de recursos: associate-ipam-resource-discovery

Desassociar uma descoberta de recursos

Esta seção descreve como desassociar uma descoberta de recursos de um IPAM. Quando você desassocia uma descoberta de recursos de um IPAM, o IPAM deixa de monitorar todos os CIDRs e contas de recursos descobertos na descoberta de recursos.

> **Note**
>
> Você não pode desassociar uma associação padrão de descoberta de recursos. Uma associação padrão de descoberta de recursos é aquela criada automaticamente quando você cria um IPAM. No entanto, a associação padrão de descoberta de recursos será excluída se você excluir o IPAM.

Essa etapa deve ser executada pela conta do IPAM da organização primária. Para obter mais informações sobre os perfis envolvidos no processo, consulte Visão geral do processo.

AWS Management Console

Para desassociar uma descoberta de recursos

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione IPAMs.
3. Selecione Descobertas associadas e escolha Desassociar descobertas de recursos.

4. Em Descobertas de recursos do IPAM, escolha uma descoberta de recursos que tenha sido compartilhada com você pela conta de administrador da organização secundária.
5. Escolha Desassociar.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

- Para desassociar uma descoberta de recursos: disassociate-ipam-resource-discovery

Excluir uma descoberta de recursos

Esta seção descreve como excluir uma descoberta de recursos.

> **Note**
>
> Você não pode excluir uma descoberta de recursos padrão. Uma descoberta de recursos padrão é aquela criada automaticamente quando você cria um IPAM. No entanto, a descoberta de recursos padrão será excluída se você excluir o IPAM.

Esta etapa deve ser executada pela conta de administrador da organização secundária. Para obter mais informações sobre os perfis envolvidos no processo, consulte Visão geral do processo.

AWS Management Console

Para excluir uma descoberta de recursos

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Descobertas de recursos.
3. Selecione uma descoberta de recursos e escolha Ações > Excluir descoberta de recursos.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

- Para excluir uma descoberta de recursos: delete-ipam-resource-discovery

Rastrear uso de endereços IP no IPAM

O Gerenciador de endereços IP da Amazon VPC oferece recursos de rastreamento de uso de endereços IP que podem beneficiar qualquer pessoa que gerencie ambientes de rede complexos. O IPAM fornece visibilidade das tendências de alocação, utilização e consumo de endereços IP na AWS. Isso ajuda você a identificar endereços IP não utilizados ou usados de forma ineficiente, otimizando o espaço de endereços e evitando o possível esgotamento de endereços IP.

O IPAM rastreia o uso de endereços IP nos níveis do CIDR, escopo e IPAM, fornecendo relatórios e analytics detalhados. Isso é importante para implantações em grande escala, configurações de várias contas e requisitos de rede em desenvolvimento.

Ao aproveitar o rastreamento de uso do IPAM, você pode tomar decisões informadas, melhorar o gerenciamento de endereços IP e garantir a utilização eficiente dos recursos de IP.

> **Note**
>
> As tarefas descritas nesta seção são opcionais. Se você quiser concluir as tarefas nesta seção e delegou uma conta do IPAM, as tarefas devem ser concluídas pela conta do IPAM.

Conteúdo

- Monitorar o uso do CIDR com o painel do IPAM
- Monitorar o uso do CIDR por recurso
- Monitorar o IPAM com o Amazon CloudWatch
- Ver histórico de endereços IP
- Visualizar insights de IPs públicos

Monitorar o uso do CIDR com o painel do IPAM

O painel do IPAM no Gerenciador de endereços IP da Amazon VPC permite que você monitore o uso do CIDR em vários cenários importantes:

- Identifique o espaço de endereços IP não utilizado ou subutilizado: o painel fornece visibilidade da utilização do CIDR, permitindo que você identifique CIDRs com capacidade disponível que pode ser recuperada ou realocada.

- Otimize o gerenciamento de endereços IP: ao rastrear de perto o uso do CIDR, você pode tomar decisões informadas sobre expansão, contratação ou reatribuição de blocos de endereços IP para atender às mudanças nos requisitos de negócios e infraestrutura.
- Evite o esgotamento de endereços IP: o monitoramento do uso do CIDR ajuda a prever quando talvez seja necessário adquirir espaço adicional de endereços IP, permitindo que você planeje e evite interrupções no serviço de forma proativa devido ao esgotamento de endereços IP.
- Garanta a conformidade e governança: o painel do IPAM pode ajudar a demonstrar padrões de uso de endereços IP para atender aos requisitos regulamentares ou às políticas internas de gerenciamento de endereços IP.
- Solucionar problemas de rede: dados detalhados de uso do CIDR podem ajudar a identificar as causas raiz de problemas de conectividade de rede ou conflitos de recursos.

Ao monitorar de perto o uso do CIDR por meio do painel do IPAM, você pode melhorar a eficiência, a resiliência e a conformidade do gerenciamento de endereços IP na AWS.

AWS Management Console

Para monitorar o uso do CIDR com o painel do IPAM

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Painel.
3. Por padrão, quando você visualiza o painel, o escopo privado padrão é selecionado. Se você não quiser usar o escopo privado padrão, no menu suspenso na parte superior do painel de conteúdo, escolha o escopo que deseja usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. O painel apresenta uma visão geral de seus grupos de IPAM e CIDRs dentro de um escopo. Você pode adicionar, remover, redimensionar e mover widgets para personalizar o painel.

    - Scope (Escopo): os detalhes desse escopo. Um escopo é o contêiner de nível mais alto dentro do IPAM. Um IPAM contém dois escopos padrão, um privado e um público. Cada escopo representa o espaço IP de uma única rede. Você pode ter vários escopos privados, mas só pode ter um escopo público.
        - Scope ID (ID do escopo): os detalhes desse escopo.
        - Scope type (Tipo de escopo): o tipo de escopo.
        - IPAM ID (ID do IPAM): o ID do IPAM no qual o escopo está.

    - Grupos do IPAM neste escopo: o ID do IPAM onde está o escopo.
    - Exibir recursos de rede neste escopo: leva você à seção Recursos do console do IPAM.
    - Pesquise o histórico de um endereço IP neste escopo: leva você à seção Pesquisar histórico de IP do console do IPAM.
- Tipos de CIDR de recursos: os tipos de CIDRs de recursos no escopo.
    - Sub-rede: o número de CIDRs para sub-redes.
    - VPC: o número de CIDRs para VPCs.
    - EIPs: o número de CIDRs para endereços IP elásticos.
    - Grupos de IPv4 públicos: o número de CIDRs para grupos de IPv4 públicos.
- Estado de gerenciamento: o estado de gerenciamento dos CIDRs.
    - Unmanaged CIDRs (CIDRs não gerenciados): o número de CIDRs de recursos para recursos não gerenciados neste escopo.
    - Ignored CIDRs (CIDRs ignorados): o número de CIDRs de recursos que você escolheu para ficarem isentos de monitoramento com IPAM no escopo. Os recursos ignorados não são avaliados pelo IPAM quanto à sobreposição ou conformidade dentro de um escopo. Quando um recurso é escolhido para ser ignorado, qualquer espaço alocado a ele de um grupo do IPAM é retornado ao grupo e o recurso não será importado novamente por meio de importação automática (se a regra de alocação de importação automática estiver definida no grupo).
    - Managed CIDRs (CIDRs gerenciados): o número de CIDRs de recursos para recursos gerenciáveis (VPCs ou grupos IPv4 públicos) alocados de um grupo do IPAM no escopo.
- CIDRs de recursos sobrepostos: o número de CIDRs sobrepostos e não sobrepostos. CIDRs sobrepostos podem levar a roteamento incorreto em suas VPCs.
    - Overlapping CIDRs (CIDRs sobrepostos): o número de CIDRs que se sobrepõem em grupos do IPAM nesse escopo. CIDRs sobrepostos podem levar a roteamento incorreto em suas VPCs.
    - CIDRs não sobrepostos: o número de CIDRs de recursos que não se sobrepõem em grupos de IPAM neste escopo.
- CIDRs de recursos compatíveis: o número de CIDRs de recursos compatíveis.
    - Compliant CIDRs (CIDRs compatíveis): o número de CIDRs de recursos que estão em conformidade com as regras de alocação para grupos do IPAM no escopo.
    - Noncompliant CIDRs (CIDRs incompatíveis): o número de CIDRs de recursos que não estão em conformidade com as regras de alocação para grupos do IPAM no escopo.

- Status de sobreposição: o número de CIDRs que se sobrepõem ao longo do tempo.
  - OverlappingResourceCidrs: o número de CIDRs que se sobrepõem em grupos do IPAM neste escopo. CIDRs sobrepostos podem levar a roteamento incorreto em suas VPCs.
- Status de conformidade: o número de CIDRs que seguem as regras de alocação em comparação com os que não seguem para grupos do IPAM no escopo ao longo do tempo.
  - CompliantResourceCidrs: o número de CIDRs de recursos que estão em conformidade com as regras de alocação.
  - NoncompliantResourceCidrs: o número de CIDRs de recursos que não estão em conformidade com as regras de alocação.
- Utilização da VPC: VPCs (IPv4 e IPv6) com a maior ou menor utilização de IPs. É possível usar essas informações para configurar alarmes do Amazon CloudWatch para receber notificações se um limite de utilização de IP for violado. Para ter mais informações, consulte Métricas de utilização de recursos do IPAM.
- Utilização de sub-redes: sub-redes (somente IPv4) com a maior ou menor utilização de IPs. É possível usar essas informações para decidir se você deseja manter ou excluir recursos subutilizados. Para ter mais informações, consulte Métricas de utilização de recursos do IPAM.
- VPCs com os IPs mais altos alocados: os VPCs que têm a maior porcentagem de espaço de endereço IP alocado para sub-redes. Isso é útil para mostrar se você precisa provisionar espaço adicional de endereço IP para as VPCs.
- Sub-redes com IPs mais altos alocados: as sub-redes que têm a maior porcentagem de espaço de endereço IP alocado aos recursos. Isso é útil para mostrar se você precisa provisionar espaço adicional de endereço IP para as sub-redes.
- Atribuição de grupos: a porcentagem do espaço IP atribuída a recursos e alocações manuais no escopo ao longo do tempo.
- Alocação de grupos: a porcentagem do espaço IP de um grupo que foi alocada para outros grupos no escopo ao longo do tempo.

Command line

As informações exibidas no painel vêm de métricas armazenadas no Amazon CloudWatch. Para obter mais informações sobre as métricas armazenadas no Amazon CloudWatch, consulte Monitorar o IPAM com o Amazon CloudWatch. Use as opções do Amazon CloudWatch na Referência da AWS CLI para exibir métricas de alocações em seus grupos e escopos do IPAM.

Se você concluir que o CIDR provisionado para um grupo está quase totalmente alocado, talvez seja necessário provisionar CIDRs adicionais. Para ter mais informações, consulte Provisionar CIDRs para um grupo.

Monitorar o uso do CIDR por recurso

A visualização de recursos no Gerenciador de endereços IP da Amazon VPC fornece uma visão geral centralizada da utilização de endereços IP em seus recursos da AWS. Isso permite que você identifique rapidamente quais recursos estão consumindo endereços IP, rastreie as tendências de alocação de endereços e otimize o gerenciamento de endereços IP para se alinhar às suas crescentes necessidades comerciais e de infraestrutura.

No IPAM, um recurso é uma entidade de serviço da AWS que recebe um endereço IP ou bloco CIDR. O IPAM gerencia alguns recursos, mas apenas monitora outros recursos, por isso é importante entender a diferença entre os dois:

- Recurso gerenciado: um recurso gerenciado tem um CIDR alocado de um grupo do IPAM. O IPAM monitora o CIDR quanto a possíveis sobreposições de endereço IP com outros CIDRs no grupo e monitora a conformidade do CIDR com as regras de alocação de um grupo. O IPAM oferece suporte aos seguintes tipos de recursos:
  - Endereços IP elásticos
  - Grupos IPv4 públicos

    > **Note**
    >
    > Os grupos IPv4 públicos e os grupos do IPAM são gerenciados por recursos distintos na AWS. O grupos IPv4 públicos são recursos de conta única que permitem converter seus CIDRs de propriedade pública em endereços IP elásticos. Os grupos do IPAM podem ser usados para alocar seu espaço público para grupos do IPv4 públicos.

  - VPCs
- Recurso monitorado: se um recurso é monitorado pelo IPAM, ele foi detectado pelo IPAM e você poderá visualizar detalhes sobre o CIDR do recurso ao usar `get-ipam-resource-cidrs` com a AWS CLI ou ao visualizar Resources (Recursos) no painel de navegação. O IPAM oferece suporte ao monitoramento dos seguintes recursos:
  - Endereços IP elásticos
  - Grupos IPv4 públicos

- VPCs
- Sub-redes VPC

AWS Management Console

Para monitorar o uso do CIDR por recurso

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Resources (Recursos).
3. No menu suspenso de IP na parte superior do painel de conteúdo, escolha o protocolo de endereço IP que você quer usar: IPv4 ou IPv6.
4. No menu suspenso de escopo na parte superior do painel de conteúdo, escolha o escopo que você quer usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
5. Use o mapa do CIDR de recursos para visualizar o espaço de endereço IP disponível, alocado e sobreposto em um escopo:

   - Disponível: um intervalo de endereços IP está disponível para alocação.
   - Compatível e sem sobreposição: um intervalo de endereços IP é alocado para um recurso gerenciado pelo IPAM.
   - Ocupado: um intervalo de endereços IP é alocado para um recurso.
   - Sobreposição: um intervalo de endereços IP foi alocado para vários recursos e está sobreposto.
   - Não compatível: um intervalo de endereços IP não é compatível. Há um recurso usando o intervalo de endereços IP que não está em conformidade com as regras de alocação configuradas para o grupo.

   No mapa do CIDR, escolha um bloco de endereços IP na parte inferior do mapa para visualizar os recursos em blocos de CIDR menores. Escolha um bloco de endereços IP na parte superior do mapa para visualizar os recursos em blocos de CIDR maiores.
6. Na tabela, você pode ver os seguintes detalhes sobre os recursos no escopo:

   - Nome (ID do recurso): o nome e o ID do recurso.
   - CIDR: o CIDR associado ao recurso.
   - Management state (Estado de gerenciamento): o estado do recurso.

- Managed (Gerenciado): o recurso tem um CIDR alocado de um grupo do IPAM e está sendo monitorado pelo IPAM quanto à possível sobreposição e conformidade do CIDR com regras de alocação de grupos.
- Não gerenciado: o recurso não tem um CIDR alocado de um grupo do IPAM e não está sendo monitorado pelo IPAM quanto à possível conformidade do CIDR com regras de alocação de grupos. O CIDR é monitorado quanto à sobreposição.
- Ignored (Ignorado): o recurso foi escolhido para ficar isento do monitoramento. Os recursos ignorados não são avaliados quanto à sobreposição ou conformidade com as regras de alocação. Quando um recurso for escolhido para ser ignorado, qualquer espaço alocado a ele de um grupo do IPAM retornará ao grupo e o recurso não será importado novamente por meio da importação automática (se a regra de alocação de importação automática estiver definida no grupo).
- -: esse recurso não é um dos tipos de recursos que o IPAM pode gerenciar.

- Compliance status (Status de conformidade): o status de conformidade do CIDR.
  - Compliant (Em conformidade): um recurso gerenciado está em conformidade com as regras de alocação do grupo do IPAM.
  - Noncompliant (Em não conformidade): o CIDR de recurso não está em conformidade com uma ou mais das regras de alocação do grupo do IPAM.

    Example

    Se uma VPC tiver um CIDR que não atenda aos parâmetros de comprimento da máscara de rede do grupo do IPAM ou se o recurso não estiver na mesma região da AWS que o grupo do IPAM, ele será sinalizado como não compatível.
  - Não gerenciado: o recurso não tem um CIDR alocado de um grupo do IPAM e não está sendo monitorado pelo IPAM quanto à possível conformidade do CIDR com regras de alocação de grupos. O CIDR é monitorado quanto à sobreposição.
  - Ignored (Ignorado): o recurso foi escolhido para ficar isento do monitoramento. Os recursos ignorados não são avaliados quanto à sobreposição ou conformidade com as regras de alocação. Quando um recurso for escolhido para ser ignorado, qualquer espaço alocado a ele de um grupo do IPAM retornará ao grupo e o recurso não será importado novamente por meio da importação automática (se a regra de alocação de importação automática estiver definida no grupo).
  - -: esse recurso não é um dos tipos de recursos que o IPAM pode gerenciar.
- Overlap status (Status de sobreposição): o status de sobreposição do CIDR.

- Nonoverlapping (Sem sobreposição): o recurso CIDR não se sobrepõe a outro CIDR no mesmo escopo.
- Overlapping (Com sobreposição): o recurso CIDR se sobrepõe a outro CIDR no mesmo escopo. Observe que, se um CIDR de recurso estiver se sobrepondo, ele poderá estar sobreposto a uma alocação manual.
- Ignored (Ignorado): o recurso foi escolhido para ficar isento do monitoramento. Os recursos ignorados não são avaliados pelo IPAM quanto à sobreposição ou conformidade com a regra de alocação. Quando um recurso for escolhido para ser ignorado, qualquer espaço alocado a ele de um grupo do IPAM retornará ao grupo e o recurso não será importado novamente por meio da importação automática (se a regra de alocação de importação automática estiver definida no grupo).
- -: esse recurso não é um dos tipos de recursos que o IPAM pode gerenciar.

- IPs alocados: para recursos que são VPCs, esse valor é a porcentagem do espaço de endereço IP na VPC que é ocupado por CIDRs de sub-rede. Para recursos que são sub-redes, se a sub-rede tiver um CIDR IPv4 provisionado para ela, esse valor será a porcentagem do espaço de endereços IPv4 da sub-rede que está em uso. Se a sub-rede tiver um CIDR IPv6 provisionado, a porcentagem de espaço de endereços IPv6 em uso não será representada. A porcentagem de espaço de endereços IPv6 em uso não pode ser calculada no momento. Para recursos que sejam grupos de IPv4 públicos, trata-se do percentual de espaço de endereço IP no grupo que foi alocado para endereços IP elásticos (EIPs).
- Region (Região): a região da AWS do recurso.
- Owner ID (ID de proprietário): o ID da conta da AWS da pessoa que criou esse recurso.
- Tipo de recurso: se o recurso é uma VPC, sub-rede, endereço IP elástico ou grupo IPv4 público.
- Pool ID (ID do grupo): o ID do grupo do IPAM no qual o recurso está.

7. Use Filtrar recursos para filtrar a tabela de recursos por propriedade da coluna, como ID da VPC ou status de conformidade.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Use os seguintes comandos da AWS CLI para monitorar o uso do CIDR por recurso:

1. Obter o ID do escopo: describe-ipam-scopes
2. Solicitar informações sobre recursos: get-ipam-resource-cidrs

Monitorar o IPAM com o Amazon CloudWatch

O IPAM armazena automaticamente as métricas relacionadas ao uso de endereços IP (como o espaço de endereços IP disponível nos grupos do IPAM e o número de CIDRs de recursos conformes com as regras de alocação) e utilização de recursos no namespace do Amazon CloudWatch `AWS/IPAM` na região inicial do IPAM.

A integração do IPAM com o CloudWatch aprimora a capacidade de monitorar, analisar e otimizar o gerenciamento de endereços IP na AWS.

Os casos de uso incluem:

- Rastreamento de tendências de utilização de endereços IP: o CloudWatch pode monitorar o uso do grupo CIDR, a alocação de escopo e outras métricas do IPAM, ajudando você a identificar proativamente possíveis riscos de esgotamento de endereços IP.
- Configuração de alertas baseados na utilização: você pode configurar os alarmes do CloudWatch para notificar quando a utilização do CIDR atingir limites predeterminados, permitindo intervenção e otimização oportunas.
- Monitoramento de eventos do IPAM: o CloudWatch pode capturar e analisar eventos relacionados ao IPAM, como alocações de CIDR, desalocações e modificações de escopo, fornecendo visibilidade das atividades de gerenciamento de endereços IP.
- Geração de painéis personalizados: ao combinar dados do IPAM com outras métricas da AWS, você pode criar painéis abrangentes para visualizar e analisar seu cenário de endereços IP junto com indicadores de infraestrutura e performance relacionados.

Conteúdo

- Gerenciar alarmes a partir da console do IPAM
- Métricas do IPAM
- Métricas de utilização de recursos do IPAM

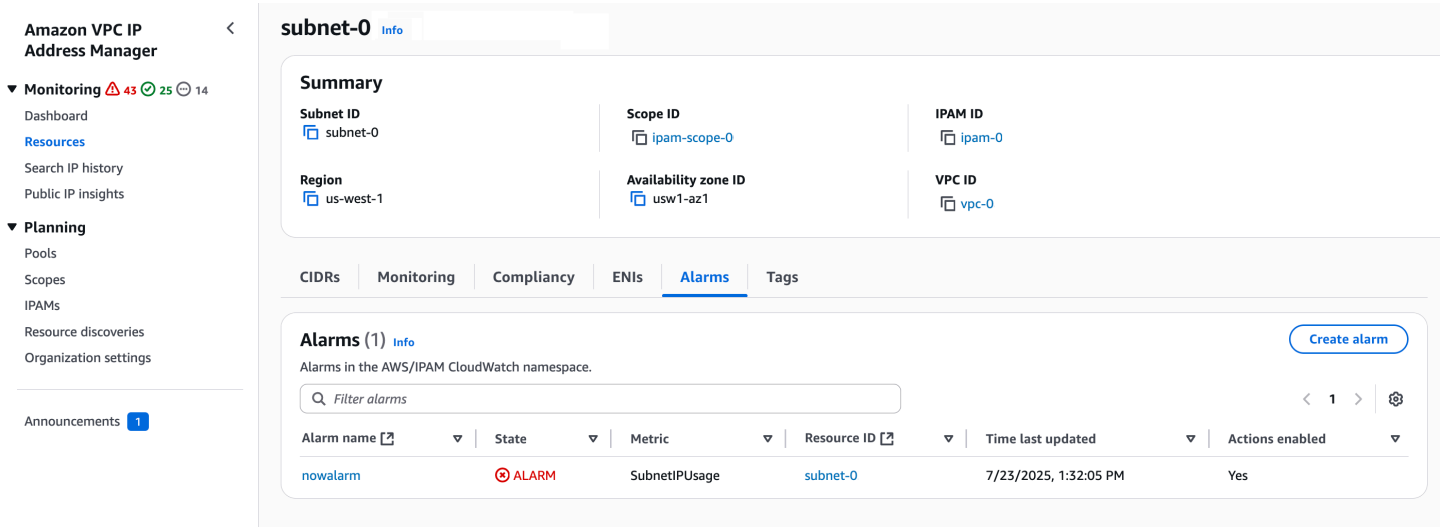
Gerenciar alarmes a partir da console do IPAM

É possível criar e gerenciar alarmes do Amazon CloudWatch diretamente do console do IPAM. Os alarmes para Métricas do IPAM ou Métricas de utilização de recursos do IPAM que estão em um estado INSUFFICIENT_DATA ou ALARM serão exibidos como barras de aviso na parte superior do console e como indicadores visuais na navegação à esquerda, ao lado de Monitoramento.

Para gerenciar alarmes para recursos específicos, selecione Recursos e, em seguida, selecione uma VPC, sub-rede ou grupo. Quando a página de detalhes do recurso abrir, escolha a guia Alarmes.

A guia Alarmes exibe todos os alarmes do CloudWatch que estão associados ao recurso selecionado. Nesaa guia, é possível realizar a visualização de detalhes do alarme, monitorar os estados atuais e acessar as opções de configuração do alarme. A guia mostra os alarmes de namespace do `AWS/IPAM` que são relevantes para o recurso que está sendo visualizado.

A captura de tela a seguir mostra a interface de gerenciamento de alarmes no console do IPAM:



A guia Alarmes dá um resumo detalhado de alarmes do CloudWatch no namespace `AWS/IPAM` do Amazon CloudWatch na região de origem do IPAM:

- Nome do alarme: nome definido pelo usuário para o alarme do CloudWatch.
- Estado: estado atual do alarme do CloudWatch:
  - ALARM: a métrica está fora do limite definido.
  - OK: a métrica está dentro do limite definido.
  - INSUFFICIENT_DATA: dados insuficientes para determinar o estado do alarme.
- Métrica: a métrica específica do CloudWatch que está sendo monitorada pelo alarme.

- ID do recurso: o identificador exclusivo do recurso AWS que está sendo monitorado pelo alarme.
- Hora da última atualização: data e hora em que o estado do alarme foi modificado ou avaliado pela última vez.
- Ações habilitadas: indica se ações do CloudWatch estão ou não habilitadas para o alarme:
  - Sim: o alarme pode disparar ações configuradas quando determinadas condições são atendidas.
  - Não: o alarme está monitorando, mas não está executando ações.

Além disso, se você estiver visualizando gráficos de utilização na guia Monitoramento para uma VPC, sub-rede ou pool, poderá optar por criar um alarme para a utilização de recursos. Em seguida, é feito o redirecionamento ao console do CloudWatch, com detalhes de recursos e métricas pré-preenchidos. A partir daí, é possível configurar um limite de alarme para, por exemplo, receber notificações quando a utilização atingir uma determinada porcentagem.

Métricas do IPAM

O IPAM publica dados sobre os pools e os escopos do IPAM no Amazon CloudWatch. Você pode usar essas métricas para criar alarmes para grupos do IPAM para receber notificações se os grupos de endereços estão se aproximando da exaustão ou se os recursos não estiverem em conformidade com as regras de alocação definidas em um grupo. A criação de alarmes e a configuração de notificações com o Amazon CloudWatch está fora do escopo desta seção. Para obter mais informações, consulte Uso de alarmes do Amazon CloudWatch no Manual do usuário do Amazon CloudWatch.

As métricas e dimensões que o IPAM envia para o Amazon CloudWatch estão listadas abaixo.

Métricas do IPAM

O namespace `AWS/IPAM` inclui as métricas do IPAM a seguir.

Nome da métrica	Descrição
TotalActiveIpCount	A contagem total de IPs ativos representa o número de endereços IP ativos no seu IPAM pelos quais seria cobrada uma taxa se você migrasse do nível gratuito para o nível avançado. Um endereço IP ativo é definido como um endereço IP ou

Nome da métrica	Descrição
	um prefixo associado a uma interface de rede elástica (ENI) anexada a um recurso, como uma instância do EC2. • Essa métrica só está disponível para os clientes do nível gratuito. • Se seu IPAM estiver integrado ao AWS Organizations, a contagem de IPs ativos cobrirá todas as contas da organizaç ão. • Você não pode ver um detalhamento do número de endereços IP ativos por tipo de IP (público/privado) ou classe (IPv4/IPv6). • O IPAM só conta os IPs de ENIs pertencentes a contas monitoradas. O número pode não ser exato para sub-redes compartilhadas. Os endereços IP serão excluídos se o proprietário da sub-rede ou da ENI não for coberto pelo IPAM.

Métricas de grupo do IPAM

O namespace da `AWS/IPAM` inclui as métricas de grupo a seguir para o IPAM.

Nome da métrica	Descrição
CompliantResourceCidrs	O número de CIDRs de recursos gerenciados que seguem as regras de alocação de grupo do IPAM. Para obter mais informações sobre etiquetas de alocação de custos, consulte Criar um grupo de IPv4 de nível superior.
NoncompliantResourceCidrs	O número de CIDRs de recursos gerenciados que não seguem as regras de alocação de grupo do IPAM. Para obter mais informações sobre etiquetas de alocação de custos, consulte Criar um grupo de IPv4 de nível superior.
PercentAllocated	A porcentagem de espaço IP de um grupo que foi alocada a outros grupos.

Nome da métrica	Descrição
PercentAssigned	A porcentagem de espaço IP de um grupo que foi alocada a recursos, incluindo alocações manuais.
PercentAvailable	A porcentagem de espaço IP de um grupo que foi alocada a outros grupos ou recursos.

Métricas de escopo do IPAM

O namespace da `AWS/IPAM` inclui as métricas de escopo a seguir para o IPAM.

Nome da métrica	Descrição
CompliantResourceCidrs	O número de CIDRs de recursos que seguem as regras de alocação para grupos do IPAM no escopo.
ManagedResourceCidrs	O número de CIDRs de recursos para recursos gerenciáveis (VPCs ou grupos IPv4 públicos) alocados de um grupo do IPAM no escopo.
NoncompliantResourceCidrs	O número de CIDRs de recursos que não seguem as regras de alocação para grupos do IPAM no escopo.
OverlappingResourceCidrs	O número de CIDRs de recursos que se sobrepõem no escopo.
UnmanagedResourceCidrs	O número de CIDRs de recursos no escopo que atualment e estão associados a recursos gerenciáveis, mas não são gerenciados pelo IPAM.

Métricas de IP público do IPAM

O namespace da `AWS/IPAM` inclui as métricas de IP público a seguir para o IPAM.

Nome da métrica	Descrição
AmazonOwnedContigIPs	O número de endereços IP nos CIDRs que são provisionados para grupos IPv4 públicos contíguos fornecidos pela Amazon, de propriedade do IPAM.
AllocatedAmazonOwnedContigIPs	O número de endereços IP que foram alocados de um bloco CIDR do grupo IPv4 público contíguo fornecido pela Amazon.
UnallocatedAmazonOwnedContigIPs	O número de endereços IP no bloco CIDR do grupo IPv4 público contíguo fornecido pela Amazon, de propriedade do IPAM.
AssociatedAmazonOwnedContigIPs	O número de endereços IP elásticos que foram alocados de um bloco CIDR do grupo IPv4 público contíguo fornecido pela Amazon que estão associados a uma interface de rede elástica.
UnassociatedAmazonOwnedContigIPs	O número de endereços IP elásticos que foram alocados de um bloco CIDR do grupo IPv4 público contíguo fornecido pela Amazon que não estão associados a uma interface de rede elástica.

Métricas do resolvedor da lista de prefixos do IPAM

Recomendamos a definição de alarmes do CloudWatch para métricas de falha, pois pode ser necessário reavaliar e ajustar as regras do resolvedor da lista de prefixos do IPAM para permanecer dentro dos limites de versão e tamanho da lista de prefixos.

Nome da métrica	Descrição
IpamPrefixListResolverSyncFailure	O resolvedor da lista de prefixos não conseguiu sincronizar com o destino. Isso pode acontecer quando uma cota, como “entradas CIDR por versão do resolvedor da lista de prefixos”, foi excedida, a lista de prefixos do destino não foi encontrada ou a sincronização está desabilitada na lista de prefixos gerenciadas do destino.

Nome da métrica	Descrição
IpamPrefixListResolverSyncSuccess	Resolvedor de lista de prefixos sincronizado com êxito com o destino.
IpamPrefixListResolverVersionCreationSuccess	A criação da versão foi bem-sucedida.
Falha na criação da versão de resolução da lista de prefixos IPAM	Houve falha na criação da versão. Isso pode acontecer se você atingiu sua cota de “entradas CIDR por versão do resolvedor de lista de prefixos”.

Dimensões da métrica

Para filtrar as métricas do IPAM, use as dimensões a seguir.

Dimensão	Descrição
AddressFamily	A família de endereços IP para CIDRs de recursos (IPv4 ou IPv6).
Locale	A região da AWS na qual um grupo do IPAM está disponível para alocações.
PoolID	O ID de um grupo.
ScopeID	O ID de um escopo.

Para obter informações sobre o monitoramento de VPCs com o Amazon CloudWatch, consulte as Métricas do CloudWatch para suas VPCs no Guia do usuário do Amazon Virtual Private Cloud.

Métricas de utilização de recursos do IPAM

O IPAM publica métricas de utilização de IPs para recursos que o IPAM monitora no Amazon CloudWatch. Esses recursos incluem:

- VPCs (IPv4 e IPv6)
- Sub-redes (IPv4)

- Grupos IPv4 públicos

O IPAM calcula e publica separadamente métricas de utilização de IP por família de endereços IP (IPv4 ou IPv6). A utilização de IP de um recurso é calculada em todos os CIDRs da mesma família de endereços.

Em cada combinação de tipo de recurso e família de endereços, o IPAM utiliza três regras para determinar quais métricas publicar:

- Até 50 recursos com a mais alta utilização de IP. É possível usar essas informações para configurar alarmes para receber notificações se um limite de utilização de IP for violado.
- Até 50 recursos com a mais baixa utilização de IP. É possível usar essas informações para decidir se você deseja manter ou excluir recursos subutilizados.
- Até 50 outros recursos. É possível usar essas informações para rastrear consistentemente a utilização de IP de recursos que podem não ser capturados no grupo de alta ou baixa utilização.
  - Até 50 VPCs contendo um CIDR alocado de um grupo IPAM (priorizado pelo tamanho total dos blocos CIDR).
  - Até 50 sub-redes cuja VPC contém um CIDR alocado de um grupo IPAM (priorizado pelo tamanho total de blocos CIDR).
  - Até 50 grupos IPv4 públicos contendo um CIDR alocado de um grupo IPAM (priorizado pelo tamanho total dos blocos CIDR).

Depois de aplicar cada regra, as métricas são agregadas e publicadas com o mesmo nome de métrica para cada tipo de recurso. Veja a seguir informações detalhadas sobre os nomes das métricas e suas dimensões.

Important

Há um limite exclusivo para cada combinação de tipo de recurso, família de endereços e regra. O valor padrão de cada limite é 50. Você pode ajustar esses limites entrando em contato com o AWS Support Center, conforme descrito em Cotas de serviço da AWS, na Referência geral da AWS.

Example Exemplo

Digamos que seu IPAM monitore 2.500 VPCs e 10.000 sub-redes, todas com CIDRs IPv4 e IPv6. O IPAM publica as métricas de utilização de IPs a seguir:

- Até 150 métricas para a utilização de IPs IPv4 para VPC, incluindo:
  - As 50 VPCs com a mais alta utilização de IPs IPv4
  - As 50 VPCs com a mais baixa utilização de IPv4
  - Até 50 VPCs contendo um CIDR IPv4 alocado de um grupo IPAM
- Até 150 métricas para a utilização de IPv6 para VPC, incluindo:
  - As 50 VPCs com a mais alta utilização de IPs IPv6
  - As 50 VPCs com a mais baixa utilização de IPv6
  - Até 50 VPCs contendo um CIDR IPv6 alocado de um grupo IPAM
- Até 150 métricas para a utilização IPv4 para sub-rede, incluindo:
  - As 50 sub-redes com a mais alta utilização de IPs IPv4
  - As 50 sub-redes com a mais baixa utilização de IPs IPv4
  - Até 50 sub-redes cujas VPCs contêm um CIDR IPv4 alocado de um grupo IPAM

Métricas da VPN

O nome e a descrição da métrica de VPC estão listados abaixo.

Nome da métrica	Descrição
VpcIPUsage	O total de IPs cobertos por CIDRs nas sub-redes de VPC, dividido pelo total de IPs cobertos por CIDRs na VPC. Isso é calculado em todos os CIDRs de VPC no mesmo escopo de IPAM e separadamente para CIDRs IPv4 e IPv6.

As dimensões que você pode usar para filtrar métricas da VPC estão listadas abaixo.

Dimensão	Descrição
AddressFamily	A família de endereços IP para CIDRs de recursos (IPv4 ou IPv6).
OwnerID	O ID do proprietário da VPC.
Região	Região da AWS onde está localizada a VPC.
ScopeID	O ID do escopo de IPAM ao qual a VPC pertence.
VpcID	O ID da VPC.

Métricas de sub-redes

O nome e a descrição da métrica de sub-redes estão listados abaixo.

Nome da métrica	Descrição
SubnetIPUsage	O número de IPs ativos, dividido pelo total de IPs no CIDR IPv4 da sub-rede.

As dimensões que você pode usar para filtrar métricas da sub-rede estão listadas abaixo.

Dimensão	Descrição
AddressFamily	A família de endereços IP para CIDRs de recursos (somente IPv4).
OwnerID	O ID do proprietário da sub-rede.
Região	Região da AWS onde está localizada a sub-rede.
ScopeID	O ID do escopo de IPAM ao qual a sub-rede pertence.
SubnetID	O ID da sub-rede.
VpcID	O ID da VPC à qual a sub-rede pertence.

Métricas de grupos IPv4 públicos

O nome e a descrição da métrica de grupos IPv4 públicos estão listados abaixo.

Nome da métrica	Descrição
PublicIPv4PoolIPUsage	O número de EIPs do grupo IPv4 público, dividido pelo total de IPs no grupo.

As dimensões que você pode usar para filtrar métricas de grupos IPv4 públicos estão listadas abaixo.

Dimensão	Descrição
OwnerID	O ID do proprietário do grupo IPv4 público.
PublicIPv4PoolID	O ID do grupo IPv4 público.
Região	A Região da AWS em que o grupo IPv4 público está localizado.
ScopeID	O ID do escopo de IPAM ao qual o grupo IPv4 público pertence.

Métricas do IP Insight público

Os nomes e descrições das métricas públicas do IP Insight estão listados abaixo.

Nome da métrica	Descrição
AmazonOwnedElasticIPs	A quantidade de endereços Elastic IP pertencentes à Amazon que você provisionou ou atribuiu a recursos em sua conta AWS.
AssociatedAmazonOwnedElasticIPs	A quantidade de endereços IP da Elastic pertencentes à Amazon que você associou a recursos em sua conta AWS.
AssociatedBringYourOwnIPs	A quantidade de endereços IPv4 públicos que você trouxe para AWS utilizando a opção "Bring your own IP addresses" (BYOIP) e que foram associados a recursos em sua conta AWS.

Nome da métrica	Descrição
BringYourOwnIPs	A quantidade de endereços IPv4 públicos que você trouxe para AWS usando a opção "Bring your own IP addresses" (BYOIP).
EC2PublicIPs	A quantidade de endereços IPv4 públicos atribuídos a instância s EC2 quando as instâncias foram lançadas em uma sub-rede predefinida ou em uma sub-rede configurada para atribuir automaticamente um endereço IPv4 público.
ServiceManagedBringYourOwnIPs	O número de endereços IPv4 públicos que você trouxe para AWS usando o BYOIP (Bring your own IP addresses) e que são provisionados e gerenciados por um serviço AWS.
ServiceManagedIPs	A quantidade de endereços IPv4 públicos fornecidos e gerenciados por um serviço da AWS.
UnassociatedAmazonOwnedElasticIPs	A quantidade de endereços Elastic IP pertencentes à Amazon que não foram associados a recursos em sua conta da AWS.
UnassociatedBringYourOwnIPs	O número de endereços IPv4 públicos que você trouxe para AWS usando a opção "Bring your own IP addresses" (BYOIP) e que não foram associados a quaisquer recursos em sua conta da AWS.

As dimensões que você pode utilizar para filtrar as métricas de percepção de IP público estão listadas abaixo.

Dimensão	Descrição
IpamId	A ID do IPAM a que pertence o endereço IP.
Região	A AWS Region em que o endereço IP público está localizado.

Dica rápida para a criação de alarmes

Para criar rapidamente um alarme do Amazon CloudWatch para recursos com alta utilização de endereços IP, abra o console do CloudWatch e escolha Métricas, Todas as métricas, escolha a guia Consulta, escolha o Namespace `AWS/IPAM > VPC IP Usage Metrics`, `AWS/IPAM > Subnet IP Usage Metrics` ou `AWS/IPAM > Public IPv4 Pool IP Usage Metrics`, escolha o Nome da métrica `MAX(VpcIPUsage)`, `MAX(SubnetIPUsage)`, ou `MAX(PublicIPv4PoolIPUsage)` e escolha Criar um alarme. Para obter mais informações, consulte Criar alarmes em consultas do Metrics Insights, no Guia do usuário do Amazon CloudWatch.

Ver histórico de endereços IP

Siga as etapas desta seção para visualizar o histórico de um endereço IP ou CIDR em um escopo do IPAM. Você pode usar os dados históricos para analisar e auditar suas políticas de roteamento e segurança de rede. O IPAM retém automaticamente seus dados de monitoramento de endereços IP por até três anos.

Você pode usar os dados históricos de IP para pesquisar a alteração de status de endereços IP ou CIDRs dos seguintes tipos de recursos:

- VPCs
- Sub-redes VPC
- Endereços IP elásticos
- Instâncias do EC2
- Interfaces de rede do EC2 anexadas a instâncias

> **Important**
>
> Embora o IPAM não monitore instâncias do Amazon EC2 ou interfaces de rede do EC2 anexadas a instâncias, é possível usar o recurso Pesquisar histórico de IP para pesquisar dados históricos em CIDRs de interfaces de rede e de instâncias do EC2.

Note

- Se você mover um recurso de um escopo do IPAM para outro, o registro de histórico anterior terminará e um novo registro de histórico será criado sob o novo escopo. Para obter mais informações, consulte Mover CIDRs da VPC entre escopos.
- Se você excluir ou transferir um recurso para uma conta da AWS que não seja monitorada pelo IPAM, qualquer novo histórico relacionado ao recurso não ficará visível e o IPAM não monitorará o recurso. O endereço IP do recurso, no entanto, ainda poderá ser pesquisado.
- Se você Integrar o IPAM a contas fora de sua organização, o proprietário do IPAM poderá visualizar o histórico de endereços IP de todos os CIDRs de recursos pertencentes a essas contas.

AWS Management Console

Para visualizar o histórico de um CIDR

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pesquisar histórico de IP.
3. Insira um endereço IP IPv4 ou IPv6 ou um CIDR. Esse deve ser um CIDR específico para o recurso.
4. Escolha um ID de escopo do IPAM.
5. Escolha um intervalo de data/hora.
6. Se você quiser filtrar os resultados por VPC, insira o ID de uma VPC. Use essa opção se o CIDR aparecer em várias VPCs.
7. Selecione a opção Pesquisar.

Command line

Os comandos nessa seção são vinculados à Referência de comando AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

- Visualizar o histórico de um CIDR: get-ipam-address-history

Para ver exemplos de como você pode usar a AWS CLI para analisar e auditar o uso de endereços IP, consulte Tutorial: ver o histórico de endereços IP usando a AWS CLI.

Os resultados da pesquisa são organizados nas seguintes colunas:

- Sampled end time (Hora de término da amostra): hora final da amostra da associação entre recurso e CIDR dentro do escopo do IPAM. As alterações são coletadas em snapshots periódicos, portanto, a hora de término pode ter ocorrido antes desse horário específico.
- Sampled start time (Hora de início da amostra): hora de início da amostra da associação entre recurso e CIDR dentro do escopo do IPAM. As alterações são coletadas em snapshots periódicos, portanto, a hora de início pode ter ocorrido antes desse horário específico.

  Example

  Para ajudar a explicar os horários que você vê em “Sampled start time” (Hora de início da amostra) e “Sampled end time” (Hora de término da amostra), vamos dar uma olhada em um exemplo de caso de uso:

  Às 14h00, uma VPC foi criada com o CIDR 10.0.0.0/16. Às 15h00, você cria um IPAM e um grupo do IPAM com o CIDR 10.0.0.0/8 e seleciona a opção de importação automática para permitir que o IPAM descubra e importe todos os CIDRs que se enquadrarem no intervalo de endereços IP 10.0.0.0/8. Como o IPAM captura as alterações nos CIDRs em snapshots periódicos, ele não descobre o CIDR da VPC existente até as 15h05. Quando você pesquisa o ID dessa VPC usando o recurso Pesquisar histórico de IP, o horário de início da amostra da sua VPC é 15h05, que é quando o IPAM a descobriu, e não às 14h, que é a hora em que a VPC foi criada. Agora, suponhamos que você decida excluir a VPC às 17h. Quando a VPC foré excluída, o CIDR 10.0.0.0/16 alocado para a VPC será reciclado de volta para o grupo do IPAM. O IPAM captura um snapshot periódico às 17h05 e captura a alteração. Quando você pesquisar o ID dessa VPC em Pesquisar histórico de IP, 17h05 será o horário de término da amostra do CIDR da VPC, e não 17h, que é a hora em que a VPC foi excluída.
- Resource ID (ID do recurso): o ID gerado quando o recurso foi associado ao CIDR.
- Name (Nome): o nome do recurso (se aplicável).
- Compliance status (Status de conformidade): o status de conformidade do CIDR.
  - Compliant (Em conformidade): um recurso gerenciado está em conformidade com as regras de alocação do grupo do IPAM.

- Noncompliant (Em não conformidade): o CIDR de recurso não está em conformidade com uma ou mais das regras de alocação do grupo do IPAM.

  Example

  Se uma VPC tiver um CIDR que não atenda aos parâmetros de comprimento da máscara de rede do grupo do IPAM ou se o recurso não estiver na mesma região da AWS que o grupo do IPAM, ele será sinalizado como não compatível.
- Não gerenciado: o recurso não tem um CIDR alocado de um grupo do IPAM e não está sendo monitorado pelo IPAM quanto à possível conformidade do CIDR com regras de alocação de grupos. O CIDR é monitorado quanto à sobreposição.
- Ignored (Ignorado): o recurso gerenciado foi escolhido para ficar isento do monitoramento. Os recursos ignorados não são avaliados quanto à sobreposição ou conformidade com as regras de alocação. Quando um recurso for escolhido para ser ignorado, qualquer espaço alocado a ele de um grupo do IPAM retornará ao grupo e o recurso não será importado novamente por meio da importação automática (se a regra de alocação de importação automática estiver definida no grupo).
- -: esse recurso não é um dos tipos de recursos que o IPAM pode monitorar ou gerenciar.

- Overlap status (Status de sobreposição): o status de sobreposição do CIDR.
  - Nonoverlapping (Sem sobreposição): o recurso CIDR não se sobrepõe a outro CIDR no mesmo escopo.
  - Overlapping (Com sobreposição): o recurso CIDR se sobrepõe a outro CIDR no mesmo escopo. Observe que, se um CIDR de recurso estiver se sobrepondo, ele poderá estar sobreposto a uma alocação manual.
  - Ignored (Ignorado): o recurso gerenciado foi escolhido para ficar isento do monitoramento. Os recursos ignorados não são avaliados pelo IPAM quanto à sobreposição ou conformidade com a regra de alocação. Quando um recurso for escolhido para ser ignorado, qualquer espaço alocado a ele de um grupo do IPAM retornará ao grupo e o recurso não será importado novamente por meio da importação automática (se a regra de alocação de importação automática estiver definida no grupo).
  - -: esse recurso não é um dos tipos de recursos que o IPAM pode monitorar ou gerenciar.
- Tipo de recurso
  - vpc: o CIDR está associado a uma VPC.
  - subnet (sub-rede): o CIDR está associado a uma sub-rede da VPC.
  - EIP: o CIDR está associado a um endereço IP elástico.

  - instance (instância): o CIDR está associado a uma instância do EC2.
  - network-interface (interface de rede): o CIDR está associado a uma interface de rede.
- VPC ID (ID da VPC): o ID da VPC a que este recurso pertence (se aplicável).
- Region (Região): a região da AWS desse recurso.
- Owner ID (ID de proprietário): o ID da conta da AWS do usuário que criou esse recurso (se aplicável).

Visualizar insights de IPs públicos

Você pode usar Insights de IP público para ver o seguinte:

- Se o IPAM estiver integrado a contas dentro de uma Organização da AWS, é possível visualizar todos os endereços IPv4 públicos utilizados pelos serviços em todas as AWS Regions da sua organização da AWS.
- No caso de o IPAM estar integrado a uma única conta, é possível visualizar todos os endereços IPv4 públicos utilizados pelos serviços em todas as AWS Regions dessa conta específica.

Um endereço IPv4 público é um endereço IPv4 roteável pela Internet. É necessário um endereço IPv4 público para um recurso poder ser acessado diretamente da Internet via IPv4.

> **Note**
>
> A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.

Você pode ver insights sobre os seguintes tipos de endereços IPv4 públicos:

- Endereços IP elásticos (EIPs): endereços IPv4 públicos estáticos fornecidos pela Amazon que você pode associar a uma instância do EC2, interface de rede elástica ou recurso da AWS.
- Endereços IPv4 públicos do EC2: endereços IPv4 públicos atribuídos a uma instância do EC2 pela Amazon (se a instância do EC2 for iniciada em uma sub-rede padrão ou for executada em uma sub-rede configurada para atribuir automaticamente um endereço IPv4 público).

- Endereços BYOIPv4: endereços IPv4 públicos no intervalo de endereços IPv4 que você trouxe para a AWS usando o recurso Traga seus próprios endereços IP (BYOIP).
- Endereços IPv4 gerenciados por serviços: endereços IPv4 públicos provisionados automaticamente em recursos da AWS e gerenciados por um serviço da AWS. Por exemplo, endereços IPv4 públicos no Amazon ECS, no Amazon RDS ou no Amazon WorkSpaces.

Os Insights de IP públicos fornecem uma visão abrangente de todos os endereços IPv4 públicos utilizados pelos serviços em todas as regiões. É possível usar esses insights para identificar o uso de endereços IPv4 públicos e ver recomendações para liberar endereços IP elásticos não utilizados.

- Tipos de IPs públicos: o número de endereços IPv4 públicos organizados por tipo.
  - EIPs de propriedade da Amazon: endereços IP elásticos que você provisionou ou atribuiu a recursos na sua conta da AWS.
  - IPs públicos do EC2: endereços IPv4 públicos atribuídos a instâncias do EC2 quando estas foram iniciadas em uma sub-rede padrão ou em uma sub-rede que foi configurada para atribuir automaticamente um endereço IPv4 público.
  - POR IP: endereços IPv4 públicos que você trouxe para a AWS usando o recurso Traga seus próprios endereços IP (BYOIP).
  - IPs gerenciados por serviços: endereços IPv4 públicos provisionados e gerenciados por um serviço da AWS.
  - BYOIP gerenciado por serviço: endereços IPv4 públicos trazidos para a AWS e gerenciados por um serviço da AWS.
  - EIPs contíguos de propriedade da Amazon: endereços IP elásticos alocados de um grupo IPv4 público contíguo do IPAM fornecido pela Amazon.
- Uso de EIPs: o número de endereços IP elásticos organizados pela forma como são usados.
  - EIPs associados de propriedade da Amazon: endereços IP elásticos que você provisionou na sua conta da AWS e que associou a uma instância do EC2, interface de rede ou recurso da AWS.
  - BYOIP associado: endereços IPv4 públicos que você trouxe para a AWS usando o BYOIP e que associou a uma interface de rede.
  - EIPs não associados de propriedade da Amazon: endereços IP elásticos que você provisionou na sua conta da AWS, mas não associou a uma interface de rede.
  - BYOIP não associado: endereços IPv4 públicos que você trouxe para a AWS usando o BYOIP, mas que não associou a uma interface de rede.

  - EIPs contíguos associados de propriedade da Amazon: endereços IP elásticos alocados de um grupo IPv4 público contíguo do IPAM fornecido pela Amazon e associado a um recurso.
  - EIPs contíguos não associados de propriedade da Amazon: endereços IP elásticos alocados de um grupo IPv4 público contíguo do IPAM fornecido pela Amazon e não associado a um recurso.
- Uso de IPs IPv4 contíguos de propriedade da Amazon: uma tabela que mostra o uso de endereços IPv4 públicos contíguos ao longo do tempo e grupos IPv4 do IPAM relacionados de propriedade da Amazon.
- Endereços IP públicos: uma tabela de endereços IPv4 públicos e seus atributos.
  - Endereço IP: o endereço IPv4 público.
  - Associado: se o endereço está ou não associado a uma instância do EC2, interface de rede ou recurso da AWS.
    - Associado: o endereço IPv4 público está associado a uma instância do EC2, interface de rede ou recurso da AWS.
    - Não associado: o endereço IPv4 público não está associado a nenhum recurso e está ocioso na sua conta da AWS.
  - Tipo de endereço: o tipo de endereço IP.
    - EIP de propriedade da Amazon: o endereço IPv4 público é um endereço IP elástico.
    - POR IP: o endereço IPv4 público foi levado para a AWS usando o recurso BYOIP.
    - IP público do EC2: o endereço IPv4 público foi atribuído automaticamente a uma instância do EC2.
    - BYOIP gerenciado pelo serviço: Este é o endereço IPv4 público que foi trazido para o AWS utilizando a opção BYOIP (Bring your own IP).
    - IP gerenciado por serviço: o endereço IPv4 público foi provisionado e é gerenciado por um serviço da AWS.
  - Serviço: o serviço ao qual o endereço IP está associado.
    - AGA: Uma AWS Global Accelerator. Se um acelerador de roteamento personalizado for usado, seus IPs públicos não serão listados. Para ver esses IPs públicos, consulte Visualizar aceleradores de roteamento personalizados.
    - Database Migration Service: uma instância de replicação do AWS Database Migration Service (DMS).
    - Redshift: um cluster do Amazon Redshift.
    - RDS: uma instância do Amazon Relational Database Service (RDS)

  - Balanceador de carga (EC2): um Application Load Balancer ou um Network Load Balancer.
  - Gateway NAT (VPC): um gateway NAT público do Amazon VPC.
  - Site-to-Site VPN: um gateway privado virtual do AWS Site-to-Site VPN.
  - Outros: outro serviço que atualmente não é identificável.
- Nome (ID EIP): se esse endereço IPv4 público for uma alocação de endereço IP elástico, esse será o nome e o ID da alocação de EIP.
- ID da interface de rede: se esse endereço IPv4 público estiver associado a uma interface de rede, esse será o ID da interface de rede.
- ID da instância: se esse endereço IPv4 público estiver associado a uma instância do EC2, esse será o ID da instância.
- Grupos de segurança: se esse endereço IPv4 público estiver associado a uma instância do EC2, esse será o nome e a ID do grupo de segurança atribuído à instância.
- Grupo IPv4 público: se for um endereço IP elástico de um pool de endereços IP de propriedade e gerenciado pela Amazon, o valor será “-”. Se for um endereço IP elástico de um intervalo de endereços IP que você possui e trouxe para a Amazon (usando BYOIP), o valor será o ID público do grupo IPv4.
- Grupo de borda de rede: se o endereço IP for anunciado, esta é a Região do AWS a partir da qual o endereço IP é anunciado.
- ID do proprietário: O número da conta da AWS do proprietário do recurso.
- Tempo de amostragem: O último tempo de descoberta de recurso bem-sucedido.
- ID de descoberta de recurso: ID da descoberta de recurso que descobriu esse endereço IPv4 público.
- Recurso de serviço: ARN ou ID do recurso.

Se um endereço IP elástico estiver alocado à sua conta, mas não estiver associado a uma interface de rede, aparecerá um banner informando que você tem EIPs não associados na sua conta e que deve liberá-los.

> **Important**
>
> As Insights de IP público foram recentemente atualizadas. Se você encontrar um erro relacionado à falta de permissões para chamar GetIpamDiscoveredPublicAddresses, é necessário atualizar a permissão gerenciada anexada a uma descoberta de recurso compartilhada com você. Recomendamos entrar em contato com a pessoa responsável

pela criação da descoberta de recursos e solicitar a atualização da permissão gerenciada de `AWSRAMPermissionIpamResourceDiscovery` para a versão mais recente. Para obter detalhes adicionais, consulte Atualização de um compartilhamento de recursos no Guia do Usuário AWS RAM.

AWS Management Console

Para ver informações sobre endereços IP públicos

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Insights de IP públicos.
3. Para ver detalhes de um endereço IP público, selecione um endereço IP clicando nele.
4. Veja as informações a seguir sobre o endereço IP:
   - Detalhes: as mesmas informações visíveis nas colunas do painel principal de insights de IP público, como Tipo de endereço e Serviço.
   - Regras do grupo de segurança de entrada: se esse endereço IP estiver associado a uma instância do EC2, essas serão as regras do grupo de segurança que controlam o tráfego de entrada na instância.
   - Regras do grupo de segurança de saída: se esse endereço IP estiver associado a uma instância do EC2, essas serão as regras do grupo de segurança que controlam o tráfego de saída da instância.
   - Etiquetas: pares de chave e valor que atuam como metadados para organizar seus recursos da AWS.

Command line

Use o comando a seguir para obter os endereços IP públicos que foram descobertos pelo IPAM: get-ipam-discovered-public-addresses

Tutoriais para o IP Address Manager da Amazon VPC

Os seguintes tutoriais do mostram como executar tarefas comuns do IPAM usando a AWS CLI. Para obter a AWS CLI, consulte Acessar o IPAM. Para obter mais informações sobre os conceitos do IPAM mencionados nesses tutoriais, consulte Como funciona o IPAM.

Conteúdo

- Conceitos básicos do IPAM usando a AWS CLI
- Tutorial: criar um IPAM e grupos usando o console
- Tutorial: criar um IPAM e grupos usando a AWS CLI
- Tutorial: ver o histórico de endereços IP usando a AWS CLI
- Tutorial: Traga o seu ASN para o IPAM
- Tutorial: trazer seus endereços IP para o IPAM
- Tutorial: transferir um CIDR IPv4 BYOIP para o IPAM
- Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede
- Alocar endereços IP elásticos sequenciais de um grupo do IPAM

Conceitos básicos do IPAM usando a AWS CLI

Neste tutorial, você receberá orientações sobre o processo de configuração e de uso do gerenciador de endereços IP (IPAM) da Amazon VPC com a AWS CLI, usando uma única conta da AWS. Quando concluir este tutorial, você terá criado um IPAM, definido uma hierarquia de grupos de endereços IP e alocado um bloco CIDR para uma VPC.

Pré-requisitos

Certifique-se de atender aos seguintes pré-requisitos antes de iniciar este tutorial:

- Ter uma conta da AWS com as permissões necessárias para criação e gerenciamento de recursos do IPAM.
- Ter a AWS CLI instalada e devidamente configurada com as credenciais apropriadas. Para obter mais informações sobre a instalação da AWS CLI, consulte Instalar ou atualizar a versão mais recente da AWS CLI. Para obter mais informações sobre a configuração da AWS CLI, consulte Configuration basics.

- Ter uma compreensão básica sobre endereçamento IP e notação CIDR.
- Ter um conhecimento básico sobre os conceitos relacionados à Amazon VPC.
- Dispor de, aproximadamente, 30 minutos para concluir o tutorial.

Criar um IPAM

A etapa inicial consiste na criação de um IPAM com regiões de operação definidas. O IPAM auxilia no planejamento, no rastreamento e no monitoramento de endereços IP usados pelas workloads da AWS.

Crie um IPAM com regiões de operação em us-east-1 e us-west-2:

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

Este comando cria um IPAM e o habilita para gerenciar endereços IP nas regiões especificadas. As regiões de operação correspondem às regiões da AWS nas quais o IPAM está autorizado a gerenciar blocos CIDR de endereços IP.

Verifique se o IPAM foi criado:

```
aws ec2 describe-ipams
```

Anote o ID do IPAM apresentado na saída, pois esse valor será necessário para as próximas etapas.

Aguarde até que o IPAM esteja totalmente criado e disponível, em um processo que demora, aproximadamente, 20 segundos:

```
sleep 20
```

Obtenção do ID do escopo do IPAM

Quando você cria um IPAM, a AWS cria automaticamente um escopo privado e um escopo público. Para este tutorial, usaremos o escopo privado.

Recupere os detalhes do IPAM e extraia o ID do escopo privado:

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

Certifique-se de substituir `ipam-0abcd1234` pelo ID correspondente ao IPAM.

Na saída, identifique e anote o ID do escopo privado usando o campo `PrivateDefaultScopeId`. Ela será parecida com `ipam-scope-0abcd1234`.

Criar um grupo de IPv4 de nível superior

Agora, vamos criar um grupo de alto nível no escopo privado. Este grupo funcionará como o grupo principal para todos os outros grupos pertencentes à hierarquia.

Crie um grupo de endereços IPv4 de alto nível:

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

Certifique-se de substituir `ipam-scope-0abcd1234` pelo ID correspondente ao escopo privado.

Aguarde até que o grupo esteja totalmente criado e disponível:

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

Certifique-se de substituir `ipam-pool-0abcd1234` pelo ID correspondente ao grupo de alto nível. Antes de prosseguir, o estado deve encontrar-se em `create-complete`.

Após o grupo ser disponibilizado, providencie um bloco CIDR para ele:

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

Aguarde até que o bloco CIDR esteja totalmente provisionado:

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

Antes de prosseguir, o estado deve encontrar-se em `provisioned`.

Criação de um grupo de endereços IPv4 regional

Em seguida, crie um grupo regional pertencente ao grupo de alto nível. Esse grupo será dedicado a uma região da AWS específica.

Crie um grupo de endereços IPv4 regional:

```
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"
```

Certifique-se de substituir `ipam-scope-0abcd1234` pelo ID correspondente ao escopo privado e `ipam-pool-0abcd1234` pelo ID correspondente ao grupo de alto nível.

Aguarde até que o grupo regional esteja totalmente criado e disponível:

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

Certifique-se de substituir `ipam-pool-1abcd1234` pelo ID correspondente ao grupo regional. Antes de prosseguir, o estado deve encontrar-se em `create-complete`.

Após o grupo ser disponibilizado, providencie um bloco CIDR para ele:

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

Aguarde até que o bloco CIDR esteja totalmente provisionado:

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

Antes de prosseguir, o estado deve encontrar-se em `provisioned`.

Criar um grupo de desenvolvimento de IPv4

Agora, crie um grupo de desenvolvimento pertencente ao grupo regional. Este grupo será destinado a ambientes de desenvolvimento.

Crie um grupo de desenvolvimento de endereços IPv4:

```
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"
```

Certifique-se de substituir `ipam-scope-0abcd1234` pelo ID correspondente ao escopo privado e `ipam-pool-1abcd1234` pelo ID correspondente ao grupo regional.

Observação: é importante incluir o parâmetro `--locale` para corresponder ao local do grupo principal.

Aguarde até que o grupo de desenvolvimento esteja totalmente criado e disponível:

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

Certifique-se de substituir `ipam-pool-2abcd1234` pelo ID correspondente ao grupo de desenvolvimento. Antes de prosseguir, o estado deve encontrar-se em `create-complete`.

Após o grupo ser disponibilizado, providencie um bloco CIDR para ele:

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

Aguarde até que o bloco CIDR esteja totalmente provisionado:

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

Antes de prosseguir, o estado deve encontrar-se em `provisioned`.

Criação de uma VPC usando um bloco CIDR do grupo do IPAM

Por fim, crie uma VPC que usa um bloco CIDR proveniente do grupo do IPAM. Isso demonstra como o IPAM pode ser usado para alocar espaços de endereços IP para recursos da AWS.

Crie uma VPC usando um bloco CIDR do grupo do 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}]'
```

Certifique-se de substituir `ipam-pool-2abcd1234` pelo ID correspondente ao grupo de desenvolvimento.

O parâmetro `--ipv4-netmask-length 26` especifica que você deseja alocar, usando o grupo, um bloco CIDR /26, que é equivalente a 64 endereços IP. Esse comprimento da máscara de rede foi escolhido para assegurar que seja menor do que o bloco CIDR do grupo, que corresponde à /24.

Verifique se a VPC foi criada:

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

Verificação da alocação no grupo do IPAM

Verifique se o bloco CIDR foi alocado usando o grupo do IPAM:

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

Certifique-se de substituir `ipam-pool-2abcd1234` pelo ID correspondente ao grupo de desenvolvimento.

Este comando apresenta todas as alocações realizadas usando o grupo do IPAM especificado, incluindo a VPC que você acabou de criar.

Solução de problemas

A seguir, apresentamos alguns problemas comuns que você pode enfrentar ao trabalhar com o IPAM:

- Erros relacionados às permissões: assegure que o perfil ou o usuário do IAM tem as permissões necessárias para realizar a criação e o gerenciamento de recursos do IPAM. Talvez seja necessário conceder as permissões `ec2:CreateIpam`, `ec2:CreateIpamPool` e demais permissões relacionadas.
- Limite de recursos excedido: por padrão, é possível criar somente um IPAM por conta. Se você já tiver um IPAM, será necessário excluí-lo antes de criar um novo ou utilizar o existente.
- Falhas relacionadas à alocação de CIDR: ao provisionar blocos CIDR para grupos, certifique-se de que o bloco CIDR que está tentando alocar não se sobreponha a alocações existentes em outros grupos.
- Tempo limite da solicitação da API: se você enfrentar erros do tipo “RequestExpired”, as causas podem estar relacionadas à latência da rede ou aos problemas de sincronização de horário. Tente executar o comando novamente.
- Erros relacionados ao estado inadequado: se receber erros “IncorrectState”, pode ser que esteja tentando executar uma operação em um recurso que ainda não está no estado adequado. Antes de prosseguir, aguarde a confirmação de que o recurso está totalmente criado ou provisionado.
- Erros relacionados ao tamanho da alocação: se receber erros “InvalidParameterValue” relacionados ao tamanho da alocação, certifique-se de que o comprimento da máscara de rede que está solicitando seja adequado ao tamanho do grupo. Por exemplo, não é possível alocar um bloco CIDR /25 usando um grupo /24.
- Violações de dependências: ao limpar os recursos, você pode enfrentar o erro “DependencyViolation”. Isso acontece porque os recursos têm dependências entre si. Certifique-se de que os recursos sejam excluídos na ordem reversa da criação e que os blocos CIDR sejam desprovisionados antes da exclusão dos grupos.

Limpar recursos

Ao concluir o presente tutorial, você deve limpar os recursos criados para evitar que incorram em cobranças desnecessárias.

1. Exclua a VPC:

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

2. Desprovisione o CIDR do grupo de desenvolvimento:

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

3. Exclua o grupo de desenvolvimento:

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

4. Desprovisione o CIDR do grupo regional:

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

5. Exclua o grupo regional:

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

6. Desprovisione o CIDR do grupo de alto nível:

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

7. Exclua o grupo de alto nível:

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

8. Exclua o IPAM:

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

Certifique-se de substituir todos os IDs pelos valores correspondentes aos IDs de recursos.

> **Note**
>
> Talvez seja necessário aguardar um tempo entre essas operações para que os recursos sejam completamente excluídos antes de prosseguir para a próxima etapa. Caso encontre violações de dependências, aguarde alguns segundos e tente novamente.

Próximas etapas

Agora que você aprendeu como criar e usar o IPAM com a AWS CLI, talvez deseje explorar recursos mais avançados:

- Planejar o provisionamento de endereços IP: saiba mais informações sobre como planejar o espaço dedicado ao endereço IP de forma eficaz
- Monitorar o uso do CIDR por recurso: compreenda como é possível monitorar o uso do endereço IP
- Compartilhar um grupo do IPAM usando o AWS RAM: saiba mais informações sobre como compartilhar grupos do IPAM entre contas da AWS
- Integrar o IPAM a contas em uma organização da AWS Organizations: descubra mais informações sobre como usar o IPAM em toda a sua organização

Tutorial: criar um IPAM e grupos usando o console

Neste tutorial, você cria um IPAM, integra com o AWS Organizations, cria grupos de endereços IP e cria uma VPC com um CIDR de um grupo do IPAM.

Este tutorial mostra como você pode usar o IPAM para organizar o espaço de endereços IP com base em diferentes necessidades de desenvolvimento. Depois de concluir este tutorial, você terá um grupo de endereços IP para recursos de pré-produção. Em seguida, você pode criar outros grupos com base em suas necessidades de roteamento e segurança, como um grupo para recursos de produção.

Embora você possa usar o IPAM como um único usuário, a integração com o AWS Organizations permite que você gerencie endereços IP em todas as contas em sua organização. Este tutorial aborda a integração do IPAM a contas em uma organização. Não aborda como Integrar o IPAM a contas fora de sua organização.

> **Note**
>
> Para os fins deste tutorial, as instruções solicitarão que você atribua um nome aos recursos do IPAM de uma maneira específica, crie recursos do IPAM em determinadas regiões e use intervalos CIDR de endereços IP específicos para seus grupos. O objetivo é agilizar as opções disponíveis no IPAM e fazer com que você comece a usá-lo rapidamente. Depois de concluir este tutorial, você pode decidir criar um novo IPAM e configurá-lo de forma diferente.

Conteúdos

- Pré-requisitos
- Como o AWS Organizations se integra ao IPAM
- Etapa 1: delegar um administrador do IPAM
- Etapa 2: criar um IPAM
- Etapa 3: criar um grupo do IPAM de nível superior
- Etapa 4: criar grupos regionais do IPAM
- Etapa 5: criar um grupo de desenvolvimento pré-produção
- Etapa 6: compartilhar o grupo do IPAM
- Etapa 7: criar uma VPC com um CIDR alocado em um grupo do IPAM
- Etapa 8: limpeza

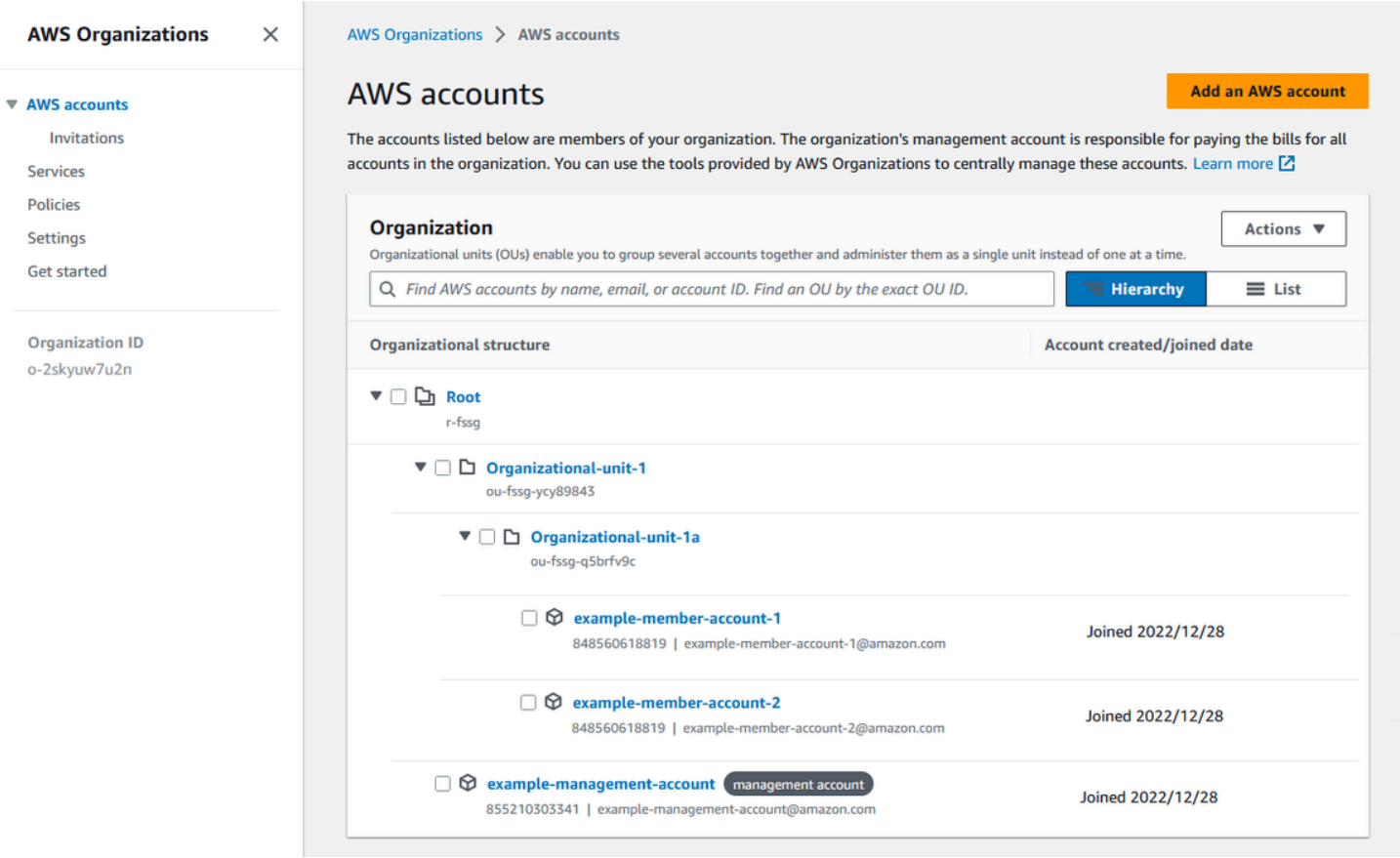
Pré-requisitos

Antes de começar, é preciso ter configurado uma conta do AWS Organizations com ao menos uma conta de membro. Para obter instruções, consulte Criar e gerenciar uma organização no Guia do usuário do AWS Organizations.

Como o AWS Organizations se integra ao IPAM

Esta seção mostra um exemplo das contas do AWS Organizations usadas neste tutorial. Há três contas em sua organização que você usa ao se integrar ao IPAM neste tutorial:

- A conta de gerenciamento (chamada example-management-account na imagem a seguir) para fazer login no console do IPAM e delegar um administrador do IPAM. Não é possível utilizar a conta de gerenciamento da organização como seu administrador do IPAM.
- Uma conta de membro (chamada example-member-account-1 na imagem a seguir) como conta de administrador do IPAM. A conta de administrador do IPAM é responsável por criar um IPAM e usá-lo para gerenciar e monitorar o uso de endereços IP em toda a organização. Qualquer conta de membro em sua organização pode ser delegada como administrador do IPAM.
- Uma conta de membro (chamada example-member-account-2 a seguir) como conta de desenvolvedor. Essa conta cria uma VPC com um CIDR alocado de um grupo do IPAM.



Além das contas, você precisará do ID da unidade organizacional (ou-fssg-q5brfv9c na imagem anterior) que contém a conta de membro que você usará como conta de desenvolvedor. Você precisa desse ID para que, em uma etapa posterior, ao compartilhar seu grupo de IPAM, seja possível compartilhá-lo com essa UO.

> **Note**
>
> Para obter mais informações sobre tipos de conta AWS Organizations, como contas de gerenciamento e de membros, consulte terminologia e conceitos do AWS Organizations.

Etapa 1: delegar um administrador do IPAM

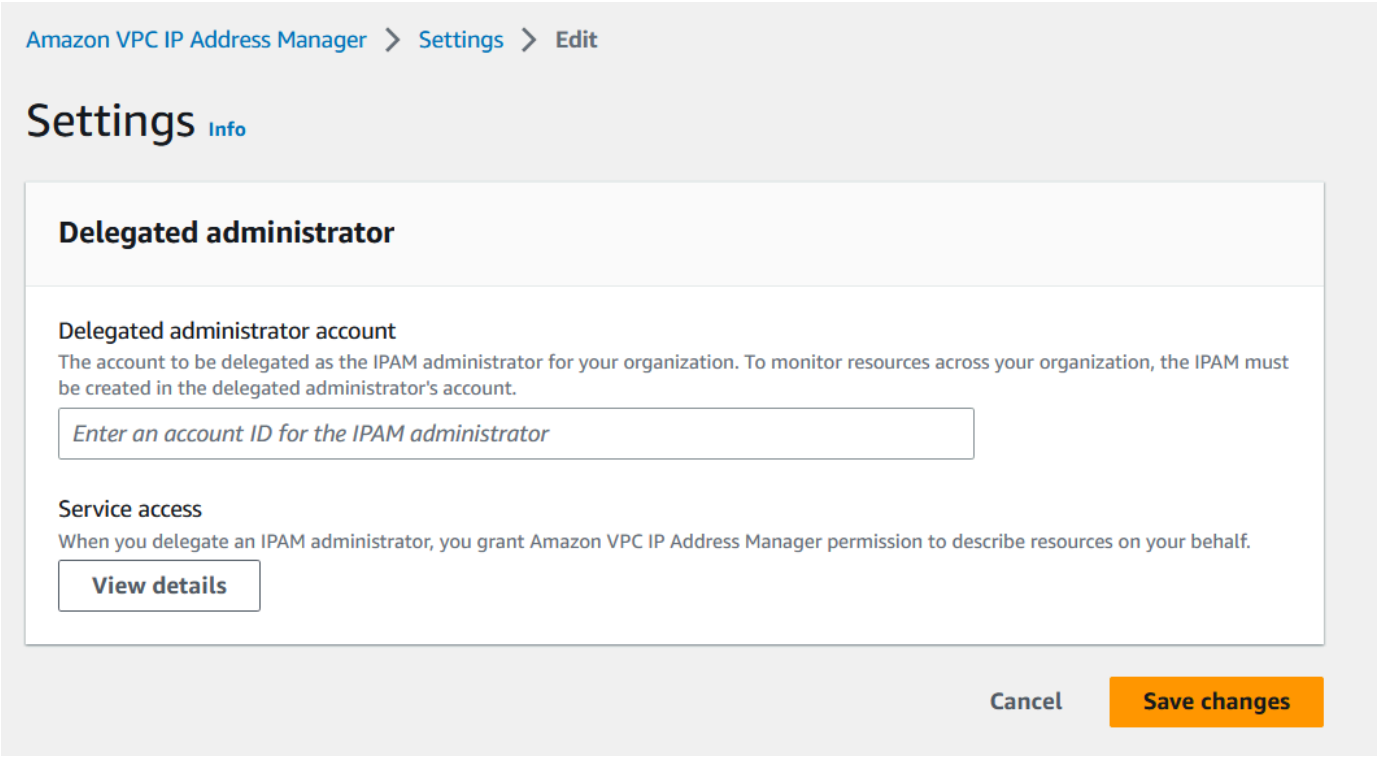
Nesta etapa, você delegará uma conta de membro do AWS Organizations como administrador do IPAM. Quando você delega um administrador do IPAM, um perfil vinculado ao serviço é criado automaticamente em cada uma das suas contas de membro do AWS Organizations. O IPAM monitora o uso de endereços IP nessas contas assumindo o perfil vinculado ao serviço em cada

conta de membro. Em seguida, ele pode descobrir os recursos e seus CIDRs, independentemente da sua unidade organizacional.

Você não pode concluir essa etapa a menos que tenha as permissões necessárias do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Integrar o IPAM a contas em uma organização da AWS Organizations.

Para delegar uma conta de administrador do IPAM

1. Use a conta de gerenciamento do AWS Organizations e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No Console de gerenciamento da AWS, escolha a região da AWS na qual você deseja trabalhar com o IPAM.
3. No painel de navegação, selecione Organization settings (Configurações da organização).
4. Selecione Delegar. A opção Delegar só estará disponível se você estiver conectado ao console como a conta de gerenciamento do AWS Organizations.
5. Insira o ID da conta da AWS para uma conta de membro da organização. O administrador do IPAM deve ser uma conta de membro do AWS Organizations, não a conta de gerenciamento.



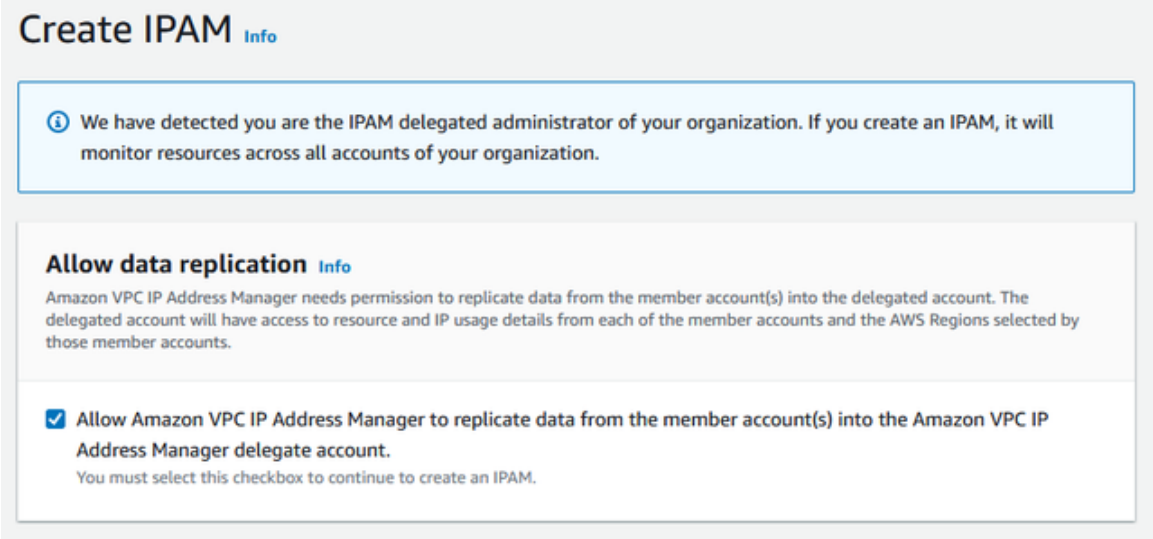
6. Escolha Salvar alterações. As informações do administrador delegado são preenchidas com detalhes relacionados à conta do membro.

Etapa 2: criar um IPAM

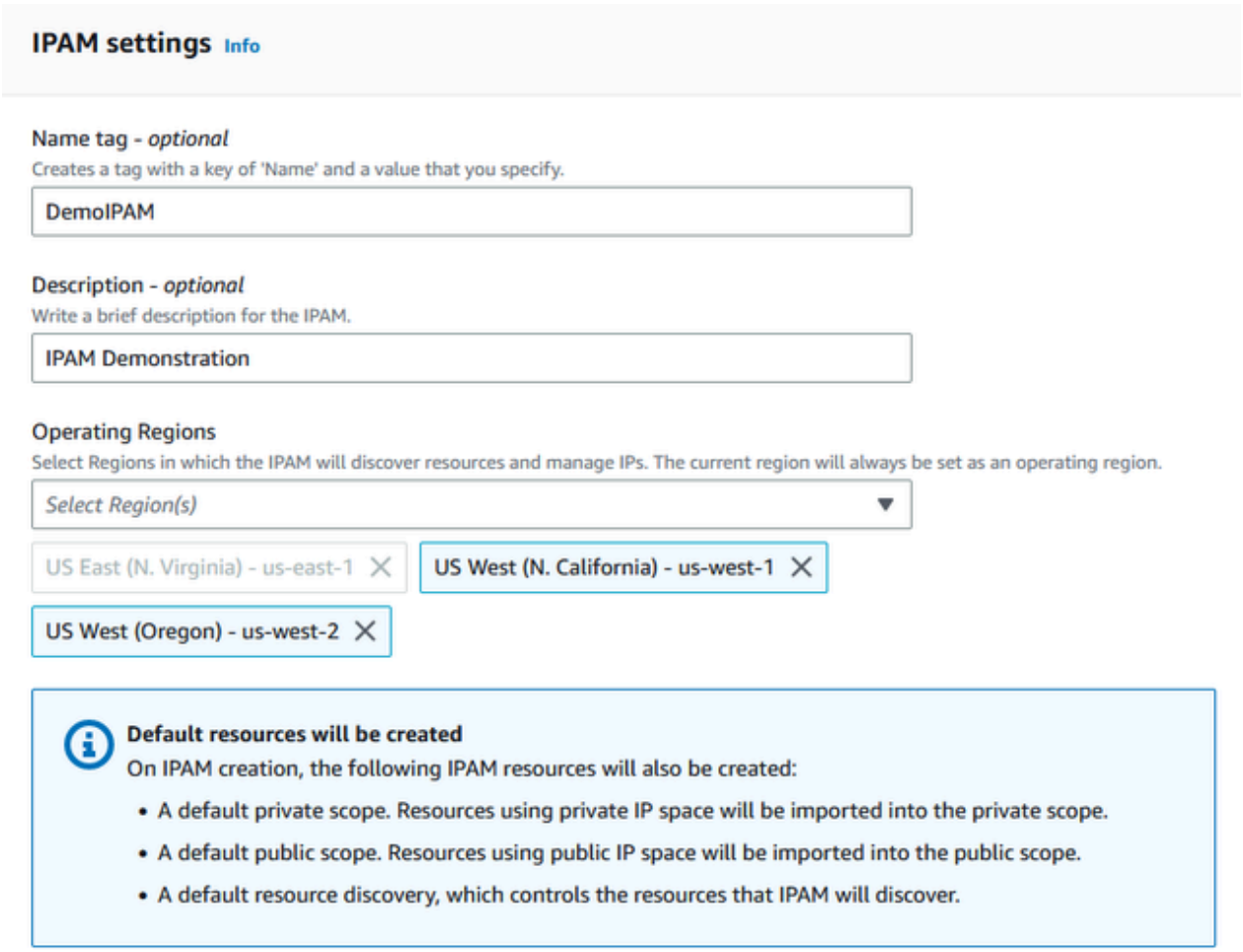
Nesta etapa, você criará um IPAM. Quando você cria um IPAM, são criados automaticamente dois escopos para o IPAM: o escopo privado destinado a todo o espaço privado e o escopo público destinado a todos os espaços públicos. Os escopos, juntamente com grupos e alocações, são componentes-chave do seu IPAM. Para obter mais informações, consulte Como funciona o IPAM.

Para criar um IPAM

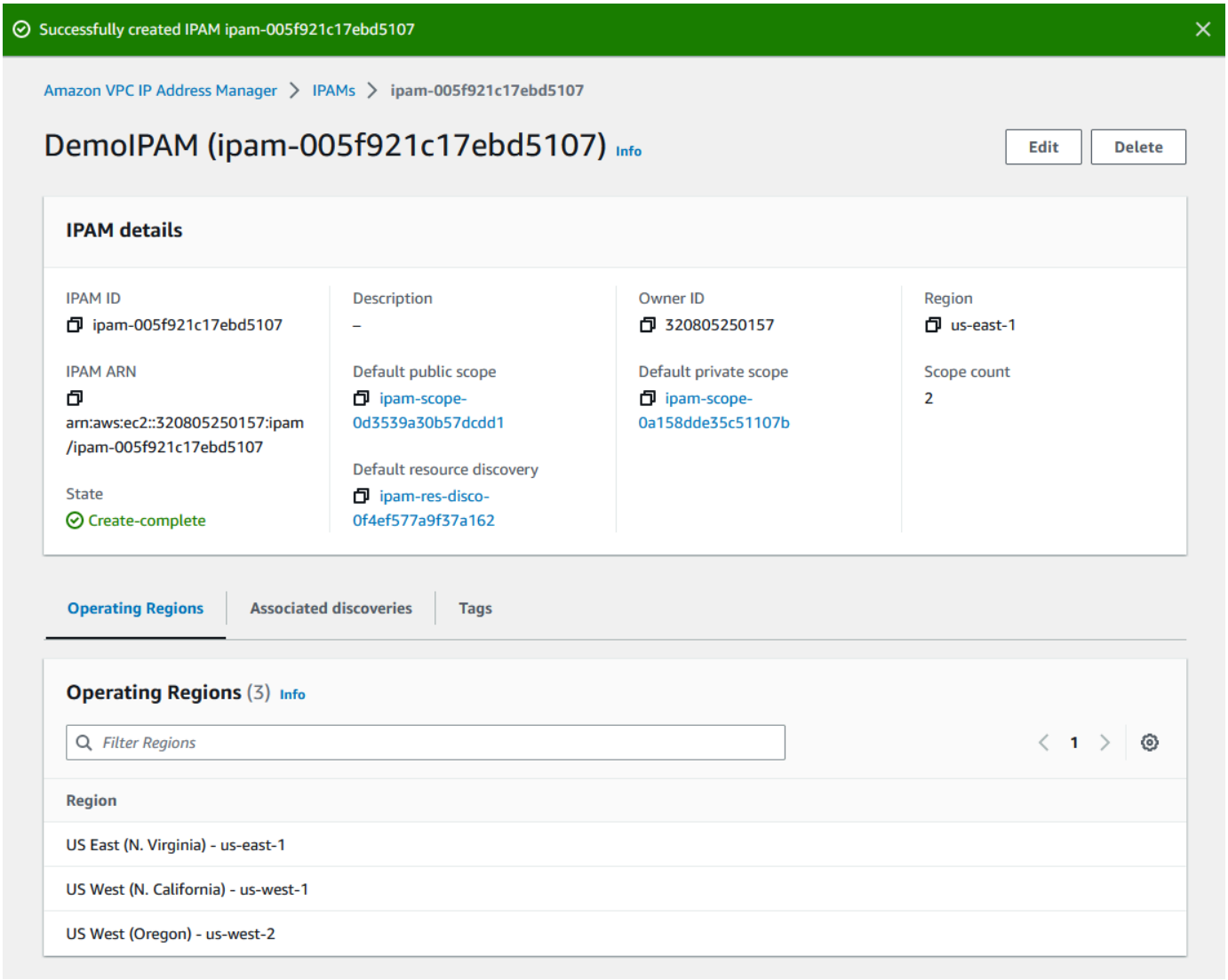
1. Usando a conta de membro do AWS Organizations delegada como administrador do IPAM na etapa anterior, abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No Console de Gerenciamento da AWS, escolha a Região da AWS em que você deseja criar o IPAM. Crie o IPAM em sua principal região de operações.
3. Na página inicial do serviço, selecione Create IPAM (Criar IPAM).
4. Selecione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir que o IP Address Manager da Amazon VPC replique dados das contas de origem para a conta delegada do IPAM). Se você não selecionar essa opção, não poderá criar um IPAM.



5. Em Regiões operacionais, escolha as regiões da AWS nas quais esse IPAM pode gerenciar e descobrir recursos. A região da AWS na qual você está criando seu IPAM é selecionada automaticamente como uma das regiões operacionais. Neste tutorial, a região de origem do nosso IPAM é us-east-1, então escolheremos us-west-1 e us-west-2 como regiões operacionais adicionais. Caso se esqueça de uma região operacional, você poderá editar as suas configurações do IPAM posteriormente e adicionar ou remover regiões.



6. Escolha Create IPAM (Criar IPAM).



Etapa 3: criar um grupo do IPAM de nível superior

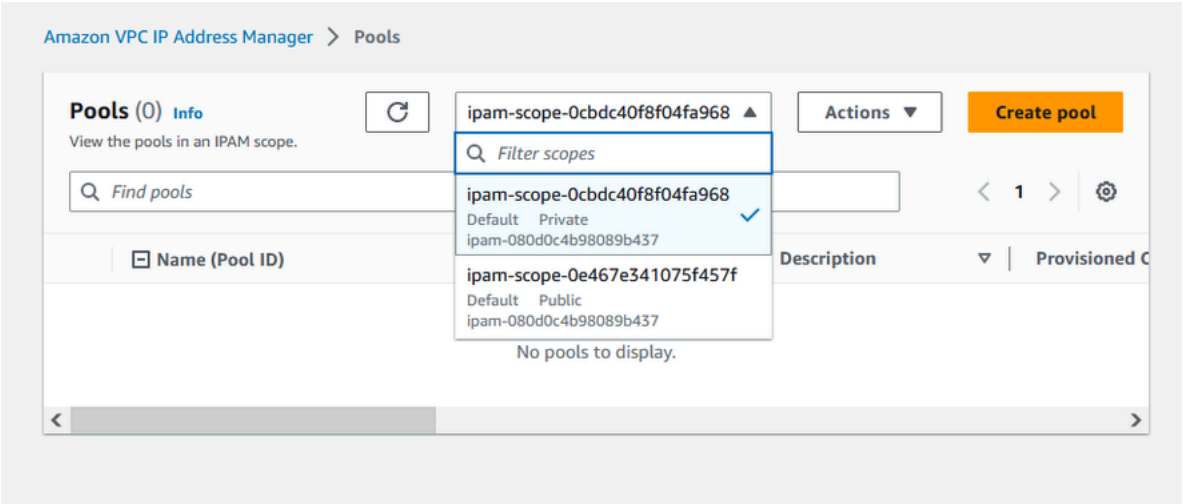
Neste tutorial, você cria uma hierarquia de grupos iniciando pelo grupo do IPAM de nível superior. Nas etapas seguintes, você criará um par de grupos regionais e um grupo de desenvolvimento de pré-produção em um dos grupos regionais.

Para obter mais informações sobre hierarquias de grupo que você pode criar com o IPAM, consulte Exemplo de planos de grupo do IPAM.

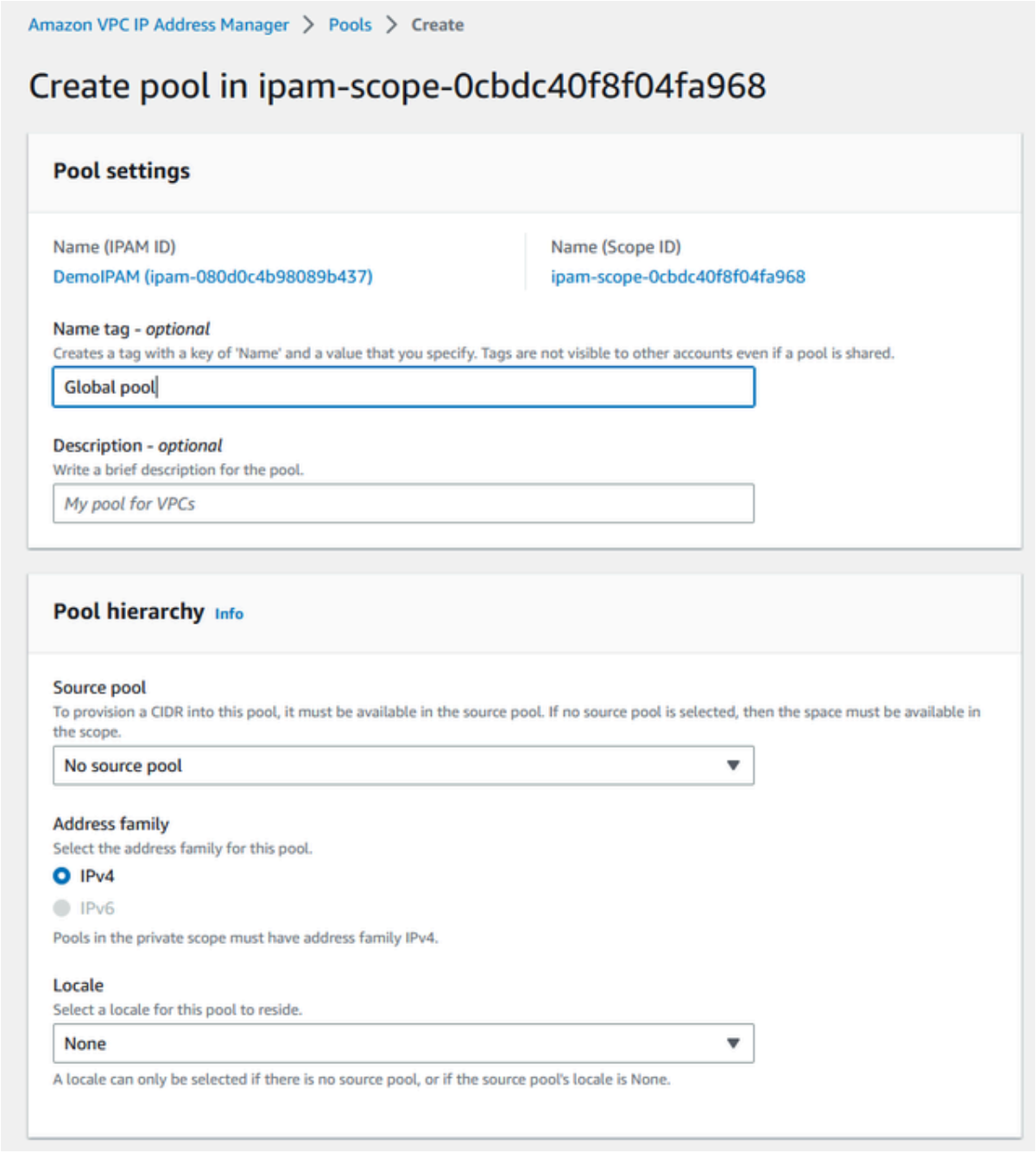
Para criar um grupo de nível superior

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.

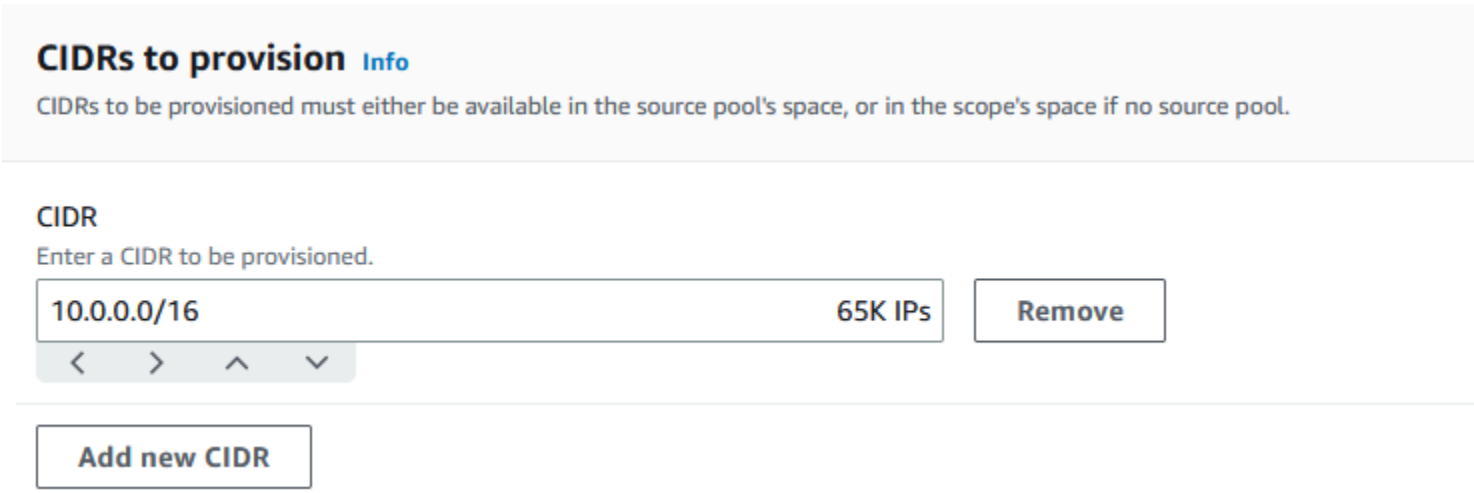
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado.



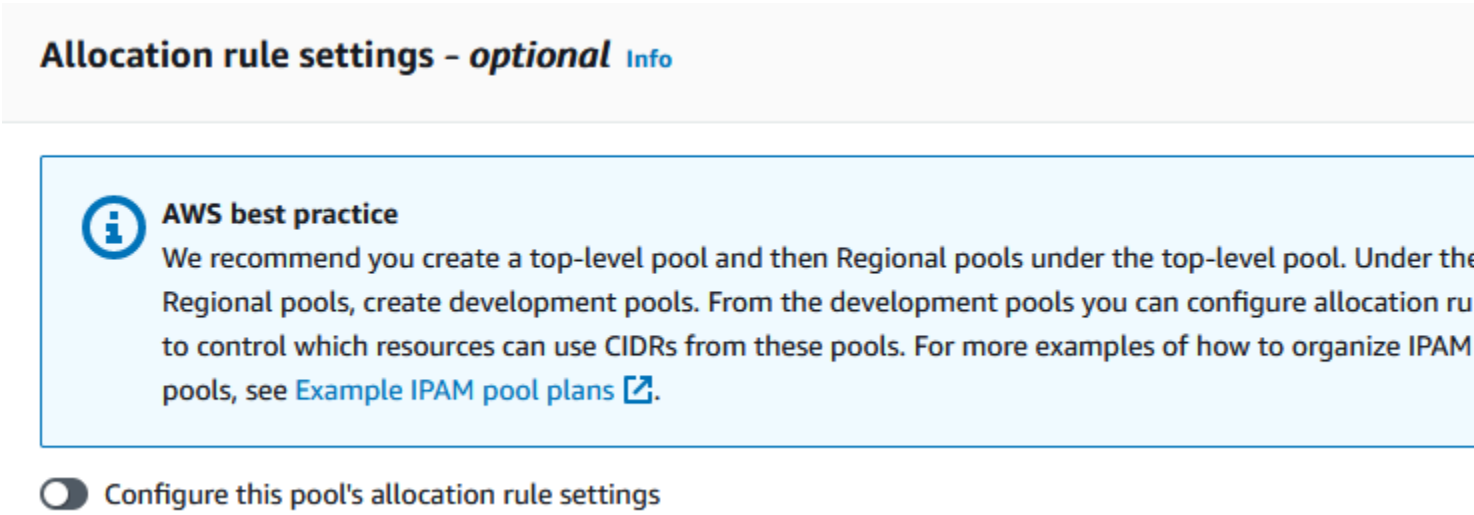
4. Selecione Criar.
5. Em Escopo do IPAM, deixe o escopo privado selecionado.
6. (Opcional) Adicionar uma Tag de nome e uma descrição para o grupo, por exemplo, “Grupo global”.
7. Em Tipo de origem, escolha Escopo do IPAM. Como esse é nosso grupo de nível superior, ele não terá um grupo de origem.
8. Em Address family (Família de endereços), escolha IPv4.
9. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
10. Para Locale (Localidade), escolha None (Nenhum). Localidades são as regiões da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. Você definirá a localidade para os grupos regionais que criar na próxima seção deste tutorial.



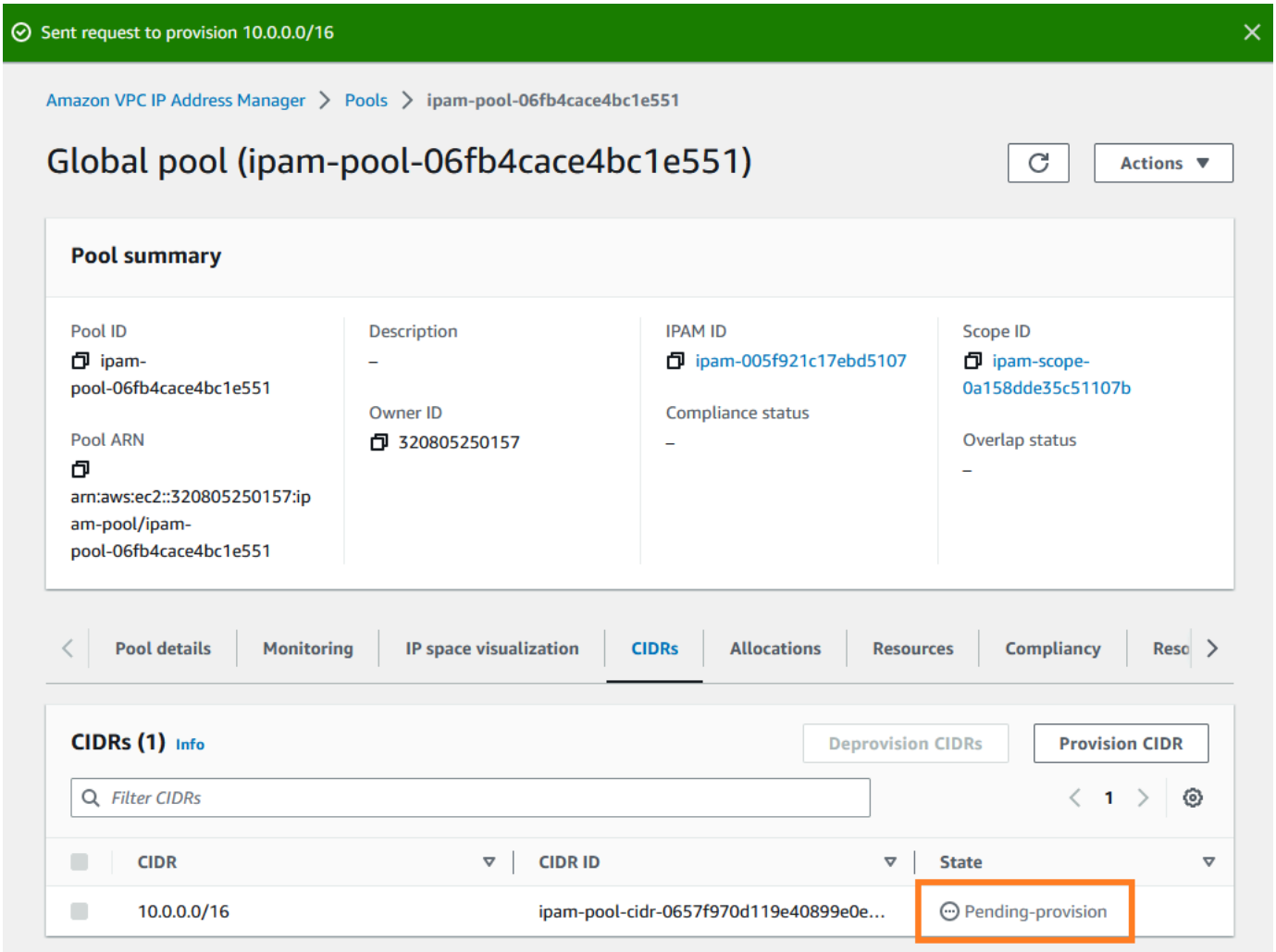
11. Escolha um CIDR para provisionar para o grupo. Neste exemplo, provisionamos 10.0.0.0/16.



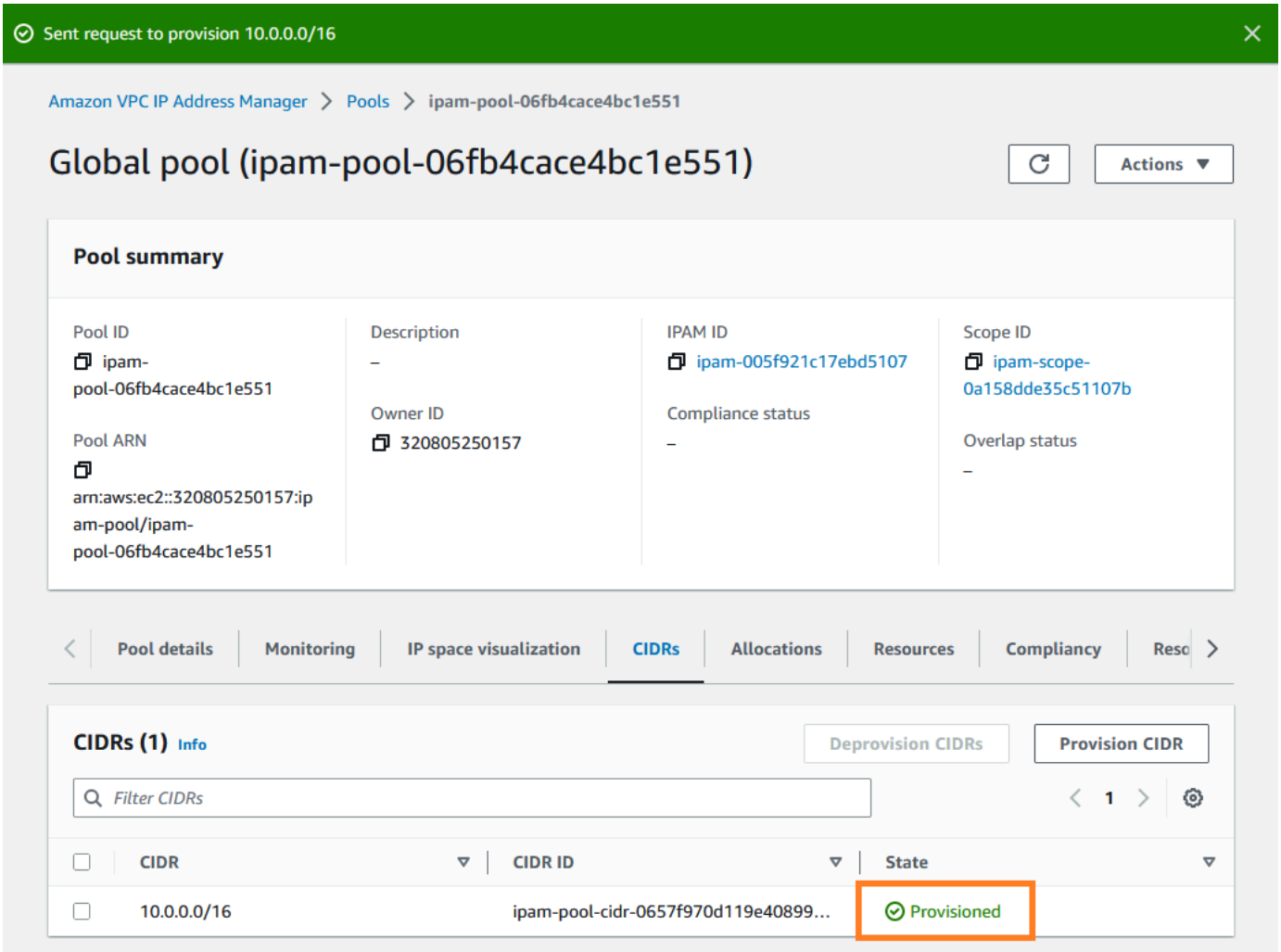
12. Deixe a opção Definir as configurações da regra de alocação deste grupo desativada. Esse é o nosso grupo de nível superior, e você não alocará CIDRs para as VPCs diretamente nesse grupo. Em vez disso, você os alocará em um subgrupo criado nesse grupo.



13. Selecione Criar. O grupo é criado e o CIDR está em um estado de Provisão pendente:



14. Aguarde até que o estado seja Provisionado antes de prosseguir para a próxima etapa.



Agora que o seu grupo de nível superior foi criado, você criará grupos regionais em us-west-1 e us-west-2.

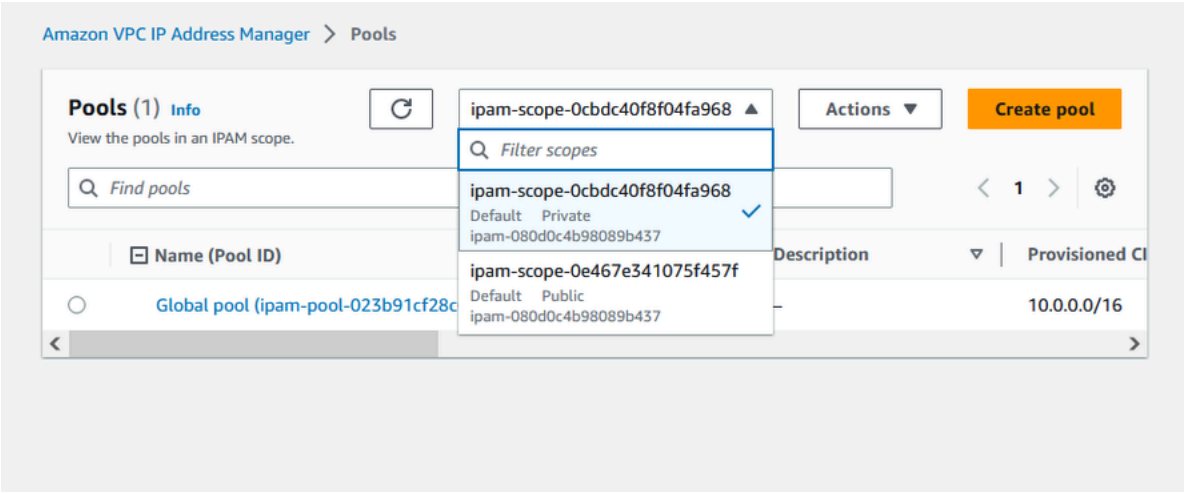
Etapa 4: criar grupos regionais do IPAM

Esta seção mostra como organizar os endereços IP usando dois grupos regionais. Neste tutorial, estamos seguindo um dos exemplos de planos de grupo do IPAM e criando dois grupos regionais que podem ser usados pelas contas dos membros em sua organização para alocar CIDRs para suas VPCs.

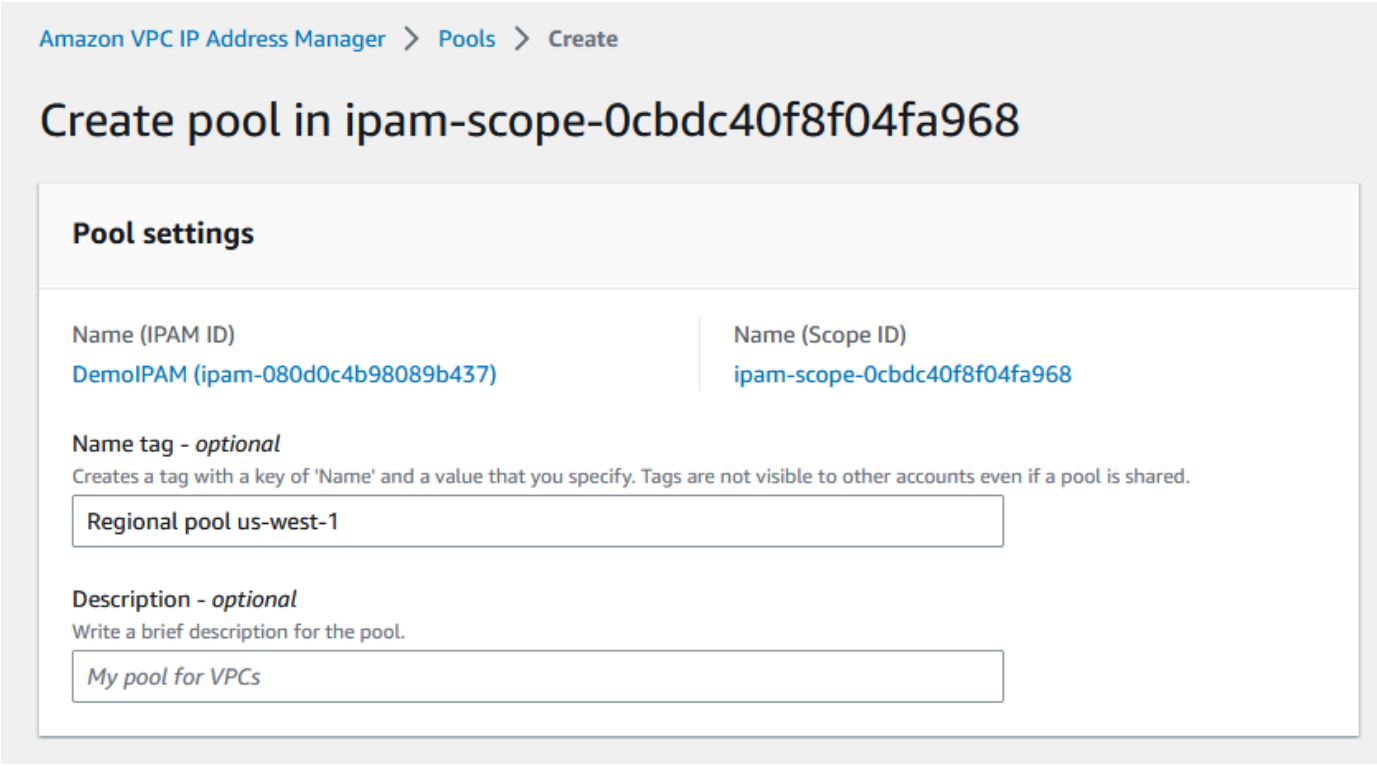
Para criar um grupo regional

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.

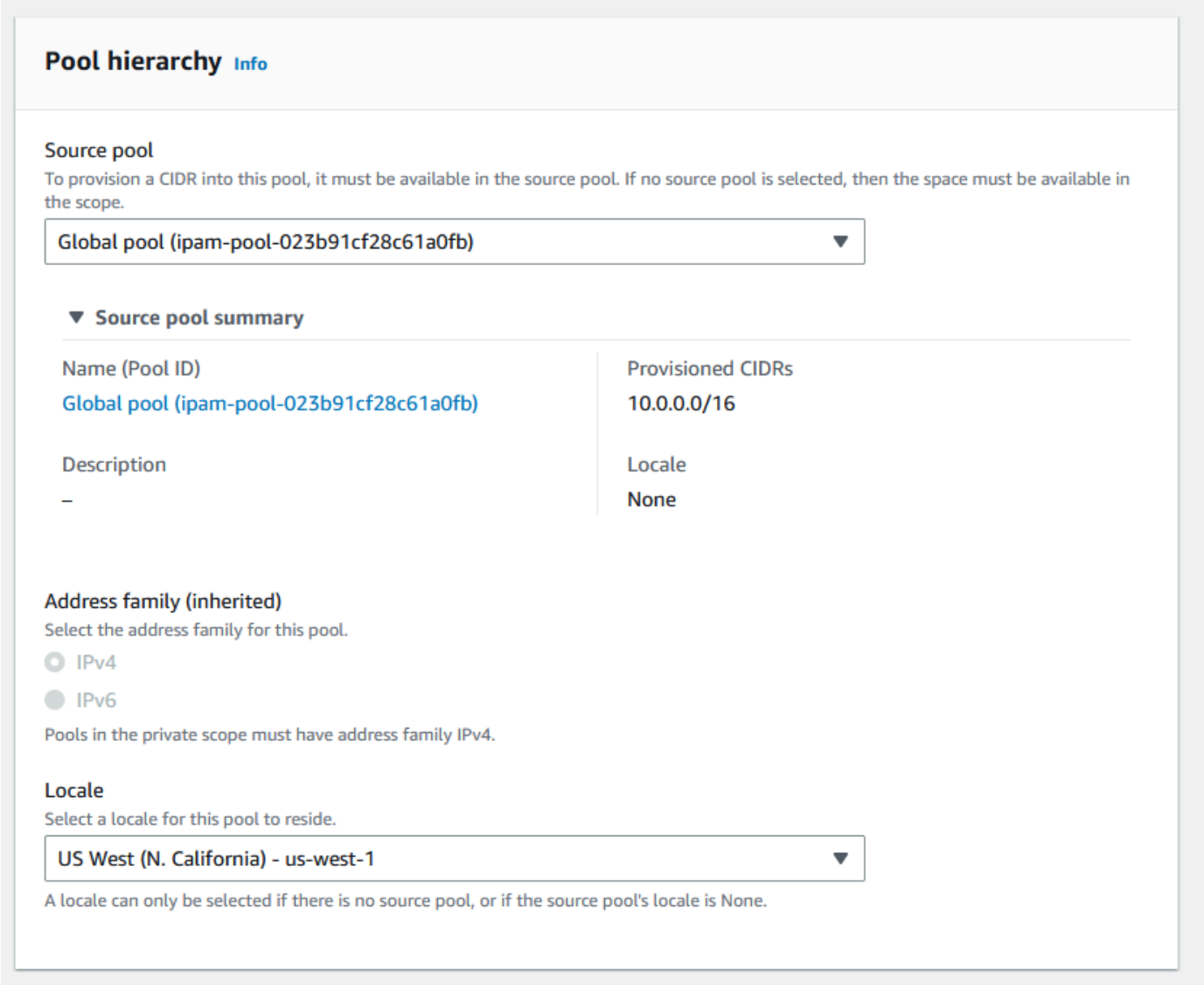
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado.



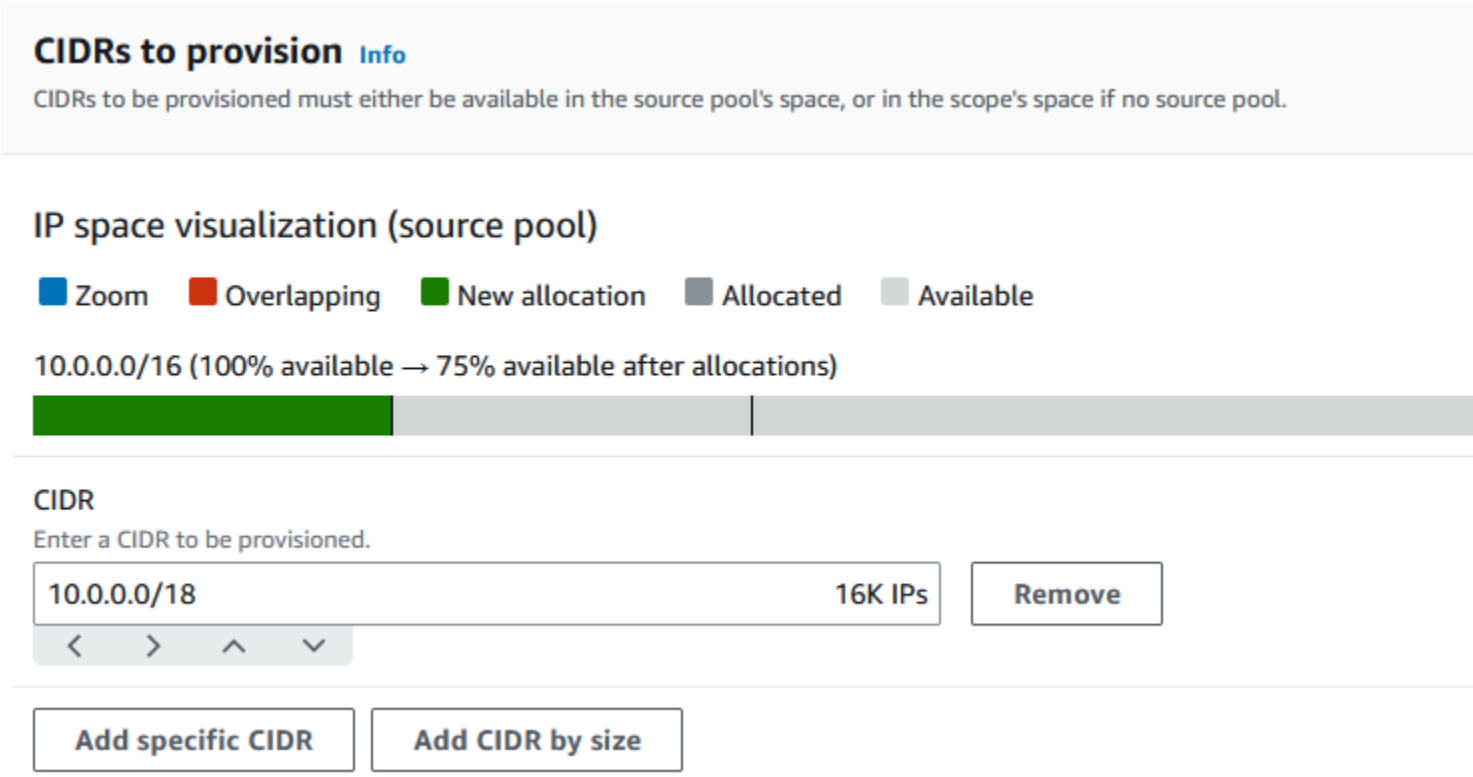
4. Selecione Criar.
5. Em Escopo do IPAM, deixe o escopo privado selecionado.
6. (Opcional) Adicione uma Tag de nome e uma descrição para o grupo, por exemplo, Grupo regional us-west-1.



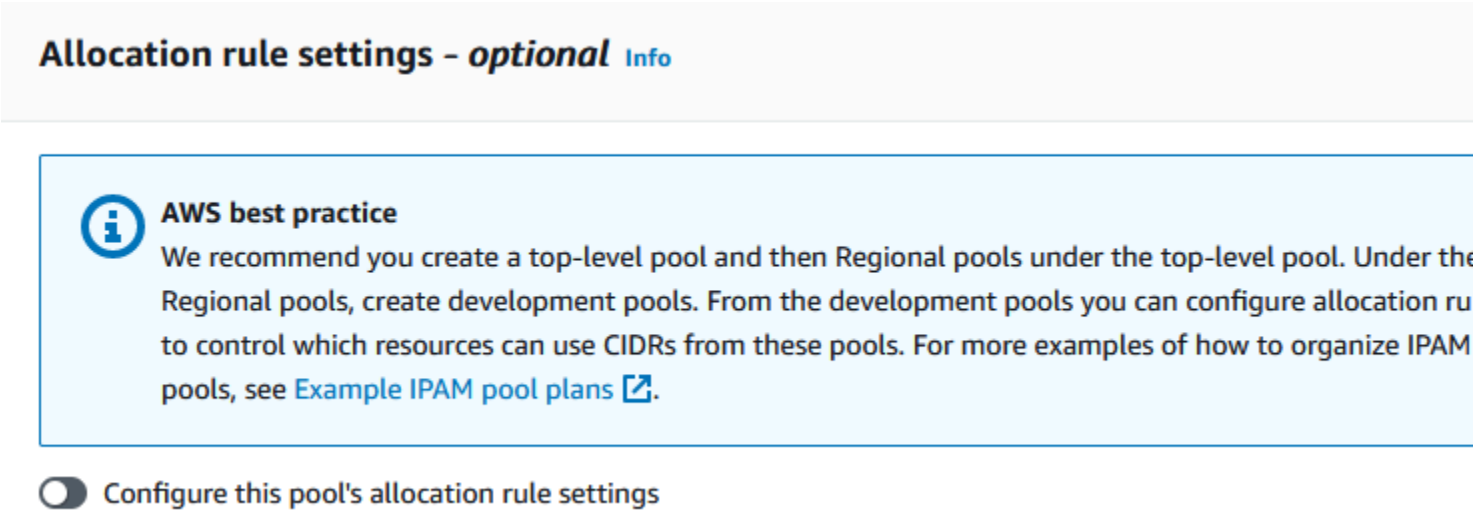
7. Em Tipo de origem, selecione Grupo do IPAM selecione o grupo de nível superior (“Grupo global”) criado em Etapa 3: criar um grupo do IPAM de nível superior. Em seguida, em Localidade, escolha us-west-1.



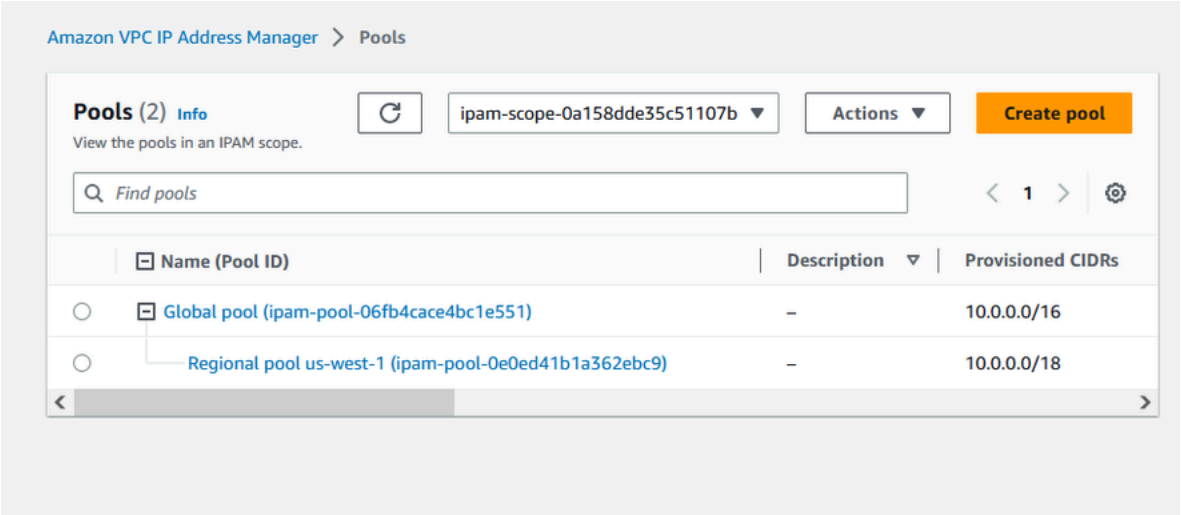
8. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
9. Em CIDRs para provisão, insira 10.0.0.0/18, que fornecerá a esse grupo cerca de 16.000 endereços IP disponíveis.



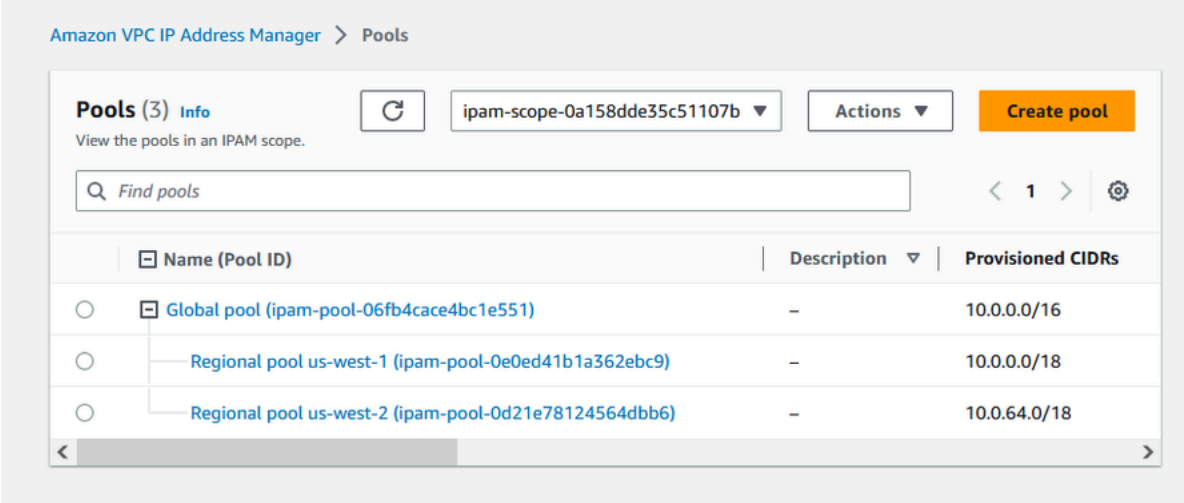
10. Deixe a opção Definir as configurações da regra de alocação deste grupo desativada. Você não alocará CIDRs para as VPCs diretamente desse grupo. Em vez disso, você os alocará em um subgrupo criado nesse grupo.



11. Selecione Criar.
12. Retorne à visualização de Grupos para ver a hierarquia dos grupos do IPAM criados.



13. Repita as etapas nesta seção e crie um segundo grupo regional na localidade us-west-2 com o CIDR 10.0.64.0/18 provisionado para ele. Ao concluir esse processo, você terá três grupos em uma hierarquia semelhante a esta:

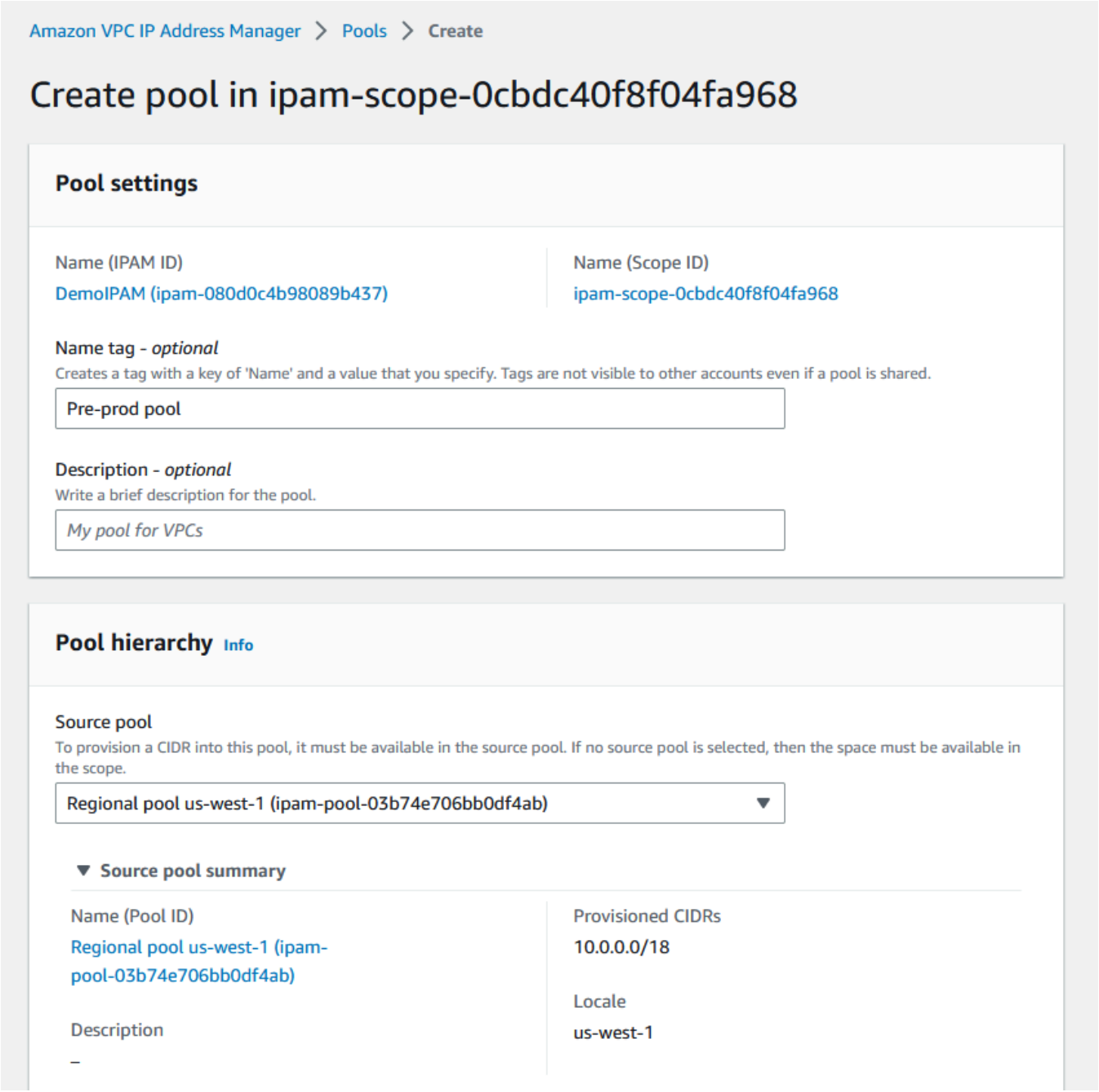


Etapa 5: criar um grupo de desenvolvimento pré-produção

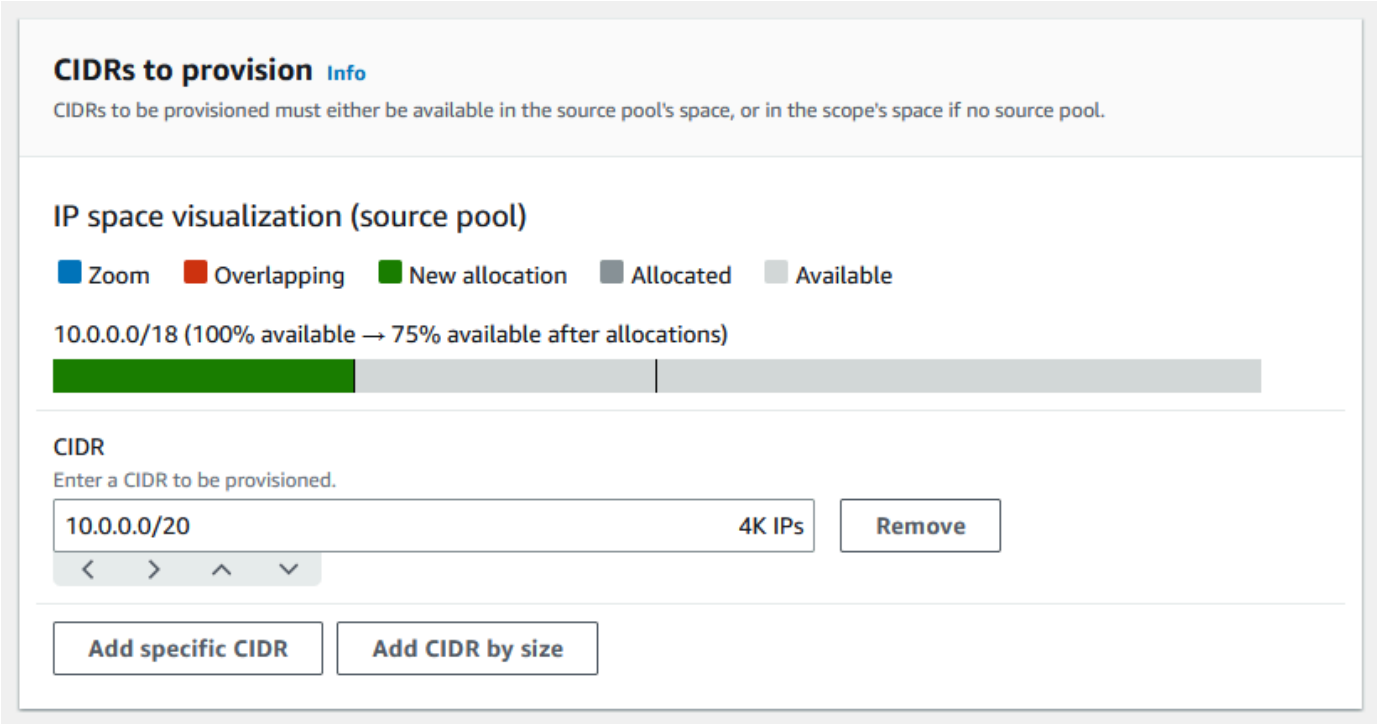
Siga as etapas desta seção para criar um grupo de desenvolvimento para recursos de pré-produção em um dos seus grupos regionais.

Para criar um grupo de desenvolvimento de pré-produção

1. Da mesma forma que você fez na seção anterior, usando a conta de administrador do IPAM, crie um grupo chamado Grupo de pré-produção, mas desta vez use o Grupo regional us-west-1 como o grupo de origem.

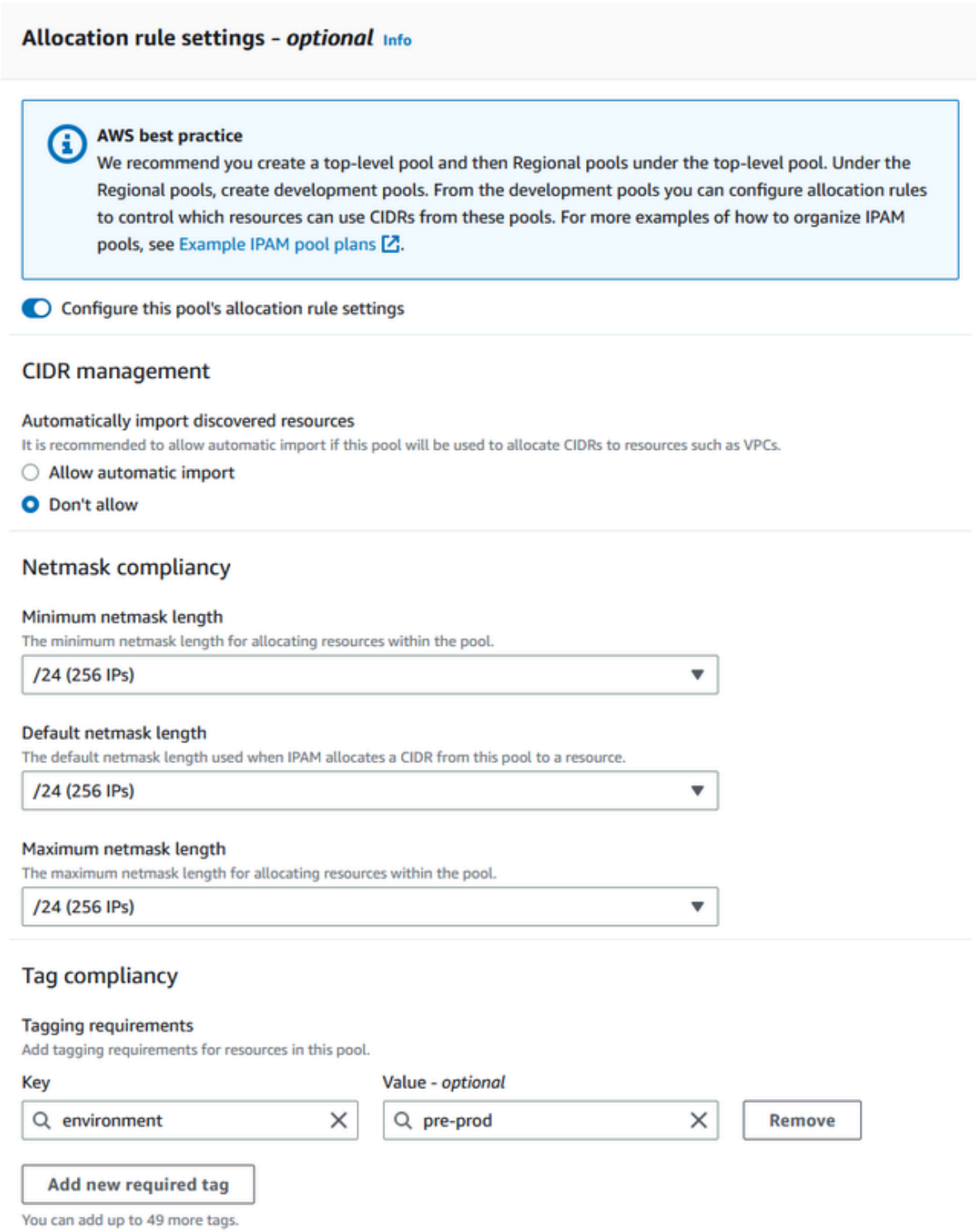


2. Especifique um CIDR de 10.0.0.0/20 para provisionar, o que fornecerá a esse grupo cerca de 4.000 endereços IP.

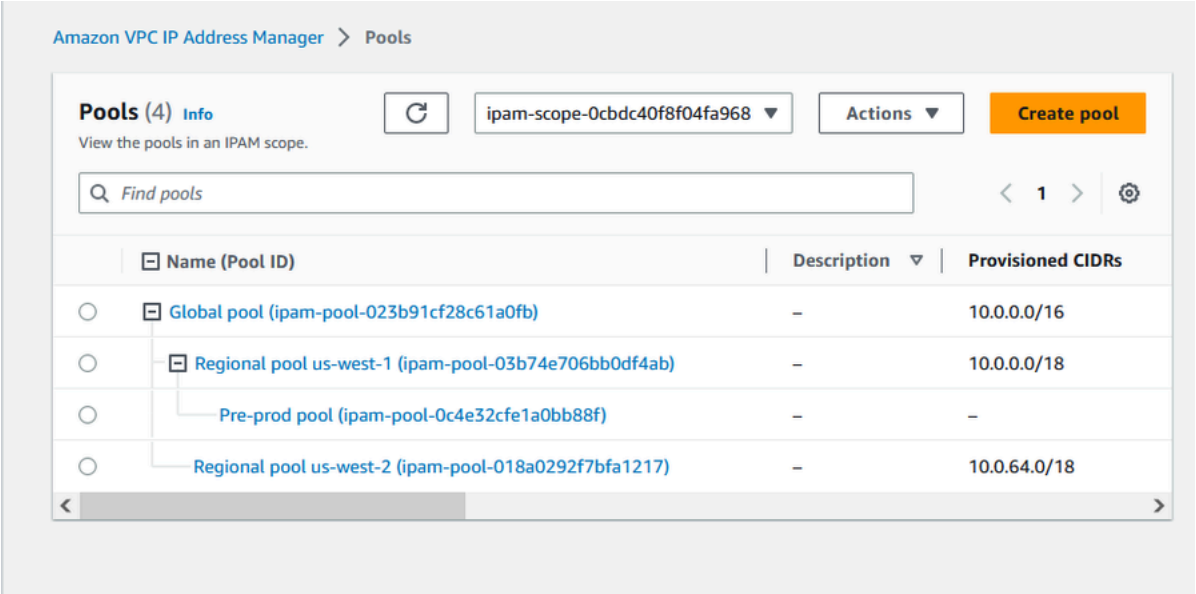


3. Alterne a opção para Definir as configurações da regra de alocação deste grupo. Faça o seguinte:

   1. Em Gerenciamento do CIDR, em Importar automaticamente recursos descobertos, deixe selecionada a opção padrão Não permitir. Essa opção permitirá que o IPAM importe automaticamente os CIDRs de recursos descobertos no local do grupo. Uma descrição detalhada dessa opção está fora do escopo deste tutorial, mas você pode ler mais sobre a opção em Criar um grupo de IPv4 de nível superior.
   2. Em Conformidade da máscara de rede, escolha /24 para o comprimento mínimo, padrão e máximo da máscara de rede. Uma descrição detalhada dessa opção está fora do escopo deste tutorial, mas você pode ler mais sobre a opção em Criar um grupo de IPv4 de nível superior. É importante observar que a VPC criada posteriormente com um CIDR nesse grupo será limitada a /24 com base no que definimos aqui.
   3. Em Conformidade de tags, insira ambiente/pré-produção. Essa tag será necessária para que as VPCs aloquem espaço no grupo. Posteriormente, demonstraremos como isso funciona.



4. Selecione Criar.
5. A hierarquia do grupo agora inclui um subgrupo adicional no Grupo regional us-west-1:



Agora você pode compartilhar o grupo do IPAM com outra conta de membro em sua organização e permitir que essa conta aloque um CIDR do grupo para criar uma VPC.

Etapa 6: compartilhar o grupo do IPAM

Siga as etapas nesta seção para compartilhar o grupo do IPAM de pré-produção usando o AWS Resource Access Manager (RAM).

Esta seção consiste em duas subseções:

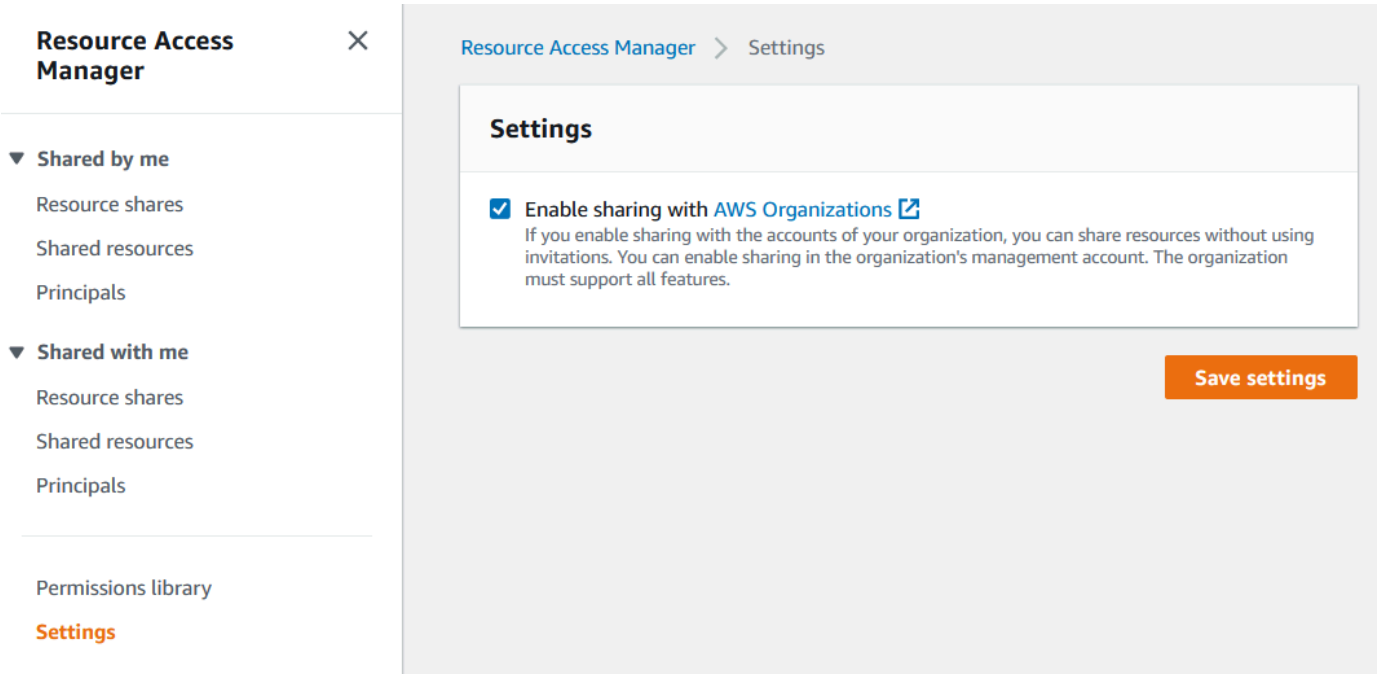
- Etapa 6.1. Habilitar o compartilhamento de recursos no AWS RAM: esta etapa deve ser realizada pela conta de gerenciamento do AWS Organizations.
- Etapa 6.2. Compartilhar um grupo do IPAM usando o AWS RAM: esta etapa deve ser realizada pelo administrador do IPAM.

Etapa 6.1. Habilitar o compartilhamento de recursos no AWS RAM

Depois de criar seu IPAM, você desejará compartilhar grupos de endereços IP com outras contas em sua organização. Antes de compartilhar um grupo do IPAM, conclua as etapas nesta seção para habilitar o compartilhamento de recursos com o AWS RAM.

Para habilitar o compartilhamento de recursos

1. Com a conta de gerenciamento do AWS Organizations, abra o console do AWS RAM em https://console.aws.amazon.com/ram/.
2. No painel de navegação esquerdo, escolha Configurações, depois Habilitar compartilhamento com o AWS Organizations e escolha Salvar configurações.



Agora você pode compartilhar um grupo do IPAM com outros membros da organização.

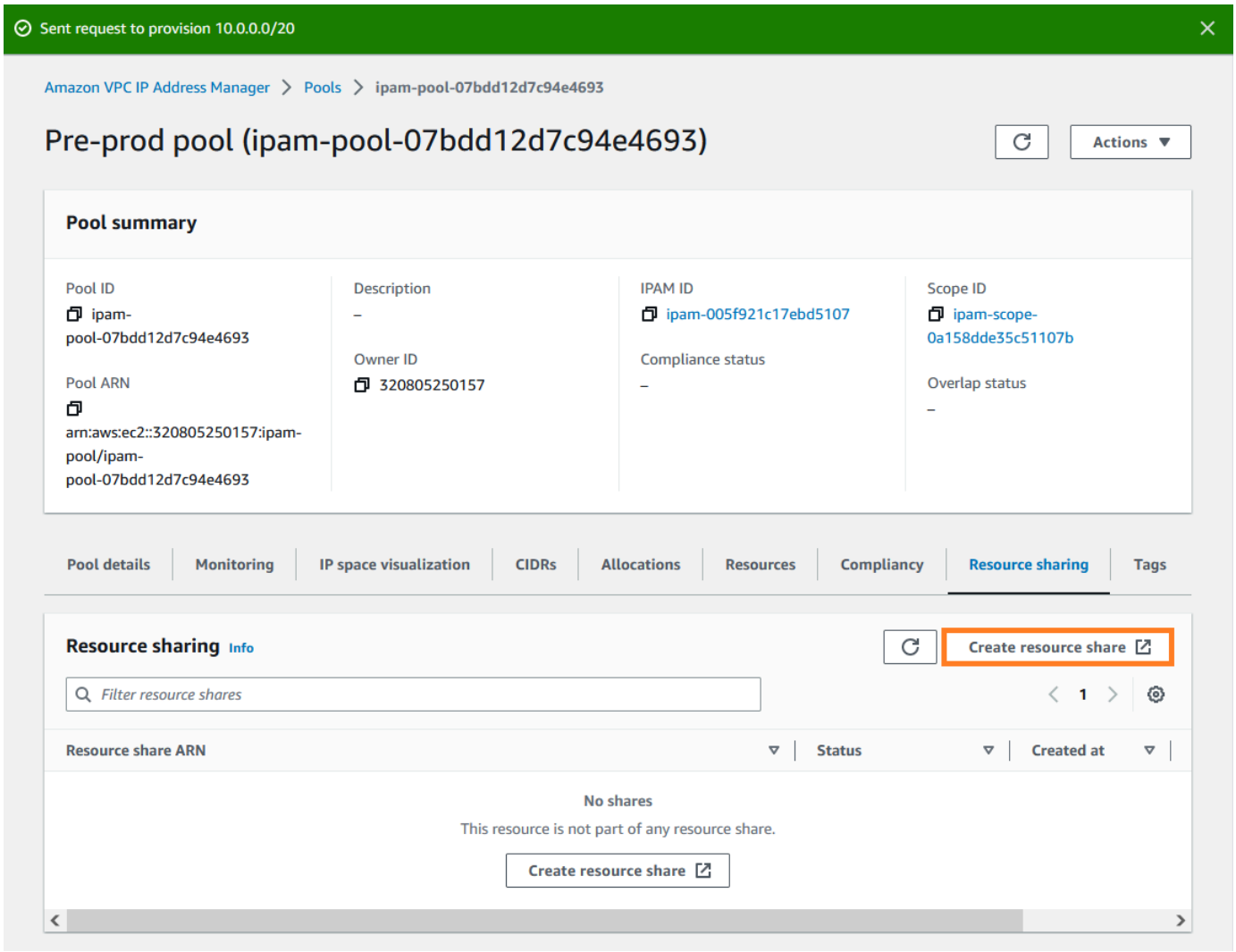
Etapa 6.2. Compartilhar um grupo do IPAM usando o AWS RAM

Nesta seção, você compartilhará o grupo de desenvolvimento de pré-produção com outra conta de membro do AWS Organizations. Para obter instruções completas sobre o compartilhamento de grupos do IPAM, incluindo informações sobre as permissões necessárias do IAM, consulte Compartilhar um grupo do IPAM usando o AWS RAM.

Para compartilhar um grupo do IPAM usando o AWS RAM

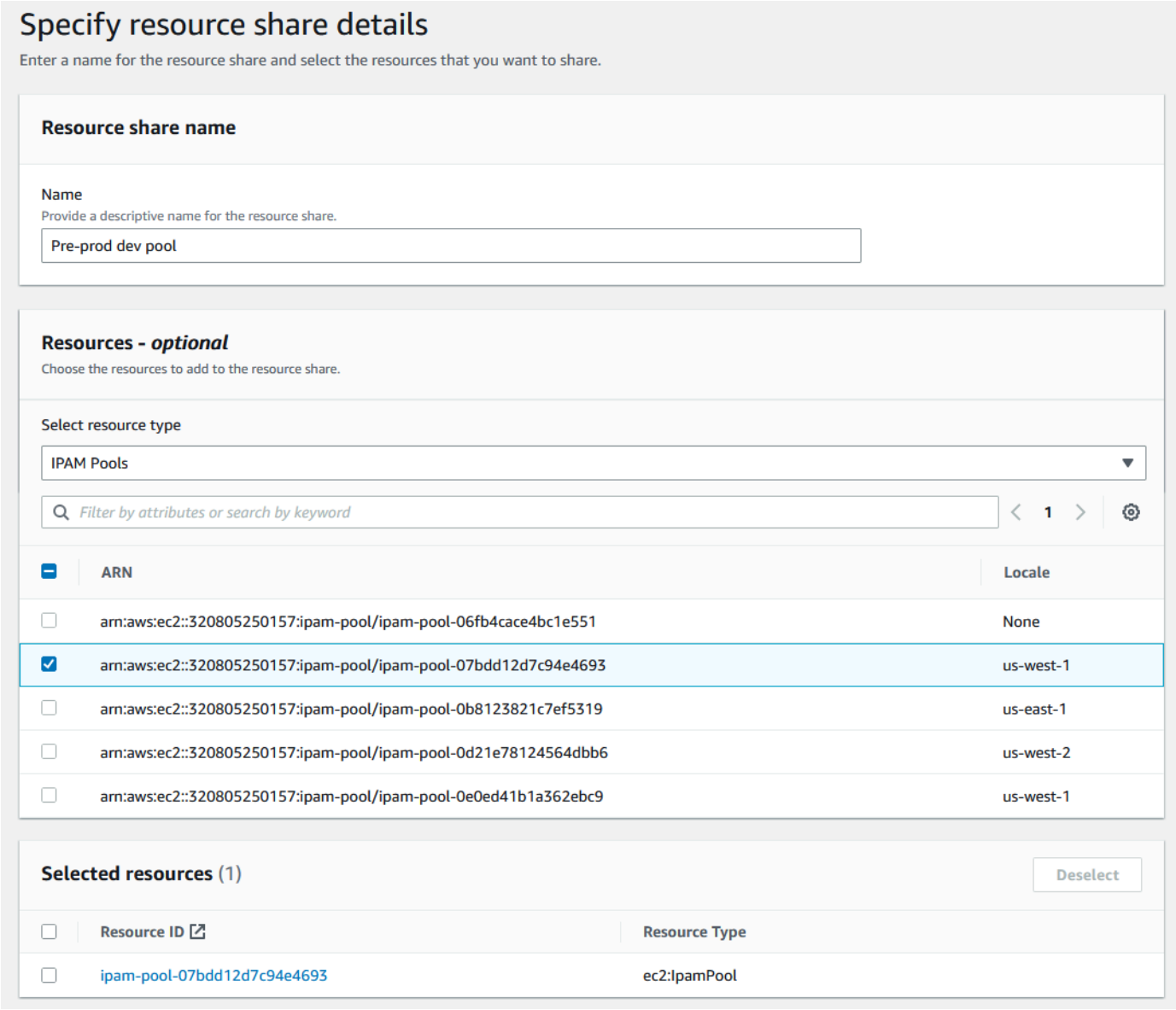
1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado, o grupo do IPAM de pré-produção e Ações > Visualizar detalhes.

4. Em Resource sharing (Compartilhamento de recursos), escolha Create resource share (Criar compartilhamento de recursos). O console do AWS RAM será aberto. Você compartilhará o grupo usando o AWS RAM.
5. Escolha Create a resource share (Criar um compartilhamento de recursos).

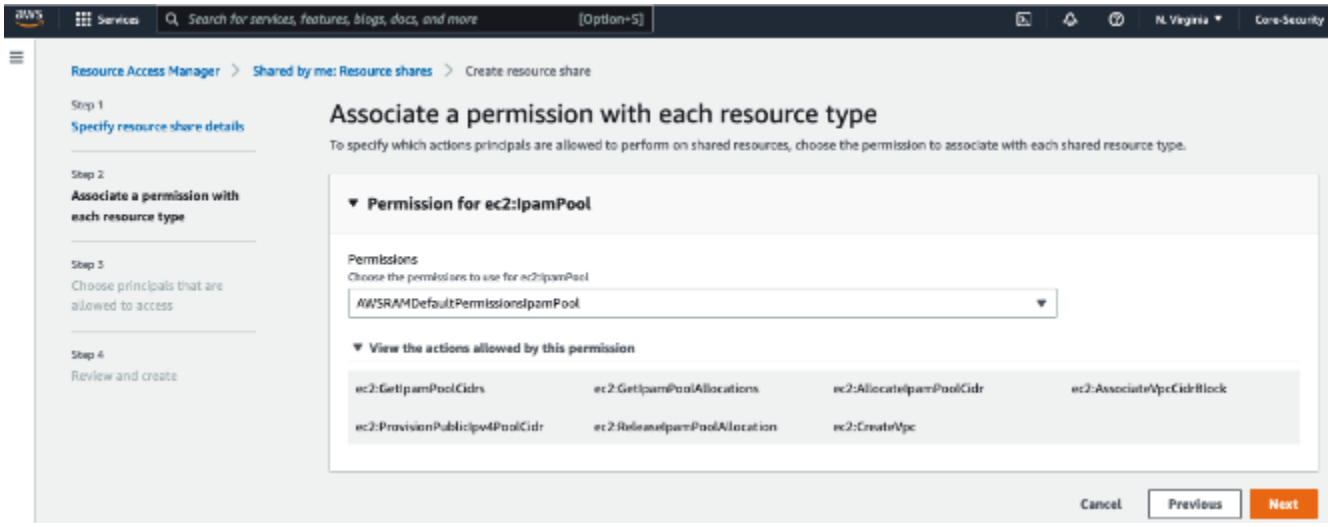


O console do AWS RAM será aberto.

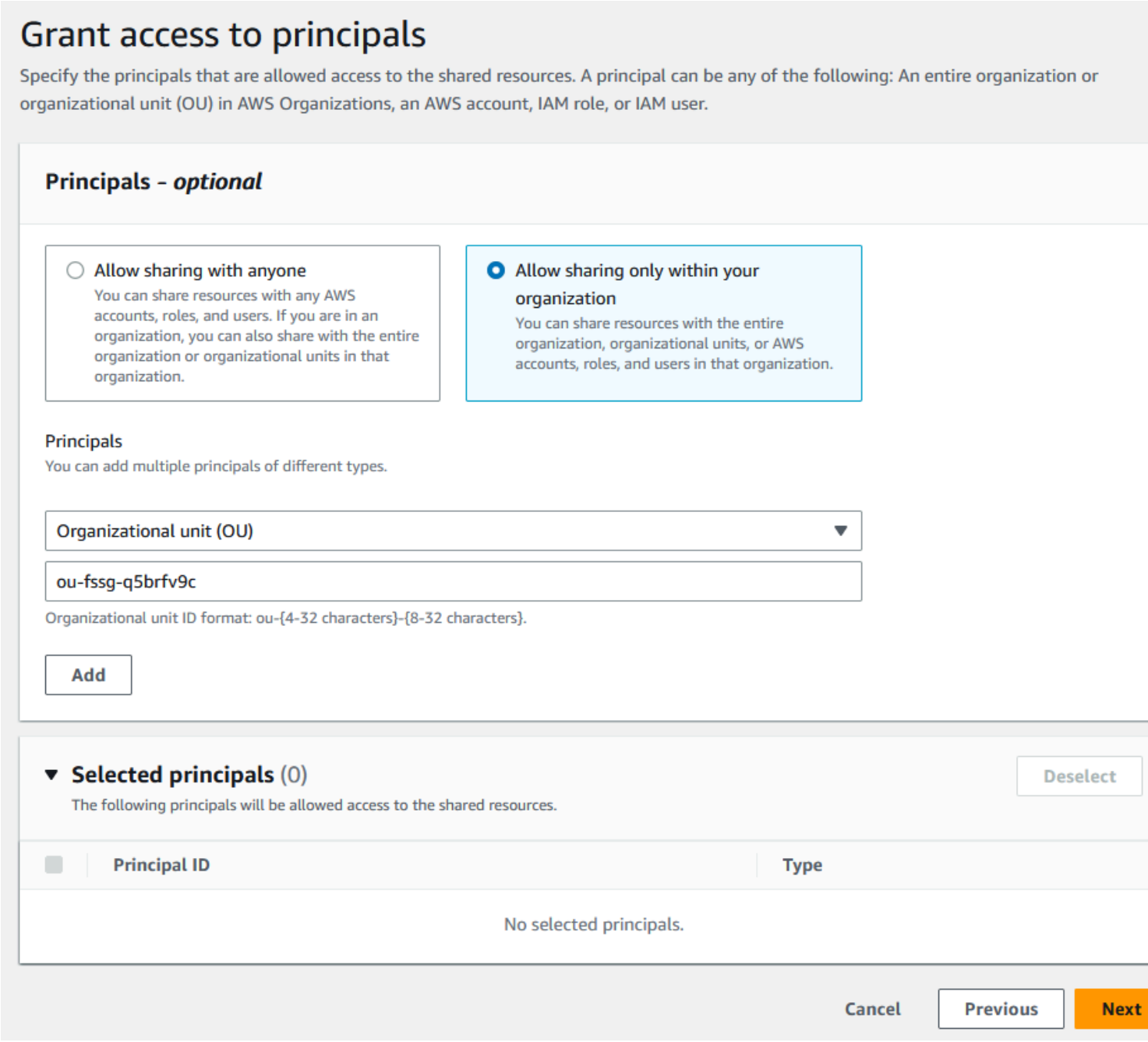
6. No console do AWS RAM, escolha Criar um compartilhamento de recursos novamente.
7. Adicione um Nome para o recurso compartilhado.
8. Em Selecionar tipo de recurso, escolha Grupos do IPAM e, em seguida, escolha o ARN do grupo de desenvolvimento de pré-produção.



9. Escolha Próximo.
10. Deixe a permissão padrão AWSRAMDefaultPermissionsIpamPool selecionada. Os detalhes das opções de permissão estão fora do escopo deste tutorial, mas você pode descobrir mais sobre essas opções em Compartilhar um grupo do IPAM usando o AWS RAM.



11. Escolha Próximo.
12. Em Entidades principais, escolha Permitir compartilhamento somente dentro da sua organização. Insira o ID da sua da unidade organizacional do AWS Organizations (conforme mencionado em Como o AWS Organizations se integra ao IPAM) e escolha Adicionar.



13. Escolha Próximo.
14. Revise as opções de compartilhamento de recursos e as entidades principais com as quais você compartilhará e escolha Criar.

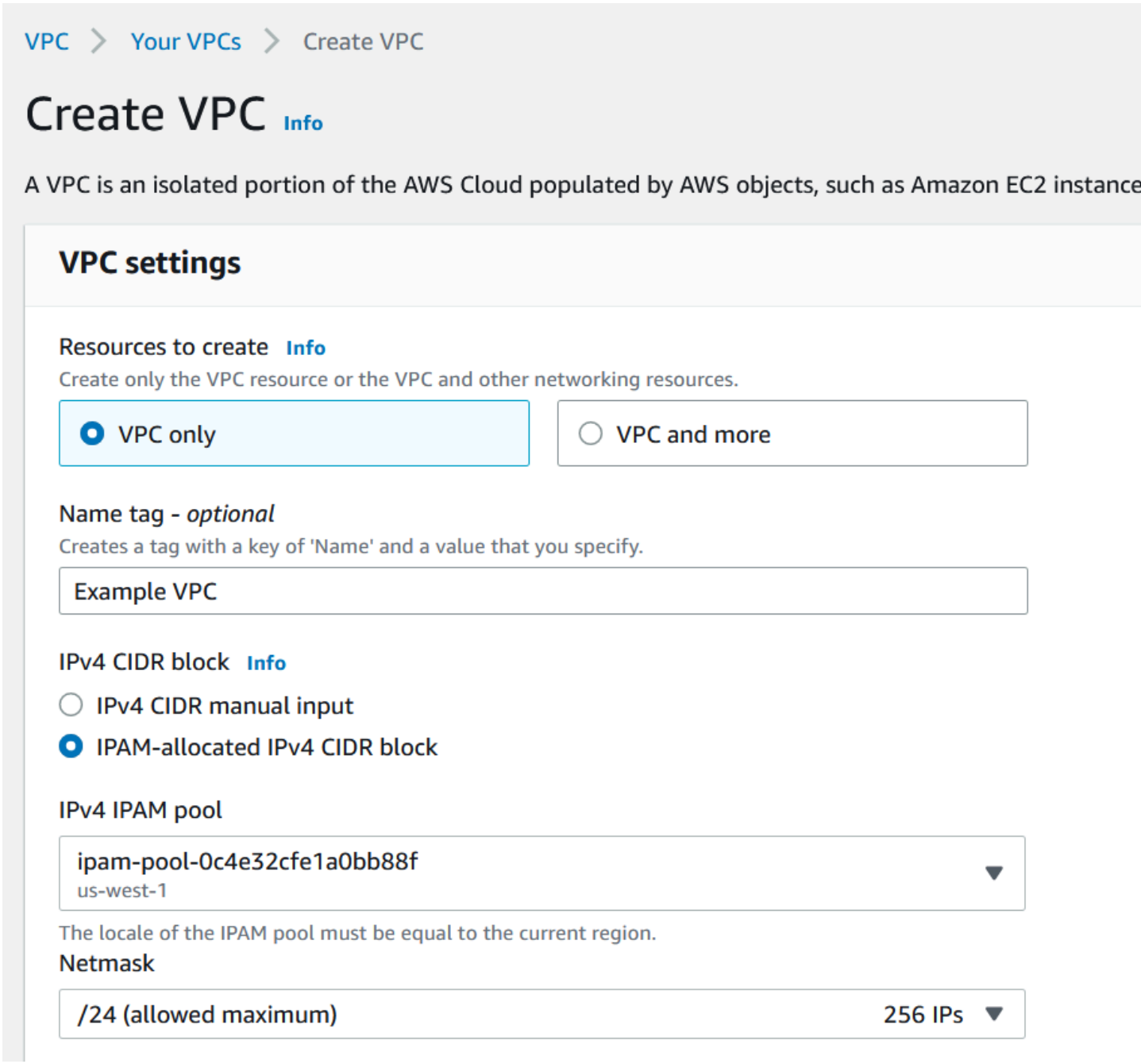
Agora que o grupo foi compartilhado, vá para a próxima etapa para criar uma VPC com um CIDR alocado em um grupo do IPAM.

Etapa 7: criar uma VPC com um CIDR alocado em um grupo do IPAM

Siga as etapas nesta seção para criar uma VPC com um CIDR alocado no grupo de pré-produção. Essa etapa deve ser concluída pela conta de membro na UO com a qual o grupo do IPAM foi compartilhado na seção anterior (chamada example-member-account-2 em Como o AWS Organizations se integra ao IPAM). Para obter mais informações sobre as permissões do IAM necessárias para criar VPCs, consulte exemplos de políticas da Amazon VPC no Guia do usuário da Amazon VPC.

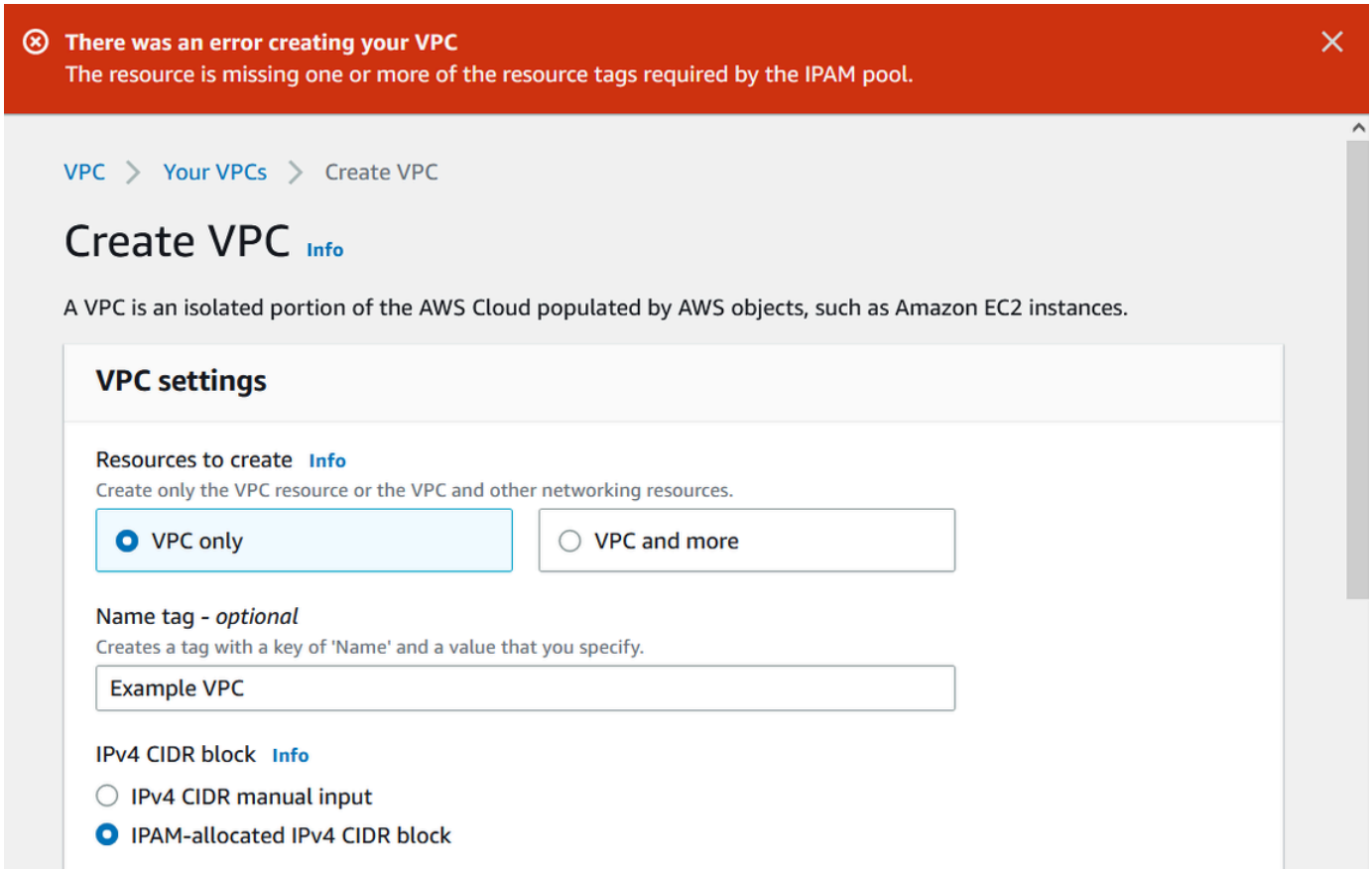
Para criar uma VPC com um CIDR alocado em um grupo do IPAM

1. Com a conta de membro, acesse o console da VPC em https://console.aws.amazon.com/vpc/ como a conta de membro que será usada como a conta de desenvolvedor.
2. Escolha Criar VPC.
3. Faça o seguinte:
    1. Insira um nome, como Exemplo de VPC.
    2. Escolha o bloco CIDR IPv4 alocado pelo IPAM.
    3. Em Grupo IPv4 do IPAM, escolha o ID do grupo de pré-produção.
    4. Escolha um comprimento de Máscara de rede. Como você limitou o comprimento da máscara de rede disponível para esse grupo a /24 (em Etapa 5: criar um grupo de desenvolvimento pré-produção), a única opção de máscara de rede disponível é /24.

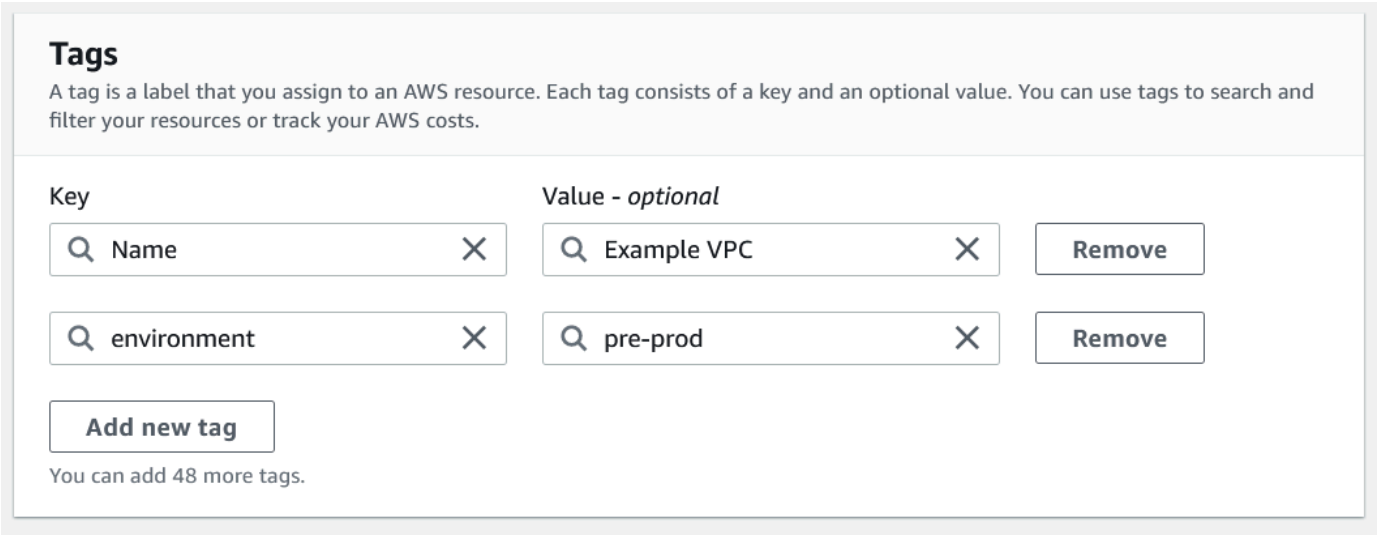


4. Para fins de demonstração, em Tags, não adicione nenhuma tag adicional no momento. Ao criar o grupo de pré-produção (em Etapa 5: criar um grupo de desenvolvimento pré-produção), você adicionou uma regra de alocação que exigia que todas as VPCs criadas com CIDRs nesse grupo tivessem uma tag de ambiente/pré-produção. Deixe a tag de ambiente/pré-produção desativada por enquanto para que você possa ver que aparece um erro informando que uma tag necessária não foi adicionada.
5. Escolha Criar VPC.

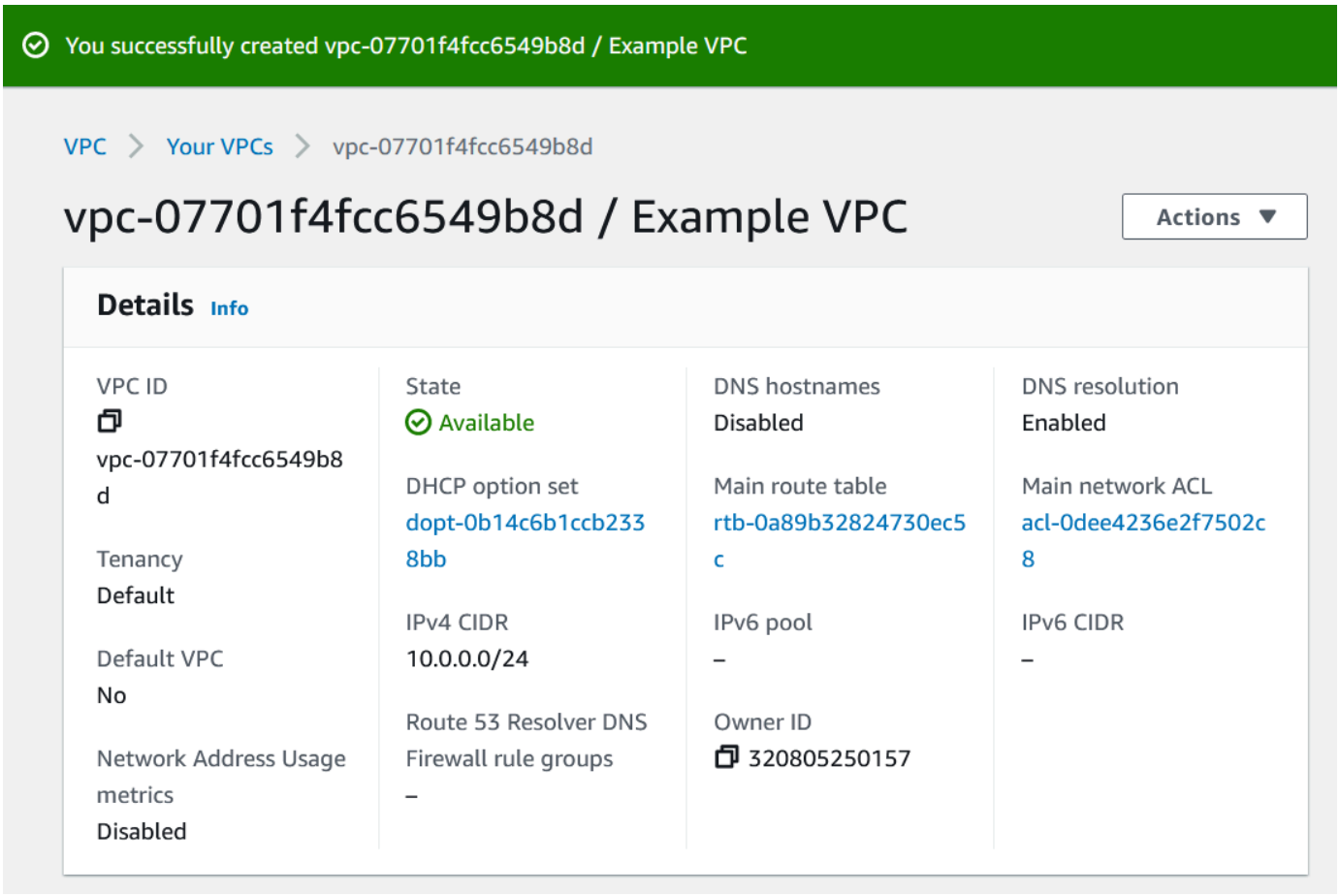
6. Aparece um erro informando que uma tag necessária não foi adicionada. O erro aparece porque você definiu uma regra de alocação ao criar o grupo de pré-produção (em Etapa 5: criar um grupo de desenvolvimento pré-produção). A regra de alocação exigia que todas as VPCs criadas com CIDRs nesse grupo tivessem uma tag de ambiente/pré-produção.



7. Agora, em Tags, adicione a tag ambiente/pré-produção e escolha Criar VPC novamente.



8. A VPC é criada com sucesso e está em conformidade com a regra de tag no grupo de pré-produção:



No painel Recursos do console do IPAM, o administrador do IPAM poderá ver e gerenciar a VPC e seu CIDR alocado. Observe que a VPC leva algum tempo para aparecer no painel Recursos.

Etapa 8: limpeza

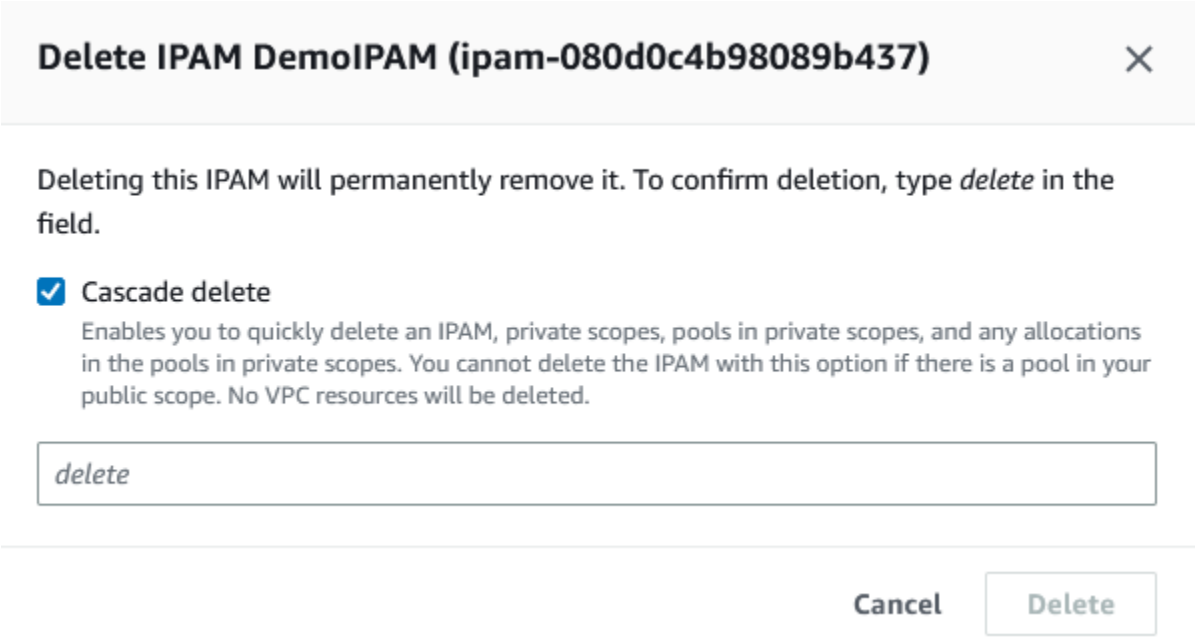
Neste tutorial, você criou um IPAM com um administrador delegado, criou vários grupos e habilitou uma conta de membro em sua organização para alocar um CIDR da VPC em um grupo.

Siga as etapas desta seção para limpar os recursos criados neste tutorial.

Para limpar os recursos criados neste tutorial

1. Usando a conta de membro que criou a VPC de exemplo, exclua a VPC. Para obter instruções detalhadas, consulte Excluir sua VPC no Guia do usuário da Amazon Virtual Private Cloud.

2. Com a conta de administrador do IPAM, exclua o exemplo de compartilhamento de recursos no console do AWS RAM. Para obter instruções detalhadas, consulte Excluir um compartilhamento de recursos no AWSAWS RAM no Guia do usuário do AWS Resource Access Manager.
3. Usando a conta de administrador do IPAM, faça login no console do RAM e desative o compartilhamento com o AWS Organizations que você habilita em Etapa 6.1. Habilitar o compartilhamento de recursos no AWS RAM.
4. Use a conta de administrador do IPAM e exclua o exemplo de IPAM ao selecionar o IPAM no console do IPAM e escolher Ações > Excluir. Para ter instruções detalhadas, consulte Excluir um IPAM.
5. Quando for solicitada a exclusão do IPAM, escolha Excluir em cascata. Isso excluirá todos os escopos e grupos dentro do IPAM antes de excluir o IPAM.



6. Insira excluir e escolha Excluir.
7. Usando a conta de gerenciamento do AWS Organizations, faça login no console do IPAM, escolha Configurações e remova a conta de administrador delegado.
8. (Opcional) Quando você integra o IPAM ao AWS Organizations, o IPAM cria automaticamente um perfil vinculado ao serviço em cada conta de membro. Usando cada uma das contas de membro do AWS Organizations, faça login no IAM e exclua o perfil vinculado ao serviço AWSServiceRoleForIPAM em cada uma delas.
9. A limpeza está completa.

Tutorial: criar um IPAM e grupos usando a AWS CLI

Siga as etapas neste tutorial para usar a AWS CLI para criar um IPAM, criar grupos de endereço IP e alocar uma VPC com um CIDR em um grupo do IPAM.

O exemplo a seguir mostra a hierarquia da estrutura de grupos que você criará seguindo as etapas nesta seção.

- IPAM operando na região da AWS 1, região da AWS 2
  - Escopo privado
    - Grupo de nível superior
      - Grupo regional na região da AWS 2
        - Grupo de desenvolvimento
          - Alocação para uma VPC

> **Note**
>
> Nesta seção, você cria um IPAM. Por padrão, é possível criar apenas um IPAM. Para obter mais informações, consulte Cotas para o IPAM. Se você já delegou uma conta do IPAM e criou um IPAM, você poderá ignorar as etapas 1 e 2.

Conteúdo

- Etapa 1: habilitar o IPAM na sua organização
- Etapa 2: criar um IPAM
- Etapa 3: criar um grupo de endereços IPv4
- Etapa 4: provisionar um CIDR para o grupo de nível superior
- Etapa 5. Criar um grupo regional com o CIDR originado do grupo de nível superior
- Etapa 6: provisionar um CIDR para o grupo regional
- Etapa 7. Criar um compartilhamento do RAM para habilitar atribuições de IP nas contas
- Etapa 8. Crie uma VPC
- Etapa 9. Limpeza

Etapa 1: habilitar o IPAM na sua organização

Esta etapa é opcional. Conclua esta etapa para habilitar o IPAM em sua organização e configurar o IPAM delegado usando a AWS CLI. Para obter mais informações sobre a função da conta do IPAM, consulte Integrar o IPAM a contas em uma organização da AWS Organizations.

Essa solicitação deve ser feita a partir de uma conta de gerenciamento do AWS Organizations. Ao executar o seguinte comando, certifique-se de estar usando uma função com uma política do IAM que permita as seguintes ações:

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

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

Você deverá ver a saída a seguir, indicando que a habilitação foi bem-sucedida.

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

Etapa 2: criar um IPAM

Siga as etapas nesta seção para criar um IPAM e visualizar informações adicionais sobre os escopos criados. Você usará esse IPAM ao criar grupos e provisionar intervalos de endereços IP para esses grupos em etapas posteriores.

> **Note**
>
> A opção regiões operacionais determina para quais regiões da AWS os grupos do IPAM podem ser usados. Para ver mais informações sobre as regiões operacionais, consulte Criar um IPAM.

Para criar um IPAM usando a AWS CLI

1. Execute o comando a seguir para criar uma instância do IPAM.

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

   Quando você cria um IPAM, a AWS faz automaticamente o seguinte:

   - Retorna um ID de recurso exclusivo globalmente (`IpamId`) para o IPAM.
   - Cria um escopo público padrão (`PublicDefaultScopeId`) e um escopo privado padrão (`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. Execute o comando a seguir para visualizar informações adicionais relacionadas aos escopos. O escopo público é destinado a endereços IP que serão acessados por meio da Internet pública. O escopo privado é destinado a endereços IP que não serão acessados por meio da Internet pública.

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

Na saída, você vê os escopos disponíveis. Você usará o ID do escopo privado na próxima etapa.


```
{
    "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
        }
    ]
}
```


Etapa 3: criar um grupo de endereços IPv4

Siga as etapas nesta seção para criar um grupo de endereços IPv4.

> **Important**
>
> Você não usará a opção `--locale` neste grupo de nível superior. Você definirá a opção de localidade no grupo regional. A localidade é a região da AWS na qual você deseja que um grupo esteja disponível para alocações de CIDR. Como a localidade não está definida

no grupo de nível superior, o padrão será adotado None. Se um grupo tiver uma localidade None, não estará disponível para recursos da VPC em nenhuma região da AWS. Você só pode alocar manualmente o espaço de endereço IP no grupo para reservar espaço.

Para criar um grupo de endereços IPv4 para todos os seus recursos da AWS usando a AWS CLI

1. Execute o comando a seguir para criar um grupo de endereços IPv4. Use o ID do escopo privado do IPAM criado na etapa anterior.

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

   Na saída, você verá um estado de `create-in-progress` para o grupo.

```
{
    "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. Execute o comando a seguir até ver um estado `create-complete` na saída.

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

   O exemplo de saída a seguir mostra o estado correto.

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

Etapa 4: provisionar um CIDR para o grupo de nível superior

Siga as etapas desta seção para provisionar um CIDR para o grupo de nível superior e, em seguida, verificar se o CIDR está provisionado. Para obter mais informações, consulte Provisionar CIDRs para um grupo.

Para provisionar um bloco CIDR para o grupo usando o AWS CLI

1. Execute o comando a seguir para provisionar o CIDR.

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

   Na saída, você pode verificar o estado do provisionamento.

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

```
    }
}
```

2. Execute o comando a seguir até ver um estado `provisioned` na saída.

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

O exemplo de saída a seguir mostra o estado correto.

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

Etapa 5. Criar um grupo regional com o CIDR originado do grupo de nível superior

Ao criar um grupo do IPAM, o grupo pertence à região da AWS do IPAM por padrão. Quando você cria uma VPC, o grupo do qual a VPC extrai deverá estar na mesma região da VPC. Você pode usar a opção `--locale` ao criar um grupo para disponibilizá-lo para serviços em uma região diferente da região do IPAM. Siga as etapas nesta seção para criar um grupo regional em outra localidade.

Para criar um grupo com um CIDR originado do grupo anterior usando a AWS CLI

1. Execute o comando a seguir para criar o grupo e inserir espaço com um CIDR disponível conhecido do grupo anterior.

```
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
```

Na saída, você verá o ID do grupo criado. Você precisará desse ID na próxima etapa.

```
{
```

```
    "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. Execute o comando a seguir até ver um estado `create-complete` na saída.

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

Na saída, você vê os grupos que tem no IPAM. Neste tutorial, criamos um grupo regional e um de nível superior. Você verá ambos.

```
{
    "IpamPools": [
        {
            "OwnerId": "123456789012",
            "IpamPoolId": "ipam-pool-0008f25d7187a08d9",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0008f25d7187a08d9",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-065e7dfe880df679c",
            "IpamScopeType": "private",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
            "Locale": "None",
            "PoolDepth": 1,
            "State": "create-complete",
            "Description": "top-level-pool",
            "AutoImport": false,
```

```
            "AddressFamily": "ipv4"
        },
        {
            "OwnerId": "123456789012",
            "IpamPoolId": "ipam-pool-0da89c821626f1e4b",
            "SourceIpamPoolId": "ipam-pool-0008f25d7187a08d9",
            "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0da89c821626f1e4b",
            "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-065e7dfe880df679c",
            "IpamScopeType": "private",
            "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
            "Locale": "us-west-2",
            "PoolDepth": 2,
            "State": "create-complete",
            "Description": "regional--pool",
            "AutoImport": false,
            "AddressFamily": "ipv4"
        }
    ]
}
```

Etapa 6: provisionar um CIDR para o grupo regional

Siga as etapas desta seção para atribuir um bloco CIDR ao grupo e validar se ele foi provisionado com sucesso.

Para atribuir um bloco CIDR ao grupo regional usando a AWS CLI

1. Execute o comando a seguir para provisionar o CIDR.

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

   Na saída, você verá o estado do grupo.

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

```
}
```

2. Execute o comando a seguir até ver um estado `provisioned` na saída.

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

O exemplo de saída a seguir mostra o estado correto.

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

3. Execute o comando a seguir para consultar o grupo de nível superior e visualizar as alocações. O grupo regional é considerado uma alocação dentro do grupo de nível superior.

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

Na saída, você vê o grupo regional como uma alocação no grupo de nível superior.

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

Etapa 7. Criar um compartilhamento do RAM para habilitar atribuições de IP nas contas

Esta etapa é opcional. Você poderá concluir esta etapa somente se tiver concluído Integrar o IPAM a contas em uma organização da AWS Organizations.

Ao criar um compartilhamento do AWS RAM do grupo do IPAM, ele habilita atribuições de IP entre contas. O compartilhamento do RAM só está disponível em sua região da AWS inicial. Observe que você cria esse compartilhamento na mesma região que o IPAM, não na região local do grupo. Todas as operações administrativas em recursos do IPAM são feitas por meio da região inicial do IPAM. O exemplo neste tutorial cria um único compartilhamento para um único grupo, mas você pode adicionar vários grupos a um único compartilhamento. Para obter mais informações, incluindo uma explicação das opções que você deve inserir, consulte Compartilhar um grupo do IPAM usando o AWS RAM.

Execute os comandos a seguir para criar um compartilhamento de recursos.

```
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
```

A saída mostra que o grupo foi criado.

```
{
    "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
    }
}
```

Etapa 8. Crie uma VPC

Execute o comando a seguir para criar uma VPC e atribuir um bloco CIDR à VPC a partir do grupo em seu IPAM recém-criado.

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

A saída mostra que a VPC foi criada.

```
{
    "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
    }
}
```

Etapa 9. Limpeza

Siga as etapas nesta seção para excluir os recursos do IPAM que você criou neste tutorial.

1. Exclua a VPC.

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

2. Exclua o compartilhamento de RAM do grupo do IPAM.

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

3. Desprovisione o CIDR de grupo do grupo regional.

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

4. Desprovisione o CIDR de grupo do grupo de nível superior.

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

5. Excluir o IPAM

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

Tutorial: ver o histórico de endereços IP usando a AWS CLI

Os cenários desta seção mostram como analisar e auditar o uso de endereços IP usando a AWS CLI. Para obter informações gerais sobre como usar a AWS CLI, consulte Como usar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Conteúdo

- Visão geral
- Cenários

Visão geral

O IPAM retém automaticamente seus dados de monitoramento de endereços IP por até três anos. Você pode usar os dados históricos para analisar e auditar suas políticas de roteamento e segurança de rede. Você pode pesquisar insights históricos dos seguintes tipos de recursos:

- VPCs
- Sub-redes VPC
- Endereços IP elásticos
- Instâncias do EC2 que estão em execução
- Interfaces de rede do EC2 anexadas a instâncias

> **Important**
>
> Embora o IPAM não monitore instâncias do Amazon EC2 ou interfaces de rede do EC2 anexadas a instâncias, é possível usar o recurso Pesquisar histórico de IP para pesquisar dados históricos em CIDRs de interfaces de rede e de instâncias do EC2.

> **Note**
>
> - Os comandos neste tutorial devem ser executados usando a conta proprietária do IPAM e a região da AWS que hospeda o IPAM.
> - Os registros de alterações nos CIDRs são coletados em snapshots periódicos, o que significa que pode levar algum tempo para que os registros apareçam ou sejam atualizados, e os valores de SampledStartTime e SampledEndTime podem diferir dos horários reais em que ocorreram.

Cenários

Os cenários desta seção mostram como analisar e auditar o uso de endereços IP usando a AWS CLI. Para obter mais informações sobre os valores mencionados neste tutorial, como as amostras de hora de término e hora de início, consulte Ver histórico de endereços IP.

Cenário 1: quais recursos foram associados a **`10.2.1.155/32`** entre 1h e 21h em 27 de dezembro de 2021 (UTC)?

1. Execute o seguinte comando:

```
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. Veja os resultados da análise. No exemplo abaixo, o CIDR foi alocado para uma interface de rede e instância do EC2 ao longo do período de tempo. Observe que a ausência de um valor SampledEndTime significa que o registro ainda está ativo. Para obter mais informações sobre os valores mostrados na saída a seguir, consulte Ver histórico de endereços 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"
        }
    ]
}
```

Se o ID do proprietário da instância à qual uma interface de rede está anexada for diferente do ID do proprietário da interface de rede (como é o caso dos gateways NAT, da interfaces de rede do Lambda em VPCs e outros serviços da AWS), o parâmetro `ResourceOwnerId` é `amazon-aws` em vez do ID da conta do proprietário da interface de rede. O exemplo a seguir mostra o registro de um CIDR associado a um gateway 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"
        }
    ]
}
```

Cenário 2: quais recursos foram associados a **`10.2.1.0/24`** de 1º de dezembro de 2021 a 27 de dezembro de 2021 (UTC)?

1. Execute o seguinte comando:

```
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. Veja os resultados da análise. No exemplo abaixo, o CIDR foi alocado para uma sub-rede e VPC ao longo do período de tempo. Observe que a ausência de um valor SampledEndTime significa que o registro ainda está ativo. Para obter mais informações sobre os valores mostrados na saída a seguir, consulte Ver histórico de endereços IP.

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0864c82a42f5bffed",
            "ResourceCidr": "10.2.1.0/24",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0f5ee7e1ba908a378",
            "ResourceCidr": "10.2.1.0/24",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
```

```
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

Cenário 3: quais recursos foram associados a **2605:9cc0:409::/56** de 1º de dezembro de 2021 a 27 de dezembro de 2021 (UTC)?

1. Execute o seguinte comando, em que --region é a região inicial do 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. Veja os resultados da análise. No exemplo abaixo, o CIDR foi alocado para duas VPCs diferentes ao longo do período de tempo em uma região fora da região inicial do IPAM. Observe que a ausência de um valor SampledEndTime significa que o registro ainda está ativo. Para obter mais informações sobre os valores mostrados na saída a seguir, consulte Ver histórico de endereços 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"
        }
    ]
}
```

Cenário 4: quais recursos foram associados a **`10.0.0.0/24`** nas últimas 24 horas (supondo que a hora atual seja meia-noite de 27 de dezembro de 2021 (UTC))?

1. Execute o seguinte comando:

```
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. Veja os resultados da análise. No exemplo abaixo, o CIDR foi alocado para uma várias sub-redes e VPCs ao longo do período de tempo. Observe que a ausência de um valor SampledEndTime significa que o registro ainda está ativo. Para obter mais informações sobre os valores mostrados na saída a seguir, consulte Ver histórico de endereços IP.

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0d1b8f899725aa72d",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "VpcId": "vpc-042b8a44f64267d67",
            "SampledStartTime": "2021-12-11T16:35:59.074000+00:00",
            "SampledEndTime": "2021-12-28T15:34:00.017000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-09754dfd85911abec",
```

```
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-09754dfd85911abec",
            "SampledStartTime": "2021-12-27T20:07:59.947000+00:00",
            "SampledEndTime": "2021-12-28T15:34:00.017000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-west-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0a8347f594bea5901",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-0a8347f594bea5901",
            "SampledStartTime": "2021-12-11T16:35:59.318000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0af7eadb0798e9148",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "VpcId": "vpc-03298ba16756a8736",
            "SampledStartTime": "2021-12-14T21:07:22.357000+00:00"
        }
    ]
}
```


Cenário 5: quais recursos estão associados a atualmente **`10.2.1.155/32`**?

1. Execute o seguinte comando:

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

2. Veja os resultados da análise. No exemplo abaixo, o CIDR foi alocado para uma interface de rede e instância do EC2 ao longo do período de tempo. Observe que a ausência de um valor

SampledEndTime significa que o registro ainda está ativo. Para obter mais informações sobre os valores mostrados na saída a seguir, consulte Ver histórico de endereços 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"
        }
    ]
}
```

Cenário 6: quais recursos estão associados a atualmente **`10.2.1.0/24`**?

1. Execute o seguinte comando:

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

2. Veja os resultados da análise. No exemplo abaixo, o CIDR foi alocado para uma VPC e sub-rede ao longo do período de tempo. Somente os resultados que correspondem a esse exato CIDR `/24` são retornados, nem todos os `/32` dentro do CIDR `/24`. Observe que a ausência de um valor SampledEndTime significa que o registro ainda está ativo. Para obter mais informações sobre os valores mostrados na saída a seguir, consulte Ver histórico de endereços IP.

```
{
    "HistoryRecords": [
```

```
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0864c82a42f5bffed",
            "ResourceCidr": "10.2.1.0/24",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0f5ee7e1ba908a378",
            "ResourceCidr": "10.2.1.0/24",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

Cenário 7: quais recursos estão associados a atualmente **`54.0.0.9/32`**?

Neste exemplo, `54.0.0.9/32` é atribuído a um endereço IP elástico que não faz parte da AWS Organization integrada a seu IPAM.

1. Execute o seguinte comando:

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

2. Como `54.0.0.9/32` é atribuído a um endereço IP elástico que não faz parte da AWS Organization integrada ao IPAM neste exemplo, nenhum registro é retornado.

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

Tutorial: Traga o seu ASN para o IPAM

Se os seus aplicativos estiverem utilizando endereços IP confiáveis e Números de Sistemas Autônomos (ASNs) que seus parceiros ou clientes permitiram listar em suas redes, é possível executar esses aplicativos em AWS sem a necessidade de solicitar que seus parceiros ou clientes modifiquem suas listas de permissão.

Um número de sistema autônomo (ASN) é uma designação globalmente exclusiva que possibilita a identificação de um conjunto de redes na Internet e a troca dinâmica de dados de roteamento com outras redes por meio do Border Gateway Protocol. Os provedores de serviços de Internet (ISPs), por exemplo, utilizam ASNs para reconhecer a origem do tráfego de rede. Embora nem todas as organizações adquiram seus próprios ASNs, aquelas que o fazem têm a opção de trazer seu ASN para a AWS.

A funcionalidade BYOASN (Bring your own autonomous system number) permite anunciar os endereços IPv4 ou IPv6 que você traz para a AWS com seu próprio ASN público, em vez do ASN da AWS. Ao utilizar o BYOASN, o tráfego originado a partir do seu endereço IP exibe o seu ASN, em vez do ASN da AWS, permitindo que suas cargas de trabalho sejam acessadas por clientes ou parceiros que autorizaram o tráfego com base no seu endereço IP e ASN.

Important

- Para seguir este tutorial, é necessário concluir as etapas usando a conta de administrador do IPAM na região inicial do seu IPAM.
- Pressupõe-se que você seja o proprietário do ASN público que deseja trazer para o IPAM e que já tenha trazido um CIDR BYOIP para AWS e o provisionado para um pool no seu escopo público. Embora seja possível trazer um ASN para o IPAM a qualquer momento, é necessário associá-lo a um CIDR que tenha sido previamente trazido para a sua conta da AWS para utilizá-lo. Este tutorial pressupõe que você já tenha feito isso. Para ter mais informações, consulte Tutorial: trazer seus endereços IP para o IPAM.
- É possível alternar entre anunciar o seu próprio ASN ou um ASN AWS sem demora, mas há uma restrição que limita a mudança de um ASN AWS para o seu próprio ASN a uma vez por hora.
- Caso o seu CIDR BYOIP esteja atualmente sendo anunciado, não é necessário retirá-lo da publicidade antes de associá-lo ao seu ASN.

Pré-requisitos de integração para seu ASN

Você precisará do seguinte para concluir este tutorial:

- Seu ASN público de 2 ou 4 bytes.
- Se você já trouxe um intervalo de endereços IP para a AWS com Tutorial: trazer seus endereços IP para o IPAM, precisará do intervalo CIDR de endereços IP. Você também precisará de uma chave privada. É possível usar a chave privada que foi criada ao importar o intervalo de CIDR do endereço IP para a AWS ou criar uma nova chave privada, como descrito em Crie uma chave privada e gere um certificado X.509 no Guia do usuário do Amazon EC2.
- Quando traz um intervalo de endereços IPv4 ou IPv6 para a AWS com Tutorial: trazer seus endereços IP para o IPAM, você cria um certificado X.509 e carrega-o no registro RDAP no RIR. Você deve carregar o mesmo certificado que criou no registro RDAP em seu RIR para o ASN. Certifique-se de incluir as strings `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` antes e depois da parte codificada. Todo esse conteúdo deve estar em uma única e longa linha. O procedimento para atualizar o RDAP depende do RIR:
  - Para o ARIN, use o portal do Account Manager para adicionar o certificado na seção “Comentários públicos” para o objeto “Informações de rede” que representa seu ASN usando a opção “Modificar ASN”. Não o adicione à seção de comentários da sua organização.
  - Para o RIPE, adicione o certificado como um novo campo “descr” ao objeto “aut-num” que representa seu ASN. Geralmente, eles podem ser encontrados na seção “Meus recursos” do portal do banco de dados RIPE. Não o adicione à seção de comentários da sua organização ou ao campo “comentários” do objeto “aut-num”.
  - Para o APNIC, envie o certificado por e-mail para helpdesk@apnic.net para adicioná-lo manualmente ao campo “observações” do seu ASN. Envie o e-mail usando o contato autorizado do APNIC para o ASN.
- Ao trazer um intervalo de endereços IP para o IPAM, você cria uma ROA para confirmar que controla o espaço de endereço IP que está trazendo para o IPAM. Além dessa ROA, você deve ter uma segunda ROA no RIR com o ASN que você está trazendo para o IPAM. Se você não tiver essa segunda ROA para o ASN no RIR, conclua o item 3. Criar um objeto ROA no seu RIR. Ignore as outras etapas.

Etapas do tutorial

Conclua as etapas abaixo usando o AWS console ou o AWS CLI.

AWS Management Console

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione IPAMs.
3. Escolha seu IPAM.
4. Escolha a guia BYOASNS e escolha Provisionar por OASNS.
5. Insira o ASN. Como resultado, o campo Mensagem é preenchido automaticamente com a mensagem que você precisará assinar na próxima etapa.

   - A estrutura da mensagem é a seguinte, em que ACCOUNT é o número da sua conta AWS, ASN é o número de Sistema Autônomo (ASN) que você está fornecendo ao IPAM, e AAAAMMDD é a data de expiração da mensagem (padrão: último dia do mês seguinte). Exemplo: .

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

6. Copie a mensagem e substitua a data de validade pelo seu próprio valor, se quiser.
7. Assine a mensagem usando a chave privada. Exemplo: .

   ```
   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. Em Assinatura, insira a assinatura.
9. (Opcional) Para provisionar outro ASN, escolha Provisionar outro ASN. Você pode provisionar até 5 ASNs. Para aumentar essa cota, consulte o Cotas para o IPAM.
10. Escolha Provisionar.
11. Veja o processo de provisionamento na guia BYOASNs. Aguarde até que o status mude de Provisão pendente para Provisionado. Os BYOASNs em um status de provisão com falha são removidos automaticamente após 7 dias. Depois que o ASN for provisionado com sucesso, você poderá associá-lo a um CIDR BYOIP.
12. No painel de navegação à esquerda, escolha Grupos.
13. Escolha seu escopo público. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
14. Escolha um grupo regional que tenha um CIDR BYOIP provisionado. O grupo deve ter o serviço definido como EC2 e deve ter uma localidade escolhida.

15. Escolha a guia CIDRs e selecione um CIDR BYOIP.
16. Escolha Ações > Gerenciar associações BYOASN.
17. Em BYOASNs associadas, escolha o ASN que você trouxe para AWS. Se você tiver vários ASNs, poderá associar vários ASNs ao CIDR BYOIP. Você pode associar o máximo de ASNs que puder trazer para o IPAM. Observe que você pode trazer até 5 ASNs para o IPAM por padrão. Para ter mais informações, consulte Cotas para o IPAM.
18. Selecione Associar .
19. Aguarde a conclusão da associação com o ASN. Depois que o ASN for associado com sucesso ao CIDR BYOIP, você poderá anunciar o CIDR BYOIP novamente.
20. Escolha a guia CIDRs do grupo.
21. Selecione o CIDR de BYOIP e escolha Actions (Ações) >Advertise (Anunciar). Como resultado, suas opções de ASN são exibidas: o ASN da Amazon e todos os ASNs que você trouxe para o IPAM.
22. Selecione o ASN que você trouxe para o IPAM e escolha Anunciar CIDR. Como resultado, o CIDR BYOIP é anunciado e o valor na coluna Anúncios muda de Withdrawn Retirado para Anunciado. A coluna Número do Sistema Autônomo exibe o ASN associado ao CIDR.
23. (opcional) Se você decidir que deseja alterar a associação de ASN de volta para o Amazon ASN, selecione o CIDR BYOIP e escolha Ações > Anunciar novamente. Desta vez, escolha o Amazon ASN. Você pode voltar ao ASN da Amazon a qualquer momento, mas só pode mudar para um ASN personalizado uma vez a cada hora.

O tutorial está completo.

Limpeza

1. Desassocie o ASN do CIDR BYOIP
   - Para retirar o BYOIP CIDR da publicidade, em seu grupo no escopo público, escolha o BYOIP CIDR e selecione Ações > Retirar anúncio.
   - Para desassociar o ASN do CIDR, escolha Ações > Gerenciar associações BYOASN.
2. Desprovisionar o ASN
   - Para desprovisionar o ASN, escolha o ASN e escolha Desprovisionar ASN na guia ByOASNS. Como resultado, o ASN é desprovisionado. Os BYOASNs em um status de desprovisionado são removidos automaticamente após 7 dias.

A limpeza está completa.

Command line

1. Provisione seu ASN incluindo seu ASN e a mensagem de autorização. A assinatura é a mensagem assinada com sua chave privada.

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

2. Descreva seu ASN para monitorar o processo de provisionamento. Se a solicitação for bem-sucedida, você deverá ver o provisionStatus definido como provisionado após alguns minutos.

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

3. Associe seu ASN ao seu CIDR BYOIP. Qualquer ASN personalizado a partir do qual você deseja anunciar deve primeiro ser associado ao seu CIDR.

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

4. Descreva seu CIDR para acompanhar o processo de associação.

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

5. Anuncie seu CIDR com seu ASN. Se o CIDR já estiver anunciado, isso trocará o ASN de origem do da Amazon para o seu.

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

6. Descreva seu CIDR para ver a alteração do estado do ASN de associado para anunciado.

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

O tutorial está completo.

Limpeza

1. Execute um destes procedimentos:

- Para retirar apenas o anúncio de ASN e voltar a usar os ASNs da Amazon, mantendo o CIDR anunciado, você deve chamar advertise-byoip-cidr com o valor AWS especial para o parâmetro asn. Você pode voltar ao ASN da Amazon a qualquer momento, mas só pode mudar para um ASN personalizado uma vez a cada hora.

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

- Para retirar seu anúncio CIDR e ASN simultaneamente, você pode chamar draw-byoip-cidr.

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

2. Para limpar seu ASN, você deve primeiro desassociá-lo do seu CIDR BYOIP.

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

3. Depois que seu ASN for desassociado de todos os CIDRs BYOIP aos quais você o associou, você poderá desprovisioná-lo.

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

4. O CIDR BYOIP também pode ser desprovisionado quando todas as associações de ASN forem removidas.

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

5. Confirme o desprovisionamento.

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

A limpeza está completa.

Tutorial: trazer seus endereços IP para o IPAM

Os tutoriais desta seção mostram como trazer o espaço de endereços IP públicos para a AWS e gerenciar o espaço com o IPAM.

O gerenciamento do espaço de endereços IP públicos com o IPAM apresenta os seguintes benefícios:

- Melhora a utilização de endereços IP públicos em toda a organização: você pode usar o IPAM para compartilhar o espaço de endereços IP com as contas da AWS. Sem usar o IPAM, não é possível compartilhar seu espaço de IPs públicos com as contas do AWS Organizations.
- Simplifica o processo de trazer o espaço de IPs públicos para a AWS: você pode usar o IPAM para integrar o espaço de endereços IP públicos uma vez e, em seguida, usar o IPAM para distribuir seus IPs públicos entre as regiões para recursos como instâncias do EC2 e application load balancers. Sem o IPAM, você precisa integrar seus IPs públicos a cada região da AWS.

Conteúdo

- Verificar o controle do domínio
- Trazer seu próprio IP para o IPAM usando o AWS Management Console e a AWS CLI
- Trazer seu próprio CIDR IP para o IPAM usando apenas a AWS CLI
- Traga seu próprio IP para o CloudFront usando o IPAM

Verificar o controle do domínio

Antes de trazer um intervalo de endereços IP para a AWS, você tem que usar uma das opções descritas nesta seção para verificar que controla o espaço de endereço IP. Mais tarde, quando você trouxer o intervalo de endereços IP para a AWS, a AWS validará que você controla o intervalo de endereços IP. Essa validação garante que os clientes não possam usar intervalos de IP pertencentes a outras pessoas, evitando problemas de roteamento e de segurança.

Existem dois métodos que você pode usar para verificar que controla o intervalo:

- Certificado X.509: se seu intervalo de endereços IP estiver registrado em um Registro compatível com RDAP (como ARIN, RIPE e APNIC), você poderá usar um certificado X.509 para verificar que é o proprietário do domínio.
- Registro TXT do DNS: independentemente de seu Registro da Internet ser ou não compatível com RDAP, você pode usar um token de verificação e um registro TXT do DNS para verificar que é o proprietário do domínio.

Conteúdo

- Verificar seu domínio com um certificado X.509
- Verifique seu domínio com um registro TXT do DNS

Verificar seu domínio com um certificado X.509

Esta seção descreve como verificar seu domínio com um certificado X.509 antes de trazer seu intervalo de endereços IP para o IPAM.

Para verificar seu domínio com um certificado X.509

1. Conclua as três etapas descritas em Pré-requisitos para o BYOIP no Amazon EC2 no Guia do usuário do Amazon EC2.

   > **Note**
   >
   > Ao criar as ROAs, para CIDRs IPv4, você deve definir o comprimento máximo de um prefixo de endereço IP como `/24`. Para CIDRs IPv6, se você estiver adicionando-os a um grupo anunciável, o tamanho máximo de um prefixo de endereço IP deve ser `/48`. Isso garante que você tenha total flexibilidade para dividir seu endereço IP público nas regiões da AWS. O IPAM impõe o comprimento máximo que você definiu. O comprimento máximo é o menor anúncio de comprimento de prefixo que você permitirá para essa rota. Por exemplo, se você trouxer um bloco CIDR `/20` para a AWS, definindo o comprimento máximo como `/24`, você pode dividir o bloco maior da maneira que quiser (como com `/21`, `/22` ou `/24`) e distribuir esses blocos CIDR menores para qualquer região. Se você definisse o comprimento máximo como `/23`, não seria capaz de dividir e anunciar um `/24` a partir do bloco maior. Além disso, observe que `/24` é o menor bloco IPv4 e `/48` é o menor bloco IPv6 que você pode anunciar de uma região para a Internet.

2. Conclua apenas as etapas 1 e 2 em Provision a publicly advertisable address range in AWS no Amazon EC2 User Guide, não provisione o intervalo de endereços (etapa 3) ainda. Salve a `text_message` e a `signed_message`. Você precisará delas posteriormente neste processo.

Depois de concluir essas etapas, continue com Trazer seu próprio IP para o IPAM usando o AWS Management Console e a AWS CLI ou Trazer seu próprio CIDR IP para o IPAM usando apenas a AWS CLI.

Verifique seu domínio com um registro TXT do DNS

Conclua as etapas desta seção para verificar seu domínio com um registro TXT do DNS antes de trazer seu intervalo de endereços IP para o IPAM.

Você pode usar registros TXT do DNS para validar que controla um intervalo de endereços IP públicos. Um registro TXT do DNS é um tipo de registro do DNS que fornece informações adicionais sobre seu domínio. Esse atributo permite que você traga endereços IP registrados em qualquer Registro da Internet (como JPNIC, LACNIC e AFRINIC), não apenas os compatíveis com validações baseadas em registro RDAP (Registration Data Access Protocol) (como ARIN, RIPE e APNIC).

> **Important**
>
> Antes de continuar, você já deve ter criado um IPAM no nível gratuito ou avançado. Se você não tiver um IPAM, conclua Criar um IPAM primeiro.

Conteúdo

- Etapa 1: criar uma ROA, se não tiver uma
- Etapa 2. Criar um token de verificação
- Etapa 3. Configurar a zona do DNS e o registro TXT

Etapa 1: criar uma ROA, se não tiver uma

Você deve ter uma ROA (Route Origin Authorization) em seu RIR (Regional Internet Registry) para os intervalos de endereços IP que deseja anunciar. Se você não tiver uma ROA em seu RIR, conclua 3. Create a ROA object in your RIR no Amazon EC2 User Guide. Ignore as outras etapas.

O intervalo de endereços IPv4 mais específico que é possível trazer é /24. O intervalo mais específico de endereços IPv6 que é possível trazer é /48 para CIDRs anunciáveis publicamente e /60 para CIDRs que não são anunciáveis publicamente.

Etapa 2. Criar um token de verificação

Um token de verificação é um valor aleatório gerado pela AWS que você pode usar para provar que tem o controle de um recurso externo. Por exemplo, você pode usar um token de verificação para validar que controla um intervalo de endereços IP públicos quando traz um intervalo de endereços IP para a AWS (BYOIP).

Conclua as etapas desta seção para criar um token de verificação do qual precisará em uma etapa posterior deste tutorial para trazer seu intervalo de endereços IP para o IPAM. Use as instruções abaixo para o console da AWS ou para a AWS CLI.

AWS Management Console

Para criar um token de verificação

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No AWS Management Console, escolha a região da AWS em que você deseja criar o IPAM.
3. No painel de navegação, selecione IPAMs.
4. Escolha seu IPAM e depois escolha a guia Tokens de verificação.
5. Selecione Criar token de verificação.
6. Depois de criar o token, deixe essa guia do navegador aberta. Você precisará do valor do token e do nome do token na próxima etapa e do ID do token em uma etapa posterior.

Observe o seguinte:

- Depois de criar um token de verificação, você pode reutilizá-lo para vários CIDRs de BYOIP que você provisiona no IPAM dentro de 72 horas. Se você quiser provisionar mais CIDRs após as 72 horas, precisará de um novo token.
- Você pode criar até 100 tokens. Se você atingir o limite, exclua os tokens expirados.

Command line

- Solicite que o IPAM crie um token de verificação que você usará para a configuração do DNS com create-ipam-external-resource-verification-token:

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

Isso retornará um IpamExternalResourceVerificationTokenId e um token com `TokenName` e `TokenValue`, e a hora de expiração (`NotAfter`) do token.

```
{
    "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" }
}
```

Observe o seguinte:

- Depois de criar um token de verificação, você pode reutilizá-lo para vários CIDRs de BYOIP que você provisiona no IPAM dentro de 72 horas. Se você quiser provisionar mais CIDRs após as 72 horas, precisará de um novo token.
- Você pode visualizar os tokens usando describe-ipam-external-resource-verification-tokens.
- Você pode criar até 100 tokens. Se você atingir o limite, poderá excluir tokens expirados usando delete-ipam-external-resource-verification-token.

Etapa 3. Configurar a zona do DNS e o registro TXT

Conclua as etapas desta seção para configurar a zona do DNS e o registro TXT. Se você não estiver usando o Route53 como DNS, siga a documentação fornecida pelo seu provedor de DNS para configurar uma zona do DNS e adicionar um registro TXT.

Se você estiver usando o Route53, observe o seguinte:

- Para criar uma zona de pesquisa reversa no console da AWS, consulte Creating a public hosted zone no Amazon Route 53 Developer Guide ou use o comando da AWS CLI create-hosted-zone.
- Para criar um registro na zona de pesquisa reversa no console da AWS, consulte Creating records by using the Amazon Route 53 console no Amazon Route 53 Developer Guide ou use o comando da AWS CLI change-resource-record-sets.
- Quando terminar de criar sua zona hospedada, delegue a zona hospedada do RIR aos servidores de nomes fornecidos pelo Route53 (como o LACNIC ou o APNIC).

Se você estiver usando outro provedor de DNS ou o Route53, ao configurar o registro TXT, observe o seguinte:

- O nome do registro deve ser o nome do seu token.
- O tipo de registro deve ser TXT.
- O valor de ResourceRecord deve ser o valor do token.

Exemplo:

- Nome: `86950620.113.0.203.in-addr.arpa`
- Tipo: `TXT`
- Valor de ResourceRecords: `a34597c3-5317-4238-9ce7-50da5b6e6dc8`

Em que:

- `86950620` é o nome do token de verificação.
- `113.0.203.in-addr.arpa` é o nome da zona de pesquisa reversa.
- `TXT` é o tipo de registro.
- `a34597c3-5317-4238-9ce7-50da5b6e6dc8` é o valor do token de verificação.

> **Note**
>
> Dependendo do tamanho do prefixo a ser levado para o IPAM com BYOIP, um ou mais registros de autenticação devem ser criados no DNS. Esses registros de autenticação são do tipo TXT e devem ser colocados na zona reversa do próprio prefixo ou do prefixo superior.
>
> - Para IPv4, os registros de autenticação precisam se alinhar com os intervalos em um limite de octeto que compõe o prefixo.
>   - Exemplos
>   - Para 198.18.123.0/24, que já está alinhado em um limite de octeto, você precisaria criar um único registro de autenticação em:
>   - *`token-name`*`.123.18.198.in-addr.arpa. IN TXT “`*`token-value`*`”`
>   - Para 198.18.12.0/22, que em si não está alinhado ao limite de octeto, você precisaria criar quatro registros de autenticação. Esses registros devem cobrir as sub-redes 198.18.12.0/24, 198.18.13.0/24, 198.18.14.0/24 e 198.18.15.0/24 que estão alinhadas em um limite de octeto. As entradas correspondentes do DNS devem ser:
>   - *`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*"
    - Para 198.18.0.0/16, que já está alinhado em um limite de octeto, você precisa criar um único registro de autenticação:
        - *token-name*.18.198.in-addr.arpa. IN TXT "*token-value*"
- Para o IPv6, os registros de autenticação precisam se alinhar com os intervalos em um limite de nibble que compõe o prefixo. Os valores em nibbles válidos são, por exemplo, 32, 36, 40, 44, 48, 52, 56 e 60.
    - Exemplos
        - Para 2001:0db8::/40, que já está alinhado em um limite de nibble, você precisa criar um único registro de autenticação:
            - *token-name*.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
        - Para 2001:0db8:80::/42, que em si não está alinhado no limite do nibble, você precisa criar quatro registros de autenticação. Esses registros devem cobrir as sub-redes 2001:db8:80::/44, 2001:db8:90::/44, 2001:db8:a0::/44 e 2001:db8:b0::/44 que estão alinhadas em um limite de nibble. As entradas correspondentes do DNS devem ser:
            - *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*"
        - Para o intervalo não anunciado 2001:db8:0:1000::/54, que em si não está alinhado em um limite de nibble, você precisa criar quatro registros de autenticação. Esses registros devem cobrir as sub-redes 2001:db8:0:1000::/56, 2001:db8:0:1100::/56, 2001:db8:0:1200::/56 e 2001:db8:0:1300::/56 que estão alinhadas em um limite de nibble. As entradas correspondentes do DNS devem ser:
            - *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*”

- Para validar que existe o número correto de números hexadecimais entre o nome do token e a string "ip6.arpa", multiplique o número por quatro. O resultado deve corresponder ao comprimento do prefixo. Por exemplo, para um prefixo /56, você deve ter 14 dígitos hexadecimais.

Depois de concluir essas etapas, continue com Trazer seu próprio IP para o IPAM usando o AWS Management Console e a AWS CLI ou Trazer seu próprio CIDR IP para o IPAM usando apenas a AWS CLI.

Trazer seu próprio IP para o IPAM usando o AWS Management Console e a AWS CLI

Trazer seu próprio IP (BYOIP) para o IPAM permite que você use os intervalos de endereços IPv4 e IPv6 existentes da sua organização na AWS. Isso permite que você mantenha uma marca consistente, melhore a performance da rede, aprimore a segurança e simplifique o gerenciamento, unificando ambientes on-premises e na nuvem em seu próprio espaço de endereços IP.

Siga estas etapas para trazer um CIDR IPv4 ou IPv6 para o IPAM usando o Console de Gerenciamento da AWS e a AWS CLI.

> **Note**
>
> Antes de começar, você deve ter o controle do domínio verificado.

Se você trouxer um intervalo de endereços IPv4 para a AWS, poderá usar todos os endereços IP do intervalo, incluindo o primeiro endereço (o endereço de rede) e o último endereço (o endereço de broadcast).

Conteúdo

- Traga seu próprio CIDR IPv4 para o IPAM usando o Console de Gerenciamento da AWS e a AWS CLI
- Traga seu próprio CIDR IPv6 para o IPAM usando o Console de Gerenciamento da AWS

Traga seu próprio CIDR IPv4 para o IPAM usando o Console de Gerenciamento da AWS e a AWS CLI

Siga estas etapas para trazer um CIDR IPv4 para o IPAM e alocar um endereço IP elástico (EIP) usando o Console de Gerenciamento da AWS e a AWS CLI.

Important

- Para este tutorial, é necessário que você já tenha concluído as etapas nas seguintes seções:
  - Integrar o IPAM a contas em uma organização da AWS Organizations.
  - Criar um IPAM.
- Cada etapa deste tutorial deve ser executada por uma das três contas do AWS Organizations:
  - A conta de gerenciamento
  - A conta de membro configurada para ser o administrador do IPAM em Integrar o IPAM a contas em uma organização da AWS Organizations. Neste tutorial, essa conta será chamada de conta IPAM.
  - A conta de membro em sua organização que alocará CIDRs de um grupo do IPAM. Neste tutorial, essa conta será chamada de conta de membro.

Conteúdo

- Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM
- Etapa 2: criar um grupo do IPAM de nível superior
- Etapa 3. Criar um grupo regional dentro de um grupo de nível superior
- Etapa 4: anunciar o CIDR
- Etapa 5. Compartilhar o grupo regional
- Etapa 6: alocar um endereço IP elástico do grupo
- Etapa 7: associar um endereço IP elástico a uma instância do EC2
- Etapa 8: limpeza
- Alternativa para a Etapa 6

Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM

Para concluir este tutorial como um usuário da AWS, você pode usar os perfis nomeados da AWS CLI para alternar de um perfil do IAM para outro. Perfis nomeados são coleções de configurações e credenciais às quais você se refere ao usar a opção `--profile` com a AWS CLI. Para obter mais informações sobre como criar perfis do IAM e perfis nomeados para contas da AWS, consulte Uso de perfis do IAM na AWS CLI.

Crie uma função e um perfil nomeado para cada uma das três contas da AWS que você usará neste tutorial:

- Um perfil chamado `management-account` para a conta de gerenciamento do AWS Organizations.
- Um perfil chamado `ipam-account` para a conta de membro do AWS Organizations configurada para ser o administrador do IPAM.
- Um perfil chamado `member-account` para a conta de membro do AWS Organizations em sua organização que alocará CIDRs de um grupo do IPAM.

Depois de criar os perfis do IAM e os perfis nomeados, volte para esta página e vá para a próxima etapa. Você notará, ao longo do restante deste tutorial, que os exemplos de comandos da AWS CLI usam a opção `--profile` com um dos perfis nomeados para indicar qual conta deve executar o comando.

Etapa 2: criar um grupo do IPAM de nível superior

Conclua as etapas nesta seção para criar um grupo do IPAM de nível superior.

Esta etapa deve ser executada pela conta do IPAM.

Para criar um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Escolha o escopo público. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Selecione Criar.
5. (Opcional) Adicione uma Name tag (Etiqueta de nome) e uma Description (Descrição) para o grupo.

6. Em Tipo de origem, escolha Escopo do IPAM.
7. Em Address family (Família de endereços), escolha IPv4.
8. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
9. Em Locale (Local), escolha None (Nenhum).

   A integração do IPAM com o BYOIP exige que a localidade seja definida em qualquer grupo que será usado para o CIDR do BYOIP. Como você vai criar um grupo do IPAM de nível superior com um grupo regional dentro dele, e vamos alocar espaço para um endereço IP elástico do grupo regional, você definirá o local no grupo regional e não no grupo de nível superior. Você adicionará a localidade ao grupo regional ao criá-lo em uma etapa posterior.

   > **Note**
   >
   > Se você estiver criando apenas um único grupo e não um grupo de nível superior com grupos regionais nele, escolha uma localidade que disponibilize o grupo para alocações.

10. Em Origem de IP público, escolha BYOIP.
11. Em CIDRs para provisionar, faça um dos seguintes procedimentos:

    - Se você verificou seu controle do domínio com um certificado X.509, deverá incluir o CIDR, a mensagem de BYOIP e a assinatura do certificado que criou nessa etapa para que possamos confirmar que você controla o espaço público.
    - Se você verificou seu controle do domínio com um registro TXT do DNS, deverá incluir o CIDR e token de verificação do IPAM criado nessa etapa para que possamos confirmar que você controla o espaço público.

    Observe que, ao provisionar um CIDR IPv4 para um grupo dentro do grupo de nível superior, o CIDR IPv4 mínimo que você pode provisionar é `/24`. CIDRs mais específicos (como `/25`) não são permitidos.

> **Important**
>
> Embora a maior parte do provisionamento seja concluída em até 2 horas, a conclusão do processo de provisionamento pode levar até 1 semana para intervalos que permitam anúncios públicos.

12. Desmarque a opção Definir as configurações da regra de alocação deste grupo.
13. (Opcional) Escolha Tags (Etiquetas) para o grupo.
14. Selecione Criar.

Certifique-se de que esse CIDR tenha sido provisionado antes de continuar. Você pode ver o estado do provisionamento na guia CIDRs na página de detalhes do grupo.

Etapa 3. Criar um grupo regional dentro de um grupo de nível superior

Crie um grupo regional dentro de um grupo de nível superior. A integração do IPAM com o BYOIP exige que a localidade seja definida em qualquer grupo que será usado para o CIDR do BYOIP. Você adicionará o local ao grupo regional ao criá-lo em uma etapa posterior. O parâmetro `Locale` deve fazer parte de uma das regiões operacionais que você configurou ao criar o IPAM. Por exemplo, uma localidade de us-east-1 significa que us-east-1 deve ser uma região operacional para o IPAM. Uma localidade de us-east-1-scl-1 (um grupo de borda de rede usado para Zonas locais) significa que o IPAM deve ter uma região operacional de us-east-1.

Esta etapa deve ser executada pela conta do IPAM.

Para criar um grupo regional dentro de um grupo de nível superior

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Se você não quiser usar o escopo privado padrão, no menu suspenso na parte superior do painel de conteúdo, escolha o escopo que deseja usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Selecione Criar.
5. (Opcional) Adicione uma Name tag (Etiqueta de nome) e uma Description (Descrição) para o grupo.

6. Em Origem, escolha o grupo de nível superior que você criou na seção anterior.
7. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
8. Em Locale (Local), escolha o local do grupo. Neste tutorial, usaremos `us-east-2` como o local para o grupo regional. As opções disponíveis são provenientes das regiões operacionais que você escolheu ao criar seu IPAM.

   A localidade do grupo deve ser uma das seguintes opções:

   - Uma região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações.
   - O grupo de borda de rede para uma Zona local da AWS em que você quer disponibilizar esse grupo do IPAM para alocações (Zonas locais com suporte). Essa opção está disponível somente para grupos IPv4 de IPAM no escopo público.
   - Uma Zona local dedicada da AWS. Para criar um grupo dentro de uma Zona local dedicada da AWS, insira a Zona local dedicada da AWS na entrada do seletor.
   - `Global` quando você quiser usar endereços IP globalmente em todas as regiões da AWS, como locais do CloudFront. A localidade `Global` só está disponível para grupos IPv4 públicos.

   Por exemplo, um CIDR pode ser alocado apenas para uma VPC de um grupo do IPAM que compartilhe uma localidade com a Região da VPC. Observe que, ao escolher uma localidade para um grupo, não será possível modificá-la. Se a região de origem do IPAM não estiver disponível devido a uma interrupção e o grupo tiver um local diferente da região de origem do IPAM, o grupo ainda poderá ser usado para alocar endereços IP.

   A escolha de uma localidade garante que não haja dependências inter-regionais entre seu grupo e os recursos alocados a partir dele.
9. Em Service (Serviço), escolha EC2 (EIP/VPC). O serviço selecionado determina o serviço da AWS no qual o CIDR poderá ser publicado. Atualmente, a única opção é EC2 (EIP/VPC), o que significa que os CIDRs alocados a partir desse pool poderão ser anunciados para o serviço Amazon EC2 (para endereços IP elásticos) e para o serviço Amazon VPC (para CIDRs associados a VPCs).
10. Em CIDRs to provision (CIDRs a provisionar), escolha a CIDR que será provisionada para o grupo.

> **Note**
>
> Quando um CIDR é provisionado para um grupo regional dentro do grupo de nível superior, o CIDR IPv4 mais específico que você pode provisionar é /24. CIDRs mais específicos (como /25) não são permitidos. Depois de criar o grupo regional, você poderá criar grupos menores (como /25) dentro do mesmo grupo regional. Observe que, se você compartilhar o pool regional ou os pools nele contidos, esses pools só poderão ser usados na localidade definida no mesmo pool regional.

11. Marque a opção Definir as configurações da regra de alocação deste grupo. Aqui, você tem as mesmas opções de regra de alocação que na criação do grupo de nível superior. Consulte Criar um grupo de IPv4 de nível superior para obter uma explicação das opções que estão disponíveis ao criar grupos. As regras de alocação para o grupo regional não são herdadas do grupo de nível superior. Se você não aplicar nenhuma regra aqui, nenhuma regra de alocação será definida para o grupo.
12. (Opcional) Escolha Tags (Etiquetas) para o grupo.
13. Ao terminar de configurar o grupo, escolha Create pool (Criar grupo).

Certifique-se de que esse CIDR tenha sido provisionado antes de continuar. Você pode ver o estado do provisionamento na guia CIDRs na página de detalhes do grupo.

Etapa 4: anunciar o CIDR

As etapas nesta seção devem ser realizadas pela conta do IPAM. Após associar o endereço IP elástico (EIP) a uma instância ou Elastic Load Balancer, você pode começar a anunciar o CIDR que trouxe para a AWS que está no grupo que tem EC2 Service (EIP/VPC) [Serviço EC2 (EIP/VPC)] configurado. Neste tutorial, esse é o seu grupo regional. Por padrão, o CIDR não é anunciado, o que significa que não é acessível publicamente pela Internet.

Esta etapa deve ser executada pela conta do IPAM.

> **Note**
>
> O status do anúncio não restringe sua capacidade de alocar endereços IP elásticos. Mesmo que seu BYOIPv4 CIDR não seja anunciado, você ainda pode criar EIPs do grupo do IPAM.

Para anunciar o CIDR

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Escolha o escopo público. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Escolha o grupo regional que você criou neste tutorial.
5. Escolha a guia CIDRs.
6. Selecione o CIDR de BYOIP e escolha Actions (Ações) >Advertise (Anunciar).
7. Escolha Advertise CIDR (Anunciar CIDR).

Como resultado, o CIDR BYOIP é anunciado e o valor na coluna Advertising (Publicidade) muda de Withdrawn (Retirado) para Advertised (Anunciado).

Etapa 5. Compartilhar o grupo regional

Siga as etapas nesta seção para compartilhar o grupo de IPAM usando o AWS Resource Access Manager (RAM).

Habilitar o compartilhamento de recursos no AWS RAM

Depois de criar seu IPAM, você desejará compartilhar o grupo regional com outras contas em sua organização. Antes de compartilhar um grupo do IPAM, conclua as etapas nesta seção para habilitar o compartilhamento de recursos com o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`management-account`**.

Para habilitar o compartilhamento de recursos

1. Com a conta de gerenciamento do AWS Organizations, abra o console do AWS RAM em https://console.aws.amazon.com/ram/.
2. No painel de navegação esquerdo, escolha Configurações, depois Habilitar compartilhamento com o AWS Organizations e escolha Salvar configurações.

Agora você pode compartilhar um grupo do IPAM com outros membros da organização.

Compartilhar um grupo do IPAM usando o AWS RAM

Nesta seção, você compartilhará o grupo regional com outra conta de membro do AWS Organizations. Para obter instruções completas sobre o compartilhamento de grupos do IPAM, incluindo informações sobre as permissões necessárias do IAM, consulte Compartilhar um grupo do IPAM usando o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`ipam-account`**.

Para compartilhar um grupo do IPAM usando o AWS RAM

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado, o grupo de IPAM e Ações > Visualizar detalhes.
4. Em Resource sharing (Compartilhamento de recursos), escolha Create resource share (Criar compartilhamento de recursos). O console do AWS RAM será aberto. Você compartilhará o grupo usando o AWS RAM.
5. Escolha Create a resource share (Criar um compartilhamento de recursos).
6. No console do AWS RAM, escolha Criar um compartilhamento de recursos novamente.
7. Adicione um Nome para o recurso compartilhado.
8. Em Selecionar tipo de recurso, escolha Grupos do IPAM e, em seguida, escolha o ARN do grupo que deseja compartilhar.
9. Escolha Próximo.
10. Escolha a permissão AWSRAMPermissionIpamPoolByoipCidrImport. Os detalhes das opções de permissão estão fora do escopo deste tutorial, mas você pode descobrir mais sobre essas opções em Compartilhar um grupo do IPAM usando o AWS RAM.
11. Escolha Próximo.
12. Em Entidades principais > Selecionar tipo de entidade principal, escolha Conta da AWS e insira o ID da conta que trará um intervalo de endereços IP para o IPAM e escolha Adicionar.
13. Escolha Próximo.
14. Revise as opções de compartilhamento de recursos e as entidades principais com as quais você compartilhará e escolha Criar.
15. Para permitir que a conta da **`member-account`** aloque o endereço IP CIDRS do grupo do IPAM, crie um segundo compartilhamento de recursos com `AWSRAMDefaultPermissionsIpamPool`. O valor para `--resource-arns` é o

ARN do grupo do IPAM criado na seção anterior. O valor para `--principals` é o ID de **`member-account`**. O valor para `--permission-arns` é o ARN da permissão `AWSRAMDefaultPermissionsIpamPool`.

Etapa 6: alocar um endereço IP elástico do grupo

Conclua as etapas desta seção para alocar um endereço IP elástico do grupo. Observe que se estiver usando grupos IPv4 públicos para alocar endereços IP elásticos, você poderá usar as etapas alternativas em Alternativa para a Etapa 6 em vez das etapas desta seção.

> **Important**
>
> Se você encontrar um erro relacionado à falta de permissões para chamar ec2:AllocateAddress, é necessário atualizar a permissão gerenciada atualmente atribuída ao grupo do IPAM compartilhado com você. Recomendamos entrar em contato com a pessoa responsável pela criação do compartilhamento de recursos e solicitar a atualização da permissão gerenciada de `AWSRAMPermissionIpamResourceDiscovery` para a versão mais recente. Para obter detalhes adicionais, consulte Atualização de um compartilhamento de recursos no Guia do Usuário AWS RAM.

AWS Management Console

Siga as etapas em Allocate an Elastic IP address no Guia do usuário do Amazon EC2 para alocar o endereço, mas observe o seguinte:

- Esta etapa deve ser executada pela conta de membro.
- Certifique-se de que a região da AWS em que você está no console do EC2 corresponda à opção de localidade que você escolheu ao criar o grupo regional.
- Ao escolher o grupo de endereços, escolha a opção Alocar usando um grupo IPV4 do IPAM e depois o grupo regional que você criou.

Command line

Aloque um endereço do grupo com o comando allocate-address. A `--region` que você usa deve corresponder à opção de `-locale` que você escolheu quando criou o grupo na Etapa 2. Inclua o ID do grupo do IPAM que você criou na Etapa 2 em `--ipam-pool-id`. Opcionalmente, você também pode escolher um `/32` específico em seu grupo do IPAM usando a opção `--address`.

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

Exemplo de resposta:

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

Para obter mais informações, consulte Allocate an Elastic IP address no Guia do usuário do Amazon EC2.

Etapa 7: associar um endereço IP elástico a uma instância do EC2

Conclua as etapas desta seção para associar um endereço IP elástico a uma instância do EC2.

AWS Management Console

Siga as etapas em Associate an Elastic IP address no Guia do usuário do Amazon EC2 para alocar um endereço IP elástico do grupo do IPAM, mas observe o seguinte: quando você usa a opção Console de Gerenciamento da AWS, a região da AWS à qual você associa o endereço IP elástico deve corresponder à opção de localidade que você escolheu ao criar o grupo regional.

Esta etapa deve ser executada pela conta de membro.

Command line

Esta etapa deve ser executada pela conta de membro. Use a opção `--profile` **`member-account`**.

Associe o endereço IP elástico a uma instância com o comando associate-address. A `--region` à qual você associa o endereço IP elástico deve corresponder à opção de `--locale` que você escolheu quando criou o grupo regional.

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

Exemplo de resposta:

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

Para obter mais informações, consulte Associate an Elastic IP address with an instance or network interface no Guia do usuário do Amazon EC2.

Etapa 8: limpeza

Siga as etapas desta seção para limpar os recursos que você provisionou e criou neste tutorial.

Etapa 1: retirar o CIDR da publicidade

Esta etapa deve ser executada pela conta do IPAM.

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Escolha o escopo público.
4. Escolha o grupo regional que você criou neste tutorial.
5. Escolha a guia CIDRs.
6. Selecione o CIDR de BYOIP e escolha Actions (Ações) >Withdraw from advertising (Retirar da publicidade).
7. Selecione Withdraw CIDR (Retirar CIDR).

Como resultado, o CIDR de BYOIP é anunciado e o valor na coluna Advertising (Publicidade) muda de Advertised (Anunciado) para Withdrawn (Retirado).

Etapa 2: desassociar o endereço IP elástico

Esta etapa deve ser executada pela conta de membro. Se você estiver usando a AWS CLI, use a opção `--profile` **`member-account`**.

- Conclua as etapas em Dissociar um endereço IP elástico no Guia do usuário do Amazon EC2 para remover a associação do EIP. Ao abrir o EC2 no Console de Gerenciamento da AWS, a

região da AWS em que você desassocia a EIP deve corresponder à opção `Locale` escolhida ao criar o grupo que será usado para o CIDR de BYOIP. Neste tutorial, esse é o seu grupo regional.

Etapa 3: liberar o endereço IP elástico

Esta etapa deve ser executada pela conta de membro. Se você estiver usando a AWS CLI, use a opção `--profile` **`member-account`**.

- Conclua as etapas em Liberar um endereço IP elástico no Guia do usuário do Amazon EC2 para liberar um endereço IP elástico (EIP) do grupo IPv4 público. Ao abrir o EC2 no Console de Gerenciamento da AWS, a região da AWS em que você aloca a EIP deve corresponder à opção `Locale` escolhida ao criar o grupo que será usado para o CIDR de BYOIP.

Etapa 4: excluir qualquer compartilhamento do RAM e desabilitar a integração do RAM com o AWS Organizations

Esta etapa deve ser executada pela conta do IPAM e pela conta de gerenciamento, respectivamente. Se você estiver usando o AWS CLI para excluir os compartilhamentos do RAM e desabilitar a integração do RAM, use as opções `--profile` **`ipam-account`** e `--profile` **`management-account`**.

- Conclua as etapas em Excluir um compartilhamento de recursos no AWS RAM e Desabilitar o compartilhamento de recursos com o AWS Organizations no Guia do usuário do AWS RAM, nessa ordem, para excluir os compartilhamentos do RAM e desabilitar a integração do RAM com o AWS Organizations.

Etapa 5: desprovisionar os CIDRs do grupo regional e do grupo de nível superior

Esta etapa deve ser executada pela conta do IPAM. Se você estiver usando a AWS CLI para compartilhar o grupo, use a opção `--profile` **`ipam-account`**.

- Conclua as etapas em Desprovisionar CIDRs de um grupo para desprovisionar os CIDRs do grupo regional e, em seguida, do grupo de nível superior, nessa ordem.

Etapa 6: excluir o grupo regional e o grupo de nível superior

Esta etapa deve ser executada pela conta do IPAM. Se você estiver usando a AWS CLI para compartilhar o grupo, use a opção `--profile` **`ipam-account`**.

- Conclua as etapas em Excluir um grupo para excluir o grupo regional e, em seguida, o grupo de nível superior, nessa ordem.

Alternativa para a Etapa 6

Caso esteja usando grupos IPv4 públicos para alocar endereços IP elásticos, você pode usar as etapas desta seção em vez das etapas apresentadas na Etapa 6: alocar um endereço IP elástico do grupo.

Conteúdo

- Etapa 1: criar um grupo IPv4 público
- Etapa 2: provisionar o IPv4 CIDR público para seu grupo IPv4 público
- Etapa 3: alocar um endereço IP elástico do grupo IPv4 público
- Alternativa para a limpeza da Etapa 6

Etapa 1: criar um grupo IPv4 público

Essa etapa deve ser executada pela conta de membro que provisionará um endereço IP elástico.

> **Note**
>
> - Esta etapa deve ser executada pela conta de membro usando a AWS CLI.
> - Os grupos IPv4 públicos e os grupos do IPAM são gerenciados por recursos distintos na AWS. O grupos IPv4 públicos são recursos de conta única que permitem converter seus CIDRs de propriedade pública em endereços IP elásticos. Os grupos do IPAM podem ser usados para alocar seu espaço público para grupos do IPv4 públicos.

Para criar um grupo IPv4 público usando a AWS CLI

- Execute o comando a seguir para provisionar o CIDR. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à opção `Locale` escolhida ao criar o grupo que será usado para o CIDR de BYOIP.

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

  Na saída, você verá o ID do grupo IPv4 público. Você precisará desse ID na próxima etapa.

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

Etapa 2: provisionar o IPv4 CIDR público para seu grupo IPv4 público

Provisione o CIDR IPv4 público para seu grupo IPv4 público. O valor de `--region` deve corresponder ao valor de `Locale` escolhido ao criar o grupo que será usado para o CIDR de BYOIP. `--netmask-length` é a quantidade de espaço fora do grupo do IPAM que você deseja levar para seu grupo público. O valor não pode ser maior do que o comprimento da máscara de rede do grupo de IPAM. O `--netmask-length` menos específico que você pode definir é `24`.

> **Note**
>
> - Se você estiver trazendo um intervalo CIDR `/24` para o IPAM a fim de compartilhar em uma organização da AWS, será possível provisionar prefixos menores para vários grupos do IPAM, digamos `/27` (usando `-- netmask-length 27`) em vez de provisionar todo o CIDR `/24` (usando `-- netmask-length 24`) como mostrado neste tutorial.
> - Esta etapa deve ser executada pela conta de membro usando a AWS CLI.

Para criar um grupo IPv4 público usando a AWS CLI

1. Execute o comando a seguir para provisionar o 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
```

   Na saída, você verá o CIDR provisionado.

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

```
        "AvailableAddressCount": 256
    }
}
```

2. Execute o comando a seguir para exibir o CIDR provisionado no grupo IPv4 público.

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

Na saída, você verá o CIDR provisionado. Por padrão, o CIDR não é anunciado, o que significa que não é acessível publicamente pela Internet. Você terá a chance de definir esse CIDR como anunciado na última etapa deste tutorial.

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

Depois de criar o grupo IPv4 público, abra o console do IPAM para visualizar o grupo IPv4 público alocado no grupo regional do IPAM em Allocations (Alocações) ou em Resources (Recursos).

Etapa 3: alocar um endereço IP elástico do grupo IPv4 público

Conclua as etapas em Allocate an Elastic IP address no Guia do usuário do Amazon EC2 para alocar um endereço IP elástico (EIP) com base no grupo IPv4 público. Ao abrir o EC2 no Console

de Gerenciamento da AWS, a região da AWS em que você aloca a EIP deve corresponder à opção `Locale` escolhida ao criar o grupo que será usado para o CIDR de BYOIP.

Esta etapa deve ser executada pela conta de membro. Se você estiver usando a AWS CLI, use a opção `--profile` **`member-account`**.

Depois de concluir essas três etapas, retorne para a Etapa 7: associar um endereço IP elástico a uma instância do EC2 e continue até concluir o tutorial.

Alternativa para a limpeza da Etapa 6

Conclua estas etapas para limpar os grupos IPv4 públicos criados com a alternativa para a Etapa 9. Você deve concluir estas etapas depois de liberar o endereço IP elástico durante o processo de limpeza padrão na Etapa 8: limpeza.

Etapa 1: desprovisionar o CIDR IPv4 público do seu grupo IPv4 público

> **Important**
>
> Esta etapa deve ser executada pela conta de membro usando a AWS CLI.

1. Veja seus CIDRs de BYOIP.

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

Na saída, você verá os endereços IP em seu CIDR de 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. Execute o comando apresentado a seguir para remover o bloco CIDR do grupo público de endereços IPv4.

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

3. Visualize seus CIDRs de BYOIP novamente e verifique se não há mais endereços provisionados. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à região do seu IPAM.

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

Na saída, você verá a contagem de endereços IP em seu grupo IPv4 público.

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

> **Note**
>
> Pode levar algum tempo para o IPAM descobrir que as alocações do grupo IPv4 público foram removidas. Você não pode continuar limpando e desprovisionando o CIDR do grupo do IPAM até ver que a alocação foi removida do IPAM.

Etapa 2: excluir o grupo IPv4 público

Esta etapa deve ser executada pela conta de membro.

- Execute o comando a seguir para excluir o grupo IPv4 público do CIDR. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à opção `Locale` escolhida ao criar o grupo que será usado para o CIDR de BYOIP. Neste tutorial, esse é o seu grupo regional. Essa etapa deve ser concluída usando a AWS CLI.

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

  Na saída, você verá o valor de retorno true (verdadeiro).

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

  Depois que você excluir o grupo, para visualizar a alocação não gerenciada pelo IPAM, abra o console do IPAM e veja os detalhes do grupo regional em Allocations (Alocações).

Traga seu próprio CIDR IPv6 para o IPAM usando o Console de Gerenciamento da AWS

Siga as etapas deste tutorial para trazer um CIDR IPv6 para o IPAM e alocar uma VPC com o CIDR usando o Console de Gerenciamento e a AWS CLI da AWS.

Se você não precisar anunciar seus endereços IPv6 pela Internet, poderá provisionar um endereço GUA IPv6 privado para um IPAM. Para obter mais informações, consulte Habilitar o provisionamento de CIDRs de GUA IPv6 privado.

⚠ Important

- Para este tutorial, é necessário que você já tenha concluído as etapas nas seguintes seções:
  - Integrar o IPAM a contas em uma organização da AWS Organizations.
  - Criar um IPAM.
- Cada etapa deste tutorial deve ser executada por uma das três contas do AWS Organizations:
  - A conta de gerenciamento
  - A conta de membro configurada para ser o administrador do IPAM em Integrar o IPAM a contas em uma organização da AWS Organizations. Neste tutorial, essa conta será chamada de conta IPAM.
  - A conta de membro em sua organização que alocará CIDRs de um grupo do IPAM. Neste tutorial, essa conta será chamada de conta de membro.

Conteúdo

- Etapa 1: criar um grupo do IPAM de nível superior
- Etapa 2. Criar um grupo regional dentro de um grupo de nível superior
- Etapa 3. Compartilhar o grupo regional
- Etapa 4: criar uma VPC
- Etapa 5: anunciar o CIDR
- Etapa 6: limpeza

Etapa 1: criar um grupo do IPAM de nível superior

Como você vai criar um grupo de IPAM de nível superior com um grupo regional dentro, e vamos alocar espaço para um recurso do grupo regional, você definirá a localidade no grupo regional e não no grupo de nível superior. Você adicionará a localidade ao grupo regional ao criá-lo em uma etapa posterior. A integração do IPAM com o BYOIP exige que a localidade seja definida em qualquer grupo que será usado para o CIDR do BYOIP.

Esta etapa deve ser executada pela conta do IPAM.

Para criar um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Escolha o escopo público. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Selecione Criar.
5. (Opcional) Adicione uma Name tag (Etiqueta de nome) e uma Description (Descrição) para o grupo.
6. Em Tipo de origem, escolha Escopo do IPAM.
7. Em Address family (Família de endereços), escolha IPv6.
8. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
9. Em Locale (Local), escolha None (Nenhum). Você definirá a localidade no grupo Regional.

   A localidade é a Região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. Por exemplo, um CIDR pode ser alocado apenas para uma VPC de um grupo do IPAM que compartilhe uma localidade com a Região da VPC. Observe que, ao escolher uma localidade para um grupo, não será possível modificá-la. Se a região de origem do IPAM não estiver disponível devido a uma interrupção e o grupo tiver um local diferente da região de origem do IPAM, o grupo ainda poderá ser usado para alocar endereços IP.

   > **Note**
   >
   > Se você estiver criando apenas um único grupo e não um grupo de nível superior com grupos regionais nele, escolha uma localidade que disponibilize o grupo para alocações.

10. Em Fonte de IP público, a opção BYOIP é selecionada por padrão.
11. Em CIDRs para provisionar, faça um dos seguintes procedimentos:

    - Se você verificou seu controle do domínio com um certificado X.509, deverá incluir o CIDR, a mensagem de BYOIP e a assinatura do certificado que criou nessa etapa para que possamos confirmar que você controla o espaço público.

- Se você verificou seu controle do domínio com um registro TXT do DNS, deverá incluir o CIDR e token de verificação do IPAM criado nessa etapa para que possamos confirmar que você controla o espaço público.

Observe que, ao provisionar um CIDR IPv6 a um grupo dentro do grupo de nível superior, o intervalo de endereços IPv6 /48 é o intervalo mais específico que você trazer para CIDRs anunciáveis publicamente e /60 para CIDRs que não são anunciáveis publicamente.

> **Important**
>
> Embora a maior parte do provisionamento seja concluída em até 2 horas, a conclusão do processo de provisionamento pode levar até 1 semana para intervalos que permitam anúncios públicos.

12. Desmarque a opção Definir as configurações da regra de alocação deste grupo.
13. (Opcional) Escolha Tags (Etiquetas) para o grupo.
14. Selecione Criar.

Certifique-se de que esse CIDR tenha sido provisionado antes de continuar. Você pode ver o estado do provisionamento na guia CIDRs na página de detalhes do grupo.

Etapa 2. Criar um grupo regional dentro de um grupo de nível superior

Crie um grupo regional dentro de um grupo de nível superior. Um local é necessário no grupo e deve ser uma das regiões operacionais que você configurou ao criar o IPAM.

Esta etapa deve ser executada pela conta do IPAM.

Para criar um grupo regional dentro de um grupo de nível superior

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Se você não quiser usar o escopo privado padrão, no menu suspenso na parte superior do painel de conteúdo, escolha o escopo que deseja usar. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Selecione Criar.

5. (Opcional) Adicionar uma Name tag (Etiqueta de nome) e uma descrição para o grupo.
6. Em Origem, escolha o grupo de nível superior que você criou na seção anterior.
7. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada. Para obter informações detalhadas sobre como utilizar essa opção para planejar o espaço IP de sub-redes em uma VPC, consulte Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede.
8. Escolha o local para o grupo. A escolha de uma localidade garante que não haja dependências inter-regionais entre seu grupo e os recursos alocados a partir dele. As opções disponíveis são provenientes das regiões operacionais que você escolheu ao criar seu IPAM. Neste tutorial, usaremos `us-east-2` como o local para o grupo regional.

   A localidade é a Região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. Por exemplo, um CIDR pode ser alocado apenas para uma VPC de um grupo do IPAM que compartilhe uma localidade com a Região da VPC. Observe que, ao escolher uma localidade para um grupo, não será possível modificá-la. Se a região de origem do IPAM não estiver disponível devido a uma interrupção e o grupo tiver um local diferente da região de origem do IPAM, o grupo ainda poderá ser usado para alocar endereços IP.
9. Em Service (Serviço), escolha EC2 (EIP/VPC). O serviço selecionado determina o serviço da AWS no qual o CIDR poderá ser publicado. Atualmente, a única opção é EC2 (EIP/VPC), o que significa que os CIDRs alocados desse grupo poderão ser anunciados para o serviço Amazon EC2 e para o serviço Amazon VPC (para CIDRs associados a VPCs).
10. Em CIDRs to provision (CIDRs a provisionar), escolha a CIDR que será provisionada para o grupo. Observe que, ao provisionar um CIDR IPv6 a um grupo dentro do grupo de nível superior, o intervalo de endereços IPv6 /48 é o intervalo mais específico que você trazer para CIDRs anunciáveis publicamente e /60 para CIDRs que não são anunciáveis publicamente.
11. Marque a opção Definir as configurações da regra de alocação deste grupo e escolha regras de alocação opcionais para este grupo:

    - Importar recursos descobertos automaticamente: essa opção não está disponível se Locale (Localidade) estiver definida como None (Nenhum). Se selecionado, o IPAM busca continuamente por recursos no intervalo de CIDRs desse grupo e os importa automaticamente para seu IPAM. Observe o seguinte:
      - Os CIDRs que serão alocados para esses recursos ainda não devem ser alocados para outros recursos para que a importação seja bem-sucedida.

    - O IPAM importará um CIDR, independentemente de sua conformidade com as regras de alocação do grupo, para que um recurso possa ser importado e posteriormente marcado como não compatível.
    - Se o IPAM descobrir vários CIDRs que se sobrepõem, importará apenas o maior deles.
    - Se o IPAM descobrir vários CIDRs com CIDRs correspondentes, importará aleatoriamente apenas um deles.
- Comprimento mínimo da máscara de rede: o comprimento mínimo da máscara de rede necessário para que as alocações CIDR nesse grupo do IPAM sejam compatíveis e o bloco CIDR de maior tamanho que pode ser alocado a partir do grupo. O comprimento mínimo da máscara de rede deve ser menor que o comprimento máximo da máscara de rede. Os possíveis comprimentos de máscara de rede para endereços IPv4 são de `0` a `32`. Os possíveis comprimentos de máscara de rede para endereços IPv6 são de `0` a `128`.
- Comprimento padrão da máscara de rede: um comprimento de máscara de rede padrão para alocações adicionadas a esse grupo.
- Comprimento máximo da máscara de rede: o comprimento máximo da máscara de rede que será necessário para alocações de CIDR nesse grupo. Esse valor dita o bloco CIDR de menor tamanho que poderá ser alocado a partir do grupo. Certifique-se de que esse valor seja de no mínimo **`/48`**.
- Requisitos de marcação: as tags necessárias para que os recursos aloquem espaço do grupo. Se os recursos tiverem suas tags alteradas depois de terem alocado espaço ou se as regras de marcação de alocação forem alteradas no grupo, o recurso poderá ser marcado como não compatível.
- Localidade: a localidade que será necessária para recursos que usam CIDRs desse grupo. Recursos importados automaticamente que não tiverem essa localidade serão marcados como não compatíveis. Os recursos que não são importados automaticamente para o grupo não terão permissão para alocar espaço do grupo, a menos que estejam nessa localidade.

12. (Opcional) Escolha Tags (Etiquetas) para o grupo.
13. Ao terminar de configurar o grupo, escolha Create pool (Criar grupo).

Certifique-se de que esse CIDR tenha sido provisionado antes de continuar. Você pode ver o estado do provisionamento na guia CIDRs na página de detalhes do grupo.

Etapa 3. Compartilhar o grupo regional

Siga as etapas nesta seção para compartilhar o grupo de IPAM usando o AWS Resource Access Manager (RAM).

Habilitar o compartilhamento de recursos no AWS RAM

Depois de criar seu IPAM, você desejará compartilhar o grupo regional com outras contas em sua organização. Antes de compartilhar um grupo do IPAM, conclua as etapas nesta seção para habilitar o compartilhamento de recursos com o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`management-account`**.

Para habilitar o compartilhamento de recursos

1. Com a conta gerencial do AWS Organizations, abra o console do AWS RAM em https://console.aws.amazon.com/ram/.
2. No painel de navegação esquerdo, escolha Configurações, depois Habilitar compartilhamento com o AWS Organizations e escolha Salvar configurações.

Agora você pode compartilhar um grupo do IPAM com outros membros da organização.

Compartilhar um grupo do IPAM usando o AWS RAM

Nesta seção, você compartilhará o grupo regional com outra conta de membro do AWS Organizations. Para obter instruções completas sobre o compartilhamento de grupos do IPAM, incluindo informações sobre as permissões necessárias do IAM, consulte Compartilhar um grupo do IPAM usando o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`ipam-account`**.

Para compartilhar um grupo do IPAM usando o AWS RAM

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado, o grupo de IPAM e Ações > Visualizar detalhes.
4. Em Resource sharing (Compartilhamento de recursos), escolha Create resource share (Criar compartilhamento de recursos). O console do AWS RAM será aberto. Você compartilhará o grupo usando o AWS RAM.
5. Escolha Create a resource share (Criar um compartilhamento de recursos).

6. No console do AWS RAM, escolha Criar um compartilhamento de recursos novamente.
7. Adicione um Nome para o recurso compartilhado.
8. Em Selecionar tipo de recurso, escolha Grupos do IPAM e, em seguida, escolha o ARN do grupo que deseja compartilhar.
9. Escolha Próximo.
10. Escolha a permissão AWSRAMPermissionIpamPoolByoipCidrImport. Os detalhes das opções de permissão estão fora do escopo deste tutorial, mas você pode descobrir mais sobre essas opções em Compartilhar um grupo do IPAM usando o AWS RAM.
11. Escolha Próximo.
12. Em Entidades principais > Selecionar tipo de entidade principal, escolha Conta da AWS e insira o ID da conta que trará um intervalo de endereços IP para o IPAM e escolha Adicionar.
13. Escolha Próximo.
14. Revise as opções de compartilhamento de recursos e as entidades principais com as quais você compartilhará e escolha Criar.
15. Para permitir que a conta da **`member-account`** aloque o endereço IP CIDRS do grupo do IPAM, crie um segundo compartilhamento de recursos com `AWSRAMDefaultPermissionsIpamPool`. O valor para `--resource-arns` é o ARN do grupo do IPAM criado na seção anterior. O valor para `--principals` é o ID de **`member-account`**. O valor para `--permission-arns` é o ARN da permissão `AWSRAMDefaultPermissionsIpamPool`.

Etapa 4: criar uma VPC

Conclua as etapas descritas em Crie uma VPC no Guia do usuário da Amazon VPC.

Esta etapa deve ser executada pela conta de membro.

> **Note**
>
> - Ao abrir o VPC no Console de Gerenciamento da AWS, a região da AWS em que você cria a VPC deve corresponder à opção `Locale` escolhida ao criar o grupo que será usado para o CIDR de BYOIP.
> - Ao chegar à etapa de escolher um CIDR para a VPC, você terá a opção de usar um CIDR de um grupo do IPAM. Escolha o grupo regional que você criou neste tutorial.

Ao criar a VPC, a AWS aloca um CIDR no grupo do IPAM para a VPC. Você pode visualizar a alocação no IPAM escolhendo um grupo no painel de conteúdo do console do IPAM e exibindo a guia Allocations (Alocações) do grupo.

Etapa 5: anunciar o CIDR

As etapas nesta seção devem ser realizadas pela conta do IPAM. Após criar a VPC, você pode começar a anunciar o CIDR que trouxe para a AWS que está no grupo que tem EC2 Service (EIP/VPC) [Serviço EC2 (EIP/VPC)] configurado. Neste tutorial, esse é o seu grupo regional. Por padrão, o CIDR não é anunciado, o que significa que não é acessível publicamente pela Internet.

Esta etapa deve ser executada pela conta do IPAM.

Para anunciar o CIDR

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Escolha o escopo público. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Escolha o grupo regional que você criou neste tutorial.
5. Escolha a guia CIDRs.
6. Selecione o CIDR de BYOIP e escolha Actions (Ações) >Advertise (Anunciar).
7. Escolha Advertise CIDR (Anunciar CIDR).

Como resultado, o CIDR BYOIP é anunciado e o valor na coluna Advertising (Publicidade) muda de Withdrawn (Retirado) para Advertised (Anunciado).

Etapa 6: limpeza

Siga as etapas desta seção para limpar os recursos que você provisionou e criou neste tutorial.

Etapa 1: retirar o CIDR da publicidade

Esta etapa deve ser executada pela conta do IPAM.

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Por padrão, quando você cria um grupo, o escopo privado padrão é selecionado. Escolha o escopo público.

4. Escolha o grupo regional que você criou neste tutorial.
5. Escolha a guia CIDRs.
6. Selecione o CIDR de BYOIP e escolha Actions (Ações) >Withdraw from advertising (Retirar da publicidade).
7. Selecione Withdraw CIDR (Retirar CIDR).

Como resultado, o CIDR de BYOIP é anunciado e o valor na coluna Advertising (Publicidade) muda de Advertised (Anunciado) para Withdrawn (Retirado).

Etapa 2: excluir a VPC

Esta etapa deve ser executada pela conta de membro.

- Conclua as etapas descritas em Excluir a VPC no Guia do usuário da Amazon VPC para excluir a VPC. Ao abrir a VPC no Console de Gerenciamento da AWS, a região da AWS da qual você excluir a VPC deve corresponder à opção `Locale` escolhida ao criar o grupo que será usado para o CIDR de BYOIP. Neste tutorial, esse é o seu grupo regional.

  Quando você exclui a VPC, leva algum tempo para o IPAM descobrir que o recurso foi excluído e desalocar o CIDR alocado para a VPC. Não é possível prosseguir para a próxima etapa na limpeza até você ver que o IPAM removeu a alocação do grupo na guia Allocations (Alocações) de detalhes do grupo.

Etapa 3: excluir os compartilhamentos do RAM e desabilitar a integração do RAM com o AWS Organizations

Esta etapa deve ser executada pela conta do IPAM e pela conta gerencial, respectivamente.

- Conclua as etapas em Excluir um compartilhamento de recursos no AWS RAM e Desabilitar o compartilhamento de recursos com o AWS Organizations no Guia do usuário do AWS RAM, nessa ordem, para excluir o compartilhamento do RAM e desabilitar a integração do RAM com o AWS Organizations.

Etapa 4: desprovisionar os CIDRs do grupo regional e do grupo de nível superior

Esta etapa deve ser executada pela conta do IPAM.

- Conclua as etapas em Desprovisionar CIDRs de um grupo para desprovisionar os CIDRs do grupo regional e, em seguida, do grupo de nível superior, nessa ordem.

Etapa 5: excluir o grupo regional e o grupo de nível superior

Esta etapa deve ser executada pela conta do IPAM.

- Conclua as etapas em Excluir um grupo para excluir o grupo regional e, em seguida, o grupo de nível superior, nessa ordem.

Trazer seu próprio CIDR IP para o IPAM usando apenas a AWS CLI

Trazer seu próprio IP (BYOIP) para o IPAM permite que você use os intervalos de endereços IPv4 e IPv6 existentes da sua organização na AWS. Isso permite que você mantenha uma marca consistente, melhore a performance da rede, aprimore a segurança e simplifique o gerenciamento, unificando ambientes on-premises e na nuvem em seu próprio espaço de endereços IP.

Siga estas etapas para trazer um CIDR IPv4 ou IPv6 para o IPAM usando apenas a AWS CLI.

> **Note**
>
> Antes de começar, você deve ter o controle do domínio verificado.

Se você trouxer um intervalo de endereços IPv4 para a AWS, poderá usar todos os endereços IP do intervalo, incluindo o primeiro endereço (o endereço de rede) e o último endereço (o endereço de broadcast).

Conteúdo

- Traga seu próprio CIDR IPv4 público para o IPAM usando somente a AWS CLI
- Traga seu próprio CIDR IPv6 para o IPAM usando somente a AWS CLI

Traga seu próprio CIDR IPv4 público para o IPAM usando somente a AWS CLI

Siga estas etapas para trazer um CIDR IPv4 para o IPAM e alocar um endereço IP elástico (EIP) com o CIDR usando somente a AWS CLI.

Important

- Para este tutorial, é necessário que você já tenha concluído as etapas nas seguintes seções:
  - Integrar o IPAM a contas em uma organização da AWS Organizations.
  - Criar um IPAM.
- Cada etapa deste tutorial deve ser executada por uma das três contas do AWS Organizations:
  - A conta de gerenciamento
  - A conta de membro configurada para ser o administrador do IPAM em Integrar o IPAM a contas em uma organização da AWS Organizations. Neste tutorial, essa conta será chamada de conta IPAM.
  - A conta de membro em sua organização que alocará CIDRs de um grupo do IPAM. Neste tutorial, essa conta será chamada de conta de membro.

Conteúdo

- Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM
- Etapa 2: criar um IPAM
- Etapa 3: criar um grupo do IPAM de nível superior
- Etapa 4: provisionar um CIDR para o grupo de nível superior
- Etapa 5: criar um grupo regional dentro de um grupo de nível superior
- Etapa 6: provisionar um CIDR para o grupo regional
- Etapa 7: anunciar o CIDR
- Etapa 8: compartilhar o grupo regional
- Etapa 9: alocar um endereço IP elástico do grupo
- Etapa 10: associar um endereço IP elástico a uma instância do EC2
- Etapa 11: limpeza
- Alternativa para a Etapa 9

Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM

Para concluir este tutorial como um usuário da AWS, você pode usar os perfis nomeados da AWS CLI para alternar de um perfil do IAM para outro. Perfis nomeados são coleções de configurações e credenciais às quais você se refere ao usar a opção `--profile` com a AWS CLI. Para obter mais informações sobre como criar perfis do IAM e perfis nomeados para contas da AWS, consulte Uso de perfis do IAM na AWS CLI.

Crie uma função e um perfil nomeado para cada uma das três contas da AWS que você usará neste tutorial:

- Um perfil chamado `management-account` para a conta de gerenciamento do AWS Organizations.
- Um perfil chamado `ipam-account` para a conta de membro do AWS Organizations configurada para ser o administrador do IPAM.
- Um perfil chamado `member-account` para a conta de membro do AWS Organizations em sua organização que alocará CIDRs de um grupo do IPAM.

Depois de criar os perfis do IAM e os perfis nomeados, volte para esta página e vá para a próxima etapa. Você notará, ao longo do restante deste tutorial, que os exemplos de comandos da AWS CLI usam a opção `--profile` com um dos perfis nomeados para indicar qual conta deve executar o comando.

Etapa 2: criar um IPAM

Esta etapa é opcional. Se você criou um IPAM com as regiões operacionais `us-east-1` e `us-west-2`, pode ignorar esta etapa. Crie um IPAM e especifique uma região operacional `us-east-1` e `us-west-2`. Você deve selecionar uma região operacional para que você possa usar a opção de localidade ao criar seu grupo do IPAM. A integração do IPAM com o BYOIP exige que a localidade seja definida em qualquer grupo que será usado para o CIDR do BYOIP.

Esta etapa deve ser realizadas pela conta do IPAM.

Execute o seguinte comando:

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

Na saída, você verá o IPAM que criou. Observe o valor para `PublicDefaultScopeId`. Você precisará do ID do escopo público na próxima etapa. Você está usando o escopo público porque os CIDRs de BYOIP são endereços IP públicos, e é para isso que o escopo público se destina.

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

Etapa 3: criar um grupo do IPAM de nível superior

Conclua as etapas nesta seção para criar um grupo do IPAM de nível superior.

Esta etapa deve ser realizadas pela conta do IPAM.

Para criar um grupo de endereços IPv4 para todos os seus recursos da AWS usando a AWS CLI

1. Execute o comando a seguir para criar um grupo do IPAM. Use o ID do escopo público do IPAM criado na etapa anterior.

   Esta etapa deve ser realizadas pela conta do 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
   ```

Na saída, você verá `create-in-progress`, o que indica que a criação do grupo está em andamento.

```
{
    "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. Execute o comando a seguir até ver um estado `create-complete` na saída.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

O exemplo a seguir mostra o estado do grupo.

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

Etapa 4: provisionar um CIDR para o grupo de nível superior

Provisione um bloco de CIDR para o grupo de nível superior. Observe que, ao provisionar um CIDR IPv4 para um grupo dentro do grupo de nível superior, o CIDR IPv4 mínimo que você pode provisionar é `/24`. CIDRs mais específicos (como `/25`) não são permitidos.

> **Note**
>
> - Se você verificou seu controle do domínio com um certificado X.509, deverá incluir o CIDR, a mensagem de BYOIP e a assinatura do certificado que criou nessa etapa para que possamos confirmar que você controla o espaço público.
> - Se você verificou seu controle do domínio com um registro TXT do DNS, deverá incluir o CIDR e token de verificação do IPAM criado nessa etapa para que possamos confirmar que você controla o espaço público.

Você só precisa verificar o controle do domínio quando provisiona o CIDR de BYOIP para o grupo superior. Para o grupo regional dentro do grupo superior, você pode omitir a opção de verificação de controle do domínio.

Esta etapa deve ser executada pela conta do IPAM.

> **Important**
>
> Você só precisa verificar o controle do domínio quando provisiona o CIDR de BYOIP para o grupo superior. Para o grupo regional dentro do grupo de nível superior, você pode omitir a opção de controle do domínio. Depois de integrar seu BYOIP ao IPAM, você não precisará executar a validação de propriedade ao dividir o BYOIP entre regiões e contas.

Para provisionar um bloco CIDR para o grupo usando o AWS CLI

1. Para provisionar o CIDR com as informações de certificado, use o exemplo de comando a seguir. Além de substituir os valores conforme necessário no exemplo, certifique-se de substituir os valores de `Message` e `Signature` pelos valores de `text_message` e `signed_message` que você obteve em Verificar seu domínio com um certificado 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~KCIsMaU0P7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRYOdRaNx8yt-uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

Para provisionar o CIDR com as informações do token de verificação, use o exemplo de comando a seguir. Além de substituir os valores no exemplo conforme necessário, certifique-se de substituir `ipam-ext-res-ver-token-0309ce7f67a768cf0` pelo ID do token `IpamExternalResourceVerificationTokenId` que você obteve em Verifique seu domínio com um registro TXT do DNS.

```
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
```

Na saída, você verá a provisão pendente do CIDR.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Certifique-se de que esse CIDR tenha sido provisionado antes de continuar.

> **Important**
>
> Embora a maior parte do provisionamento seja concluída em até 2 horas, a conclusão do processo de provisionamento pode levar até 1 semana para intervalos que permitam anúncios públicos.

Execute o comando a seguir até ver um estado `provisioned` na saída.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

O exemplo de saída a seguir mostra o estado.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

Etapa 5: criar um grupo regional dentro de um grupo de nível superior

Crie um grupo regional dentro de um grupo de nível superior.

A localidade do grupo deve ser uma das seguintes opções:

- Uma região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações.
- O grupo de borda de rede para uma Zona local da AWS em que você quer disponibilizar esse grupo do IPAM para alocações (Zonas locais com suporte). Essa opção está disponível somente para grupos IPv4 de IPAM no escopo público.
- Uma Zona local dedicada da AWS. Para criar um grupo dentro de uma Zona local dedicada da AWS, insira a Zona local dedicada da AWS na entrada do seletor.

- `Global` quando você quiser usar endereços IP globalmente em todas as regiões da AWS, como locais do CloudFront. A localidade `Global` só está disponível para grupos IPv4 públicos.

Por exemplo, um CIDR pode ser alocado apenas para uma VPC de um grupo do IPAM que compartilhe uma localidade com a Região da VPC. Observe que, ao escolher uma localidade para um grupo, não será possível modificá-la. Se a região de origem do IPAM não estiver disponível devido a uma interrupção e o grupo tiver um local diferente da região de origem do IPAM, o grupo ainda poderá ser usado para alocar endereços IP.

Ao executar os comandos nesta seção, o valor de `--region` deve incluir a opção `--locale` inserida ao criar o grupo que será usado para o CIDR de BYOIP. Por exemplo, se você criou o grupo BYOIP com a localidade us-east-1, `--region` deverá ser us-east-1. Se você criou o grupo BYOIP com a localidade us-east-1-scl-1 (um grupo de borda de rede usado para Zonas locais), `--region` deverá ser us-east-1 porque essa região gerencia a localidade us-east-1-scl-1.

Esta etapa deve ser executada pela conta do IPAM.

A escolha de uma localidade garante que não haja dependências inter-regionais entre seu grupo e os recursos alocados a partir dele. As opções disponíveis são provenientes das regiões operacionais que você escolheu ao criar seu IPAM. Neste tutorial, usaremos `us-west-2` como o local para o grupo regional.

> **Important**
>
> Ao criar o grupo, é necessário incluir `--aws-service ec2`. O serviço selecionado determina o serviço da AWS no qual o CIDR poderá ser publicado. No momento, a única opção é `ec2`, ou seja, os CIDRs alocados a partir desse grupo poderão ser publicados no serviço Amazon EC2 (para endereços IP elásticos) e no serviço Amazon VPC (para CIDRs associados a VPCs).

Para criar um grupo regional usando a AWS CLI

1. Execute o comando a seguir para criar o grupo.

```
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
```

Na saída, você verá o IPAM criando o grupo.

```
{
     "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. Execute o comando a seguir até ver um estado `create-complete` na saída.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Na saída, você vê os grupos que tem no IPAM. Neste tutorial, criamos um grupo regional e um de nível superior. Você verá ambos.

Etapa 6: provisionar um CIDR para o grupo regional

Provisione um bloco CIDR para o grupo regional.

> **Note**
>
> Quando um CIDR é provisionado para um grupo regional dentro do grupo de nível superior, o CIDR IPv4 mais específico que você pode provisionar é `/24`. CIDRs mais específicos (como `/25`) não são permitidos. Depois de criar o grupo regional, você poderá criar grupos menores

(como /25) dentro do mesmo grupo regional. Observe que, se você compartilhar o pool regional ou os pools nele contidos, esses pools só poderão ser usados na localidade definida no mesmo pool regional.

Esta etapa deve ser executada pela conta do IPAM.

Para atribuir um bloco CIDR ao grupo regional usando a AWS CLI

1. Execute o comando a seguir para provisionar o 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
```

   Na saída, você verá a provisão pendente do CIDR.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Execute o comando a seguir até ver um estado `provisioned` na saída.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   O exemplo de saída a seguir mostra o estado correto.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
```

```
}
```

Etapa 7: anunciar o CIDR

As etapas nesta seção devem ser realizadas pela conta do IPAM. Depois de associar o endereço IP elástico (EIP) a uma instância ou Elastic Load Balancer, você pode começar a anunciar o CIDR que trouxe para a AWS que está no grupo com `--aws-service ec2` definido. Neste tutorial, esse é o seu grupo regional. Por padrão, o CIDR não é anunciado, o que significa que não é acessível publicamente pela Internet. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo que será usado para o CIDR de BYOIP.

Esta etapa deve ser executada pela conta do IPAM.

> **Note**
>
> O status do anúncio não restringe sua capacidade de alocar endereços IP elásticos. Mesmo que seu BYOIPv4 CIDR não seja anunciado, você ainda pode criar EIPs do grupo do IPAM.

Comece anunciando o CIDR usando a AWS CLI

- Execute o comando a seguir para anunciar o CIDR.

  ```
  aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
  profile ipam-account
  ```

  Na saída, você verá o CIDR anunciado.

  ```
  {
      "ByoipCidr": {
          "Cidr": "130.137.245.0/24",
          "State": "advertised"
      }
  }
  ```

Etapa 8: compartilhar o grupo regional

Siga as etapas nesta seção para compartilhar o grupo de IPAM usando o AWS Resource Access Manager (RAM).

Habilitar o compartilhamento de recursos no AWS RAM

Depois de criar seu IPAM, você desejará compartilhar o grupo regional com outras contas em sua organização. Antes de compartilhar um grupo do IPAM, conclua as etapas nesta seção para habilitar o compartilhamento de recursos com o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`management-account`**.

Para habilitar o compartilhamento de recursos

1. Com a conta de gerenciamento do AWS Organizations, abra o console do AWS RAM em https://console.aws.amazon.com/ram/.
2. No painel de navegação esquerdo, escolha Configurações, depois Habilitar compartilhamento com o AWS Organizations e escolha Salvar configurações.

Agora você pode compartilhar um grupo do IPAM com outros membros da organização.

Compartilhar um grupo do IPAM usando o AWS RAM

Nesta seção, você compartilhará o grupo regional com outra conta de membro do AWS Organizations. Para obter instruções completas sobre o compartilhamento de grupos do IPAM, incluindo informações sobre as permissões necessárias do IAM, consulte Compartilhar um grupo do IPAM usando o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`ipam-account`**.

Para compartilhar um grupo do IPAM usando o AWS RAM

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado, o grupo de IPAM e Ações > Visualizar detalhes.
4. Em Resource sharing (Compartilhamento de recursos), escolha Create resource share (Criar compartilhamento de recursos). O console do AWS RAM será aberto. Você compartilhará o grupo usando o AWS RAM.
5. Escolha Create a resource share (Criar um compartilhamento de recursos).
6. No console do AWS RAM, escolha Criar um compartilhamento de recursos novamente.
7. Adicione um Nome para o recurso compartilhado.

8. Em Selecionar tipo de recurso, escolha Grupos do IPAM e, em seguida, escolha o ARN do grupo que deseja compartilhar.
9. Escolha Próximo.
10. Escolha a permissão AWSRAMPermissionIpamPoolByoipCidrImport. Os detalhes das opções de permissão estão fora do escopo deste tutorial, mas você pode descobrir mais sobre essas opções em Compartilhar um grupo do IPAM usando o AWS RAM.
11. Escolha Próximo.
12. Em Entidades principais > Selecionar tipo de entidade principal, escolha Conta da AWS e insira o ID da conta que trará um intervalo de endereços IP para o IPAM e escolha Adicionar.
13. Escolha Avançar.
14. Revise as opções de compartilhamento de recursos e as entidades principais com as quais você compartilhará e escolha Criar.
15. Para permitir que a conta da **`member-account`** aloque o endereço IP CIDRS do grupo do IPAM, crie um segundo compartilhamento de recursos com `AWSRAMDefaultPermissionsIpamPool`. O valor para `--resource-arns` é o ARN do grupo do IPAM criado na seção anterior. O valor para `--principals` é o ID de **`member-account`**. O valor para `--permission-arns` é o ARN da permissão `AWSRAMDefaultPermissionsIpamPool`.

Etapa 9: alocar um endereço IP elástico do grupo

Conclua as etapas desta seção para alocar um endereço IP elástico do grupo. Observe que se estiver usando grupos IPv4 públicos para alocar endereços IP elásticos, você poderá usar as etapas alternativas em Alternativa para a Etapa 9 em vez das etapas desta seção.

> **Important**
>
> Se você encontrar um erro relacionado à falta de permissões para chamar ec2:AllocateAddress, é necessário atualizar a permissão gerenciada atualmente atribuída ao grupo do IPAM compartilhado com você. Recomendamos entrar em contato com a pessoa responsável pela criação do compartilhamento de recursos e solicitar a atualização da permissão gerenciada de `AWSRAMPermissionIpamResourceDiscovery` para a versão mais recente. Para obter detalhes adicionais, consulte Atualização de um compartilhamento de recursos no Guia do Usuário AWS RAM.

AWS Management Console

Siga as etapas em Allocate an Elastic IP address no Guia do usuário do Amazon EC2 para alocar o endereço, mas observe o seguinte:

- Esta etapa deve ser executada pela conta de membro.
- Certifique-se de que a região da AWS em que você está no console do EC2 corresponda à opção de localidade que você escolheu ao criar o grupo regional.
- Ao escolher o grupo de endereços, escolha a opção Alocar usando um grupo IPV4 do IPAM e depois o grupo regional que você criou.

Command line

Aloque um endereço do grupo com o comando allocate-address. A `--region` que você usa deve corresponder à opção de `-locale` que você escolheu quando criou o grupo na Etapa 2. Inclua o ID do grupo do IPAM que você criou na Etapa 2 em `--ipam-pool-id`. Opcionalmente, você também pode escolher um `/32` específico em seu grupo do IPAM usando a opção `--address`.

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

Exemplo de resposta:

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

Para obter mais informações, consulte Allocate an Elastic IP address no Guia do usuário do Amazon EC2.

Etapa 10: associar um endereço IP elástico a uma instância do EC2

Conclua as etapas desta seção para associar um endereço IP elástico a uma instância do EC2.

AWS Management Console

Siga as etapas em Associate an Elastic IP address no Guia do usuário do Amazon EC2 para alocar um endereço IP elástico do grupo do IPAM, mas observe o seguinte: quando você usa a opção Console de Gerenciamento da AWS, a região da AWS à qual você associa o endereço IP elástico deve corresponder à opção de localidade que você escolheu ao criar o grupo regional.

Esta etapa deve ser executada pela conta de membro.

Command line

Esta etapa deve ser executada pela conta de membro. Use a opção `--profile` **`member-account`**.

Associe o endereço IP elástico a uma instância com o comando associate-address. A `--region` à qual você associa o endereço IP elástico deve corresponder à opção de `--locale` que você escolheu quando criou o grupo regional.

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

Exemplo de resposta:

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

Para obter mais informações, consulte Associate an Elastic IP address with an instance or network interface no Guia do usuário do Amazon EC2.

Etapa 11: limpeza

Siga as etapas desta seção para limpar os recursos que você provisionou e criou neste tutorial. Ao executar os comandos nesta seção, o valor de `--region` deve incluir a opção `--locale` inserida ao criar o grupo que será usado para o CIDR de BYOIP.

Limpar usando a AWS CLI

1. Veja a alocação de EIP gerenciada no IPAM.

Esta etapa deve ser realizadas pela conta do IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

A saída mostra a alocação no 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. Pare de anunciar o CIDR IPv4.

   Esta etapa deve ser realizadas pela conta do IPAM.

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
   profile ipam-account
   ```

   Na saída, você verá que o estado do CIDR mudou de advertised (anunciado) para provisioned (provisionado).

   ```
   {
       "ByoipCidr": {
           "Cidr": "130.137.245.0/24",
           "State": "provisioned"
       }
   }
   ```

3. Libere os endereços IP elásticos.

   Esta etapa deve ser realizadas pela conta de membro.

```
aws ec2 release-address --region us-west-2 --allocation-
id eipalloc-0db3405026756dbf6 --profile member-account
```

Você não verá nenhuma saída ao executar esse comando.

4. Veja que a alocação de EIP não é mais gerenciada no IPAM. Pode levar algum tempo para o IPAM descobrir que o endereço IP elástico foi removido. Você não pode continuar limpando e desprovisionando o CIDR do grupo do IPAM até ver que a alocação foi removida do IPAM. Ao executar o comando nesta seção, o valor de `--region` deve incluir a opção `--locale` inserida ao criar o grupo que será usado para o CIDR de BYOIP.

   Esta etapa deve ser executada pela conta do IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   A saída mostra a alocação no IPAM.

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

5. Desprovisione o CIDR do grupo regional. Ao executar os comandos nesta etapa, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa deve ser realizadas pela conta do 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
   ```

   Na saída, você verá o desprovisionamento pendente do CIDR.

   ```
   {
       "IpamPoolCidr": {

           "Cidr": "130.137.245.0/24",

           "State": "pending-deprovision"
   ```

```
    }

}
```

O desprovisionamento demora para ser concluído. Verifique o status do desprovisionamento.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Espere até ver deprovisioned (desprovisionado) antes de continuar para a próxima etapa.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

6. Exclua os compartilhamentos do RAM e desabilite a integração do RAM com o AWS Organizations. Conclua as etapas em Excluir um compartilhamento de recursos no AWS RAM e Desabilitar o compartilhamento de recursos com o AWS Organizations no Guia do usuário do AWS RAM, nessa ordem, para excluir os compartilhamentos do RAM e desabilitar a integração do RAM com o AWS Organizations.

   Esta etapa deve ser executada pela conta do IPAM e pela conta de gerenciamento, respectivamente. Se você estiver usando o AWS CLI para excluir os compartilhamentos do RAM e desabilitar a integração do RAM, use as opções `--profile` **`ipam-account`** e `--profile` **`management-account`**.

7. Exclua o grupo regional. Ao executar o comando nesta etapa, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa deve ser realizadas pela conta do IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Na saída, você pode ver o estado de exclusão.

```
{
   "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. Desprovisione o CIDR do grupo de nível superior. Ao executar os comandos nesta etapa, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa deve ser realizadas pela conta do 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
```

   Na saída, você verá o desprovisionamento pendente do CIDR.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"
```

```
    }

}
```

O desprovisionamento demora para ser concluído. Use o comando a seguir para verificar o status do desprovisionamento.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Espere até ver deprovisioned (desprovisionado) antes de continuar para a próxima etapa.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. Exclua grupo de nível superior. Ao executar o comando nesta etapa, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa deve ser realizadas pela conta do IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

   Na saída, você pode ver o estado de exclusão.

```
{
  "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. Exclua o IPAM Ao executar o comando nesta etapa, o valor de `--region` deve corresponder à região do seu IPAM.

    Esta etapa deve ser realizadas pela conta do IPAM.

    ```
    aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
    profile ipam-account
    ```

    Na saída, você verá a resposta do IPAM. Isso significa que o IPAM foi excluído.

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

Alternativa para a Etapa 9

Caso esteja usando grupos IPv4 públicos para alocar endereços IP elásticos, você pode usar as etapas desta seção em vez das etapas apresentadas na Etapa 9: alocar um endereço IP elástico do grupo.

Conteúdo

- Etapa 1: criar um grupo IPv4 público
- Etapa 2: provisionar o IPv4 CIDR público para seu grupo IPv4 público
- Etapa 3: criar um endereço IP elástico do grupo IPv4 público
- Alternativa para a limpeza da Etapa 9

Etapa 1: criar um grupo IPv4 público

Normalmente, esta etapa seria realizada por uma conta da AWS diferente que deseja provisionar um endereço IP elástico, como o membro da conta.

> **Important**
>
> Os grupos IPv4 públicos e os grupos do IPAM são gerenciados por recursos distintos na AWS. O grupos IPv4 públicos são recursos de conta única que permitem converter seus CIDRs de propriedade pública em endereços IP elásticos. Os grupos do IPAM podem ser usados para alocar seu espaço público para grupos do IPv4 públicos.

Para criar um grupo IPv4 público usando a AWS CLI

- Execute o comando a seguir para provisionar o CIDR. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo que será usado para o CIDR de BYOIP.

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

Na saída, você verá o ID do grupo IPv4 público. Você precisará desse ID na próxima etapa.

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

Etapa 2: provisionar o IPv4 CIDR público para seu grupo IPv4 público

Provisione o CIDR IPv4 público para seu grupo IPv4 público. O valor de `--region` deve corresponder ao valor de `--locale` inserido ao criar o grupo que será usado para o CIDR de BYOIP. O `--netmask-length` menos específico que você pode definir é `24`.

Esta etapa deve ser executada pela conta de membro.

Para criar um grupo IPv4 público usando a AWS CLI

1. Execute o comando a seguir para provisionar o 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
```

Na saída, você verá o CIDR provisionado.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. Execute o comando a seguir para exibir o CIDR provisionado no grupo IPv4 público.

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-
account
```

Na saída, você verá o CIDR provisionado. Por padrão, o CIDR não é anunciado, o que significa que não é acessível publicamente pela Internet. Você terá a chance de definir esse CIDR como anunciado na última etapa deste tutorial.

```
{
    "ByoipCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "StatusMessage": "Cidr successfully provisioned",
            "State": "provisioned"
        }
    ]
}
```

Etapa 3: criar um endereço IP elástico do grupo IPv4 público

Crie um endereço IP elástico (EIP) do grupo IPv4 público. Ao executar os comandos nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo que será usado para o CIDR de BYOIP.

Esta etapa deve ser realizadas pela conta de membro.

Para criar um EIP do grupo IPv4 público usando a AWS CLI

1. Execute o comando da a seguir para criar o EIP.

```
aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
ec2-0019eed22a684e0b2 --profile member-account
```

Na saída, você verá a alocação.

```
{
    "PublicIp": "130.137.245.100",
    "AllocationId": "eipalloc-0db3405026756dbf6",
    "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
    "NetworkBorderGroup": "us-east-1",
```

```
    "Domain": "vpc"
}
```

2. Execute o comando a seguir para visualizar a alocação de EIP gerenciada no IPAM.

   Esta etapa deve ser realizadas pela conta do IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   A saída mostra a alocação no IPAM.

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "130.137.245.0/24",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
               "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
               "ResourceType": "ec2-public-ipv4-pool",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

Alternativa para a limpeza da Etapa 9

Conclua estas etapas para limpar os grupos IPv4 públicos criados com a alternativa para a Etapa 9. Você deve concluir estas etapas depois de liberar o endereço IP elástico durante o processo de limpeza padrão na Etapa 10: limpeza.

1. Veja seus CIDRs de BYOIP.

   Esta etapa deve ser realizadas pela conta de membro.

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

   Na saída, você verá os endereços IP em seu CIDR de 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. Remova o bloco CIDR do grupo público de endereços IPv4. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa deve ser executada pela conta de membro.

```
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. Visualize seus CIDRs de BYOIP novamente e verifique se não há mais endereços provisionados. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa deve ser realizadas pela conta de membro.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
```

   Na saída, você verá a contagem de endereços IP em seu grupo IPv4 público.

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

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

Traga seu próprio CIDR IPv6 para o IPAM usando somente a AWS CLI

Siga estas etapas para trazer um CIDR IPv6 para o IPAM e alocar uma VPC usando somente a AWS CLI.

Se você não precisar anunciar seus endereços IPv6 pela Internet, poderá provisionar um endereço GUA IPv6 privado para um IPAM. Para obter mais informações, consulte Habilitar o provisionamento de CIDRs de GUA IPv6 privado.

Important

- Para este tutorial, é necessário que você já tenha concluído as etapas nas seguintes seções:
  - Integrar o IPAM a contas em uma organização da AWS Organizations.
  - Criar um IPAM.
- Cada etapa deste tutorial deve ser executada por uma das três contas do AWS Organizations:
  - A conta gerencial
  - A conta de membro configurada para ser o administrador do IPAM em Integrar o IPAM a contas em uma organização da AWS Organizations. Neste tutorial, essa conta será chamada de conta IPAM.
  - A conta de membro em sua organização que alocará CIDRs de um grupo do IPAM. Neste tutorial, essa conta será chamada de conta de membro.

Conteúdo

- Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM

- Etapa 2: criar um IPAM
- Etapa 3: criar um grupo do IPAM
- Etapa 4: provisionar um CIDR para o grupo de nível superior
- Etapa 5: criar um grupo regional dentro de um grupo de nível superior
- Etapa 6: provisionar um CIDR para o grupo regional
- Etapa 7. Compartilhar o grupo regional
- Etapa 8: criar uma VPC usando o CIDR IPv6
- Etapa 9: anunciar o CIDR
- Etapa 10: limpeza

Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM

Para concluir este tutorial como um usuário da AWS, você pode usar os perfis nomeados da AWS CLI para alternar de um perfil do IAM para outro. Perfis nomeados são coleções de configurações e credenciais às quais você se refere ao usar a opção `--profile` com a AWS CLI. Para obter mais informações sobre como criar perfis do IAM e perfis nomeados para contas da AWS, consulte Uso de perfis do IAM na AWS CLI.

Crie uma função e um perfil nomeado para cada uma das três contas da AWS que você usará neste tutorial:

- Um perfil chamado `management-account` para a conta gerencial do AWS Organizations.
- Um perfil chamado `ipam-account` para a conta de membro do AWS Organizations configurada para ser o administrador do IPAM.
- Um perfil chamado `member-account` para a conta de membro do AWS Organizations em sua organização que alocará CIDRs de um grupo do IPAM.

Depois de criar os perfis do IAM e os perfis nomeados, volte para esta página e vá para a próxima etapa. Você notará, ao longo do restante deste tutorial, que os exemplos de comandos da AWS CLI usam a opção `--profile` com um dos perfis nomeados para indicar qual conta deve executar o comando.

Etapa 2: criar um IPAM

Esta etapa é opcional. Se você criou um IPAM com as regiões operacionais `us-east-1` e `us-west-2`, pode ignorar esta etapa. Crie um IPAM e especifique uma região operacional `us-east-1`

e `us-west-2`. Você deve selecionar uma região operacional para que você possa usar a opção de localidade ao criar seu grupo do IPAM. A integração do IPAM com o BYOIP exige que a localidade seja definida em qualquer grupo que será usado para o CIDR do BYOIP.

Esta etapa deve ser realizadas pela conta do IPAM.

Execute o seguinte comando:

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

Na saída, você verá o IPAM que criou. Observe o valor para `PublicDefaultScopeId`. Você precisará do ID do escopo público na próxima etapa.

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

Etapa 3: criar um grupo do IPAM

Como você vai criar um grupo do IPAM de nível superior com um grupo regional dentro dele, e vamos alocar espaço para um recurso (uma VPC) do grupo regional, você definirá a localidade no grupo regional e não no grupo de nível superior. Você adicionará a localidade ao grupo regional ao criá-lo em uma etapa posterior. A integração do IPAM com o BYOIP exige que a localidade seja definida em qualquer grupo que será usado para o CIDR do BYOIP.

Esta etapa deve ser realizadas pela conta do IPAM.

Escolha se você deseja que o CIDR desse grupo do IPAM seja anunciado pela AWS por meio da internet pública (`--publicly-advertisable` ou `--no-publicly-advertisable`).

> **Note**
>
> Observe que o ID do escopo deve ser o ID do escopo público, e a família de endereços deve ser `ipv6`.

Para criar um grupo de endereços IPv6 para todos os seus recursos da AWS usando a AWS CLI

1. Execute o comando a seguir para criar um grupo do IPAM. Use o ID do escopo público do IPAM criado na etapa anterior.

   ```
   aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-
   scope-0087d83896280b594 --description "top-level-IPv6-pool" --address-
   family ipv6 --publicly-advertisable --profile ipam-account
   ```

   Na saída, você verá `create-in-progress`, o que indica que a criação do grupo está em andamento.

   ```
   {
       "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. Execute o comando a seguir até ver um estado `create-complete` na saída.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

O exemplo a seguir mostra o estado do grupo.

```
{
    "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": []

    }

}
```

Etapa 4: provisionar um CIDR para o grupo de nível superior

Provisione um bloco CIDR para o grupo de nível superior. Observe que, ao provisionar um CIDR IPv6 a um grupo dentro do grupo de nível superior, o intervalo de endereços IPv6 /48 é o intervalo mais específico que você trazer para CIDRs anunciáveis publicamente e /60 para CIDRs que não são anunciáveis publicamente.

> **Note**
>
> - Se você verificou seu controle do domínio com um certificado X.509, deverá incluir o CIDR, a mensagem de BYOIP e a assinatura do certificado que criou nessa etapa para que possamos confirmar que você controla o espaço público.
> - Se você verificou seu controle do domínio com um registro TXT do DNS, deverá incluir o CIDR e token de verificação do IPAM criado nessa etapa para que possamos confirmar que você controla o espaço público.

Você só precisa verificar o controle do domínio quando provisiona o CIDR de BYOIP para o grupo superior. Para o grupo regional dentro do grupo superior, você pode omitir a opção de controle do domínio.

Esta etapa deve ser executada pela conta do IPAM.

Para provisionar um bloco CIDR para o grupo usando o AWS CLI

1. Para provisionar o CIDR com as informações de certificado, use o exemplo de comando a seguir. Além de substituir os valores conforme necessário no exemplo, certifique-se de substituir os valores de `Message` e `Signature` pelos valores de `text_message` e `signed_message` que você obteve em Verificar seu domínio com um certificado 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~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

Para provisionar o CIDR com as informações do token de verificação, use o exemplo de comando a seguir. Além de substituir os valores no exemplo conforme necessário, certifique-se de substituir `ipam-ext-res-ver-token-0309ce7f67a768cf0` pelo ID do token `IpamExternalResourceVerificationTokenId` que você obteve em Verifique seu domínio com um registro TXT do DNS.

```
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
```

Na saída, você verá a provisão pendente do CIDR.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "pending-provision"

    }

}
```

2. Certifique-se de que esse CIDR tenha sido provisionado antes de continuar.

> **Important**
>
> Embora a maior parte do provisionamento seja concluída em até 2 horas, a conclusão do processo de provisionamento pode levar até 1 semana para intervalos que permitam anúncios públicos.

Execute o comando a seguir até ver um estado `provisioned` na saída.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

O exemplo de saída a seguir mostra o estado.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Etapa 5: criar um grupo regional dentro de um grupo de nível superior

Crie um grupo regional dentro do grupo de nível superior. `--locale` é necessária no grupo e deve ser uma das regiões operacionais que você configurou ao criar o IPAM.

Esta etapa deve ser executada pela conta do IPAM.

> **Important**
>
> Ao criar o grupo, é necessário incluir `--aws-service ec2`. O serviço selecionado determina o serviço da AWS no qual o CIDR poderá ser publicado. No momento, a única opção é `ec2`, ou seja, os CIDRs alocados desse grupo poderão ser anunciados para o serviço Amazon EC2 e o serviço Amazon VPC (para CIDRs associados a VPCs).

Para criar um grupo regional usando a AWS CLI

1. Execute o comando a seguir para criar o grupo.

```
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
```

   Na saída, você verá o IPAM criando o grupo.

```
{
    "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. Execute o comando a seguir até ver um estado `create-complete` na saída.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

   Na saída, você vê os grupos que tem no IPAM. Neste tutorial, criamos um grupo regional e um de nível superior. Você verá ambos.

Etapa 6: provisionar um CIDR para o grupo regional

Provisione um bloco CIDR para o grupo regional. Observe que, ao provisionar o CIDR a um grupo dentro do grupo de nível superior, o intervalo de endereços IPv6 /48 é o intervalo mais específico que você trazer para CIDRs anunciáveis publicamente e /60 para CIDRs que não são anunciáveis publicamente.

Esta etapa deve ser executada pela conta do IPAM.

Para atribuir um bloco CIDR ao grupo regional usando a AWS CLI

1. Execute o comando a seguir para provisionar o 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
```

   Na saída, você verá a provisão pendente do CIDR.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
}
```

2. Execute o comando a seguir até ver um estado `provisioned` na saída.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   O exemplo de saída a seguir mostra o estado correto.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Etapa 7. Compartilhar o grupo regional

Siga as etapas nesta seção para compartilhar o grupo de IPAM usando o AWS Resource Access Manager (RAM).

Habilitar o compartilhamento de recursos no AWS RAM

Depois de criar seu IPAM, você desejará compartilhar o grupo regional com outras contas em sua organização. Antes de compartilhar um grupo do IPAM, conclua as etapas nesta seção para habilitar o compartilhamento de recursos com o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`management-account`**.

Para habilitar o compartilhamento de recursos

1. Com a conta gerencial do AWS Organizations, abra o console do AWS RAM em https://console.aws.amazon.com/ram/.
2. No painel de navegação esquerdo, escolha Configurações, depois Habilitar compartilhamento com o AWS Organizations e escolha Salvar configurações.

Agora você pode compartilhar um grupo do IPAM com outros membros da organização.

Compartilhar um grupo do IPAM usando o AWS RAM

Nesta seção, você compartilhará o grupo regional com outra conta de membro do AWS Organizations. Para obter instruções completas sobre o compartilhamento de grupos do IPAM, incluindo informações sobre as permissões necessárias do IAM, consulte Compartilhar um grupo do IPAM usando o AWS RAM. Se você estiver usando a AWS CLI para habilitar o compartilhamento de recursos, use a opção `--profile` **`ipam-account`**.

Para compartilhar um grupo do IPAM usando o AWS RAM

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado, o grupo de IPAM e Ações > Visualizar detalhes.
4. Em Resource sharing (Compartilhamento de recursos), escolha Create resource share (Criar compartilhamento de recursos). O console do AWS RAM será aberto. Você compartilhará o grupo usando o AWS RAM.

5. Escolha Create a resource share (Criar um compartilhamento de recursos).
6. No console do AWS RAM, escolha Criar um compartilhamento de recursos novamente.
7. Adicione um Nome para o recurso compartilhado.
8. Em Selecionar tipo de recurso, escolha Grupos do IPAM e, em seguida, escolha o ARN do grupo que deseja compartilhar.
9. Escolha Próximo.
10. Escolha a permissão AWSRAMPermissionIpamPoolByoipCidrImport. Os detalhes das opções de permissão estão fora do escopo deste tutorial, mas você pode descobrir mais sobre essas opções em Compartilhar um grupo do IPAM usando o AWS RAM.
11. Escolha Próximo.
12. Em Entidades principais > Selecionar tipo de entidade principal, escolha Conta da AWS e insira o ID da conta que trará um intervalo de endereços IP para o IPAM e escolha Adicionar.
13. Escolha Próximo.
14. Revise as opções de compartilhamento de recursos e as entidades principais com as quais você compartilhará e escolha Criar.
15. Para permitir que a conta da **`member-account`** aloque o endereço IP CIDRS do grupo do IPAM, crie um segundo compartilhamento de recursos com `AWSRAMDefaultPermissionsIpamPool`. O valor para `--resource-arns` é o ARN do grupo do IPAM criado na seção anterior. O valor para `--principals` é o ID de **`member-account`**. O valor para `--permission-arns` é o ARN da permissão `AWSRAMDefaultPermissionsIpamPool`.

Etapa 8: criar uma VPC usando o CIDR IPv6

Crie uma VPC usando o ID do grupo do IPAM. Você deve associar um bloco CIDR IPv4 à VPC também, usando a opção `--cidr-block`, ou a solicitação falhará. Quando você executa o comando nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo que será usado para o CIDR de BYOIP.

Esta etapa deve ser realizadas pela conta de membro.

Para criar uma VPC com o CIDR IPv6 usando a AWS CLI

1. Execute o comando a seguir para provisionar o 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
```

Na saída, você verá a VPC sendo criada.

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-2afccf50",
        "State": "pending",
        "VpcId": "vpc-00b5573ffc3b31a29",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-01b5703d6cc695b5b",
                "Ipv6CidrBlock": "2605:9cc0:409::/56",
                "Ipv6CidrBlockState": {
                    "State": "associating"
                },
                "NetworkBorderGroup": "us-east-1",
                "Ipv6Pool": "ipam-pool-0053b7d2b4fc3f730"
            }
        ],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-09cccb07d4e9a0e0e",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false
    }
}
```

2. Visualize a alocação da VPC no IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Na saída, você verá a alocação no IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Etapa 9: anunciar o CIDR

Depois de criar a VPC com o CIDR alocado no IPAM, você pode começar a anunciar o CIDR que você trouxe para a AWS que está no grupo com `--aws-service ec2` definido. Neste tutorial, esse é o seu grupo regional. Por padrão, o CIDR não é anunciado, o que significa que não é acessível publicamente pela Internet. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo regional que será usado para o CIDR de BYOIP.

Esta etapa deve ser realizadas pela conta do IPAM.

Comece anunciando o CIDR usando a AWS CLI

- Execute o comando a seguir para anunciar o CIDR.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

Na saída, você verá o CIDR anunciado.

```
{
```

```
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "advertised"
    }
}
```

Etapa 10: limpeza

Siga as etapas desta seção para limpar os recursos que você provisionou e criou neste tutorial. Ao executar os comandos nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo regional que será usado para o CIDR de BYOIP.

Limpar usando a AWS CLI

1. Execute o comando a seguir para visualizar a alocação da VPC gerenciada no IPAM.

   Esta etapa deve ser realizadas pela conta do IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   A saída mostra a alocação no IPAM.

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "2605:9cc0:409::/56",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
               "ResourceId": "vpc-00b5573ffc3b31a29",
               "ResourceType": "vpc",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

2. Execute o comando a seguir para interromper o anúncio do CIDR. Ao executar o comando nesta etapa, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo regional que será usado para o CIDR de BYOIP.

   Esta etapa deve ser realizadas pela conta do IPAM.

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

Na saída, você verá que o estado do CIDR mudou de advertised (anunciado) para provisioned (provisionado).

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "provisioned"
    }
}
```

3. Execute o comando a seguir para excluir a VPC. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo regional que será usado para o CIDR de BYOIP.

   Esta etapa deve ser realizadas pela conta de membro.

   ```
   aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
   profile member-account
   ```

   Você não verá nenhuma saída ao executar esse comando.

4. Execute o comando a seguir para visualizar a alocação da VPC no IPAM. Pode levar algum tempo para o IPAM descobrir que a VPC foi excluída e remover essa alocação. Ao executar os comandos nesta seção, o valor de `--region` deve corresponder à opção `--locale` inserida ao criar o grupo regional que será usado para o CIDR de BYOIP.

   Esta etapa deve ser realizadas pela conta do IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   A saída mostra a alocação no IPAM.

   ```
   {
      "IpamPoolAllocations": [
   ```

```
        {

            "Cidr": "2605:9cc0:409::/56",

            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",

            "ResourceType": "vpc",

            "ResourceOwner": "123456789012"

        }

    ]

}
```

Execute novamente o comando e procure a alocação a ser removida. Não é possível continuar limpando e desprovisionando o CIDR do grupo do IPAM até ver que a alocação foi removida do IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

A saída mostra a alocação removida do IPAM.

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

5. Exclua os compartilhamentos do RAM e desabilite a integração do RAM com o AWS Organizations. Conclua as etapas em Excluir um compartilhamento de recursos no AWS RAM e Desabilitar o compartilhamento de recursos com o AWS Organizations no Guia do usuário do AWS RAM, nessa ordem, para excluir o compartilhamento do RAM e desabilitar a integração do RAM com o AWS Organizations.

   Esta etapa deve ser executada pela conta do IPAM e pela conta gerencial, respectivamente. Se você estiver usando o AWS CLI para excluir os compartilhamentos do RAM e desabilitar a integração do RAM, use as opções `--profile ipam-account` e `--profile management-account`.

6. Use o comando a seguir para desprovisionar o CIDR do grupo regional.

   Esta etapa deve ser realizadas pela conta do 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
```

   Na saída, você verá o desprovisionamento pendente do CIDR.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   O desprovisionamento demora para ser concluído. Continue executando o comando até ver o estado deprovisioned (desprovisionado) do CIDR.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   Na saída, você verá o desprovisionamento pendente do CIDR.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "deprovisioned"
    }
}
```

7. Execute o comando a seguir para excluir o grupo regional.

   Esta etapa deve ser realizadas pela conta do IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   Na saída, você pode ver o estado de exclusão.

```
{
    "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. Use o comando a seguir para desprovisionar o CIDR do grupo de nível superior.

   Esta etapa deve ser realizadas pela conta do 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
```

   Na saída, você verá o desprovisionamento pendente do CIDR.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   O desprovisionamento demora para ser concluído. Use o comando a seguir para verificar o status do desprovisionamento.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Espere até ver deprovisioned (desprovisionado) antes de continuar para a próxima etapa.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. Execute o comando a seguir para excluir o grupo de nível superior.

   Esta etapa deve ser realizadas pela conta do IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

   Na saída, você pode ver o estado de exclusão.

```
{
    "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. Execute o comando a seguir para excluir o IPAM.

    Esta etapa deve ser realizadas pela conta do IPAM.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    Na saída, você verá a resposta do IPAM. Isso significa que o IPAM foi excluído.

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

Traga seu próprio IP para o CloudFront usando o IPAM

O BYOIP do IPAM para serviços globais permite que você use seus próprios endereços IPv4 com serviços globais da AWS como o CloudFront. Diferentemente do BYOIP regional, seus endereços IP são anunciados em vários locais da borda simultaneamente usando o roteamento anycast.

Por que usar esse recurso?

- Manter a lista de permissões de IP: use endereços IP aprovados existentes em vez de atualizar as configurações de firewall
- Simplificar as migrações: migre de outras CDNs sem alterar a infraestrutura de IP
- Manter a consistência da marca: mantenha seu espaço de endereço IP existente ao mudar para a AWS

Quem deve usar esse recurso?

Organizações que precisam de seus próprios endereços IP com entrega global de conteúdo:

- Grandes empresas com requisitos de lista de permissões de IP
- Empresas migrando de outras CDNs com endereços IP existentes
- Organizações com políticas de segurança rígidas que exigem intervalos de IP específicos

Quando usar esse recurso?

Use o BYOIP para serviços globais quando precisar:

- Manter as listas de permissões de IP existentes com parceiros/clientes
- Migrar de outra CDN usando seus endereços IP
- Atender aos requisitos de conformidade para intervalos de IP específicos

> **Note**
>
> Requer blocos CIDR IPv4 /24. Atualmente disponível somente para o CloudFront.

Pré-requisitos

Conclua estas etapas antes de começar:

- Configuração do IPAM: Integrar o IPAM a contas em uma organização da AWS Organizations e Criar um IPAM
- Verificação de domínio: Verificar o controle do domínio

- Crie um pool de nível superior: siga as Etapas 1 e 2 em Traga seu próprio CIDR IPv4 para o IPAM

Etapas de configuração do serviço global

As seguintes etapas diferem do processo BYOIP regional padrão e estabelecem o padrão para serviços globais:

Etapa 1: criar um pool global para serviços anycast

Em vez de criar um pool regional, crie um pool global para serviços anycast:

Console

Para criar um pool global usando o console:

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Pools
3. Selecione Criar pool
4. Fonte: escolha seu pool BYOIP de nível superior
5. Localidade: escolha Global
6. Serviço: escolha Serviços globais (aparece quando a opção Global é selecionada)
7. Origem de IP público: escolha BYOIP
8. CIDRs a serem provisionados: especifique seu intervalo de CIDR /24
9. Selecione Criar pool

CLI

Use `aws ec2 create-ipam-pool` com a localidade definida como “Global” e a família de endereços “ipv4".

Em seguida, provisione o CIDR usando `aws ec2 provision-ipam-pool-cidr`.

> **Important**
>
> Você deve alocar o bloco /24 completo a esse pool. Você pode provisionar intervalos mais específicos dentro desse bloco para diferentes usos.

Etapa 2: criar recursos específicos para o serviço

Para o CloudFront, crie uma lista de IP anycast que use seu pool do IPAM. Para obter instruções detalhadas, consulte a Documentação sobre BYOIP do CloudFront (link a definir).

Parâmetros-chave para a integração do IPAM:

- Tipo de endereço IP: escolha BYOIP
- Pool do IPAM: selecione seu pool global na Etapa 1
- Contagem de IP: insira 3 (necessário para o CloudFront)

Etapa 3: associar a recursos de serviços

Associe sua lista de IPs estáticos do Anycast a uma distribuição do CloudFront. Para obter instruções detalhadas, consulte a Documentação sobre BYOIP do CloudFront (link a definir).

Configuração principal:

- Nas configurações de distribuição, selecione sua Lista de IP Anycast na Etapa 2

Etapa 4: Preparar-se para a migração

- Diminua o TTL do DNS: defina o TTL do DNS para seus registros para 60 segundos ou menos
- Aguarde a propagação: aguarde até que o novo TTL entre em vigor na internet

Etapa 5: anunciar o CIDR globalmente

Use o comando de anúncio global do IPAM:

Console

Para anunciar o CIDR usando o console:

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, escolha Pools
3. Selecione seu pool global
4. Escolha a guia CIDRs

5. Selecione seu CIDR e escolha Ações >Anunciar CIDR.
6. Confirme o anúncio

CLI

Use `aws ec2 advertise-ipam-byoip-cidr` com seu ID de pool do IPAM e CIDR.

> **Important**
>
> - Retire o anúncio do seu provedor anterior antes de executar esse comando
> - Atualize os registros de DNS para apontar para o CloudFront e concluir a migração

Limpeza

Para limpar os recursos criados neste tutorial:

- Excluir recursos do CloudFront: siga as instruções de limpeza na documentação sobre BYOIP do CloudFront (link a definir)
- Retire o CIDR e exclua os pools do IPAM: siga o processo de limpeza padrão em Etapa 8: limpeza

> **Important**
>
> Exclua primeiro os recursos do CloudFront e, em seguida, prossiga com a limpeza do IPAM para evitar interrupções no serviço.

Tutorial: transferir um CIDR IPv4 BYOIP para o IPAM

Siga estas etapas para transferir um CIDR IPv4 existente para o IPAM. Se você já tem um CIDR IPv4 BYOIP com a AWS, pode mover o CIDR para o IPAM de um grupo IPv4 público. Não é possível transferir um CIDR IPv6 para o IPAM.

Este tutorial presume que você já trouxe com sucesso um intervalo de endereços IP para a AWS usando o processo descrito em Traga seus próprios endereços IP (BYOIP) no Amazon EC2 e agora deseja transferir esse intervalo de endereços IP para o IPAM. Se você estiver trazendo

um novo endereço IP para a AWS pela primeira vez, conclua as etapas em Tutorial: trazer seus endereços IP para o IPAM.

Se você transferir um grupo de IPv4 público para o IPAM, não haverá impacto nas alocações existentes. Depois de transferir um grupo de IPv4 público para o IPAM, dependendo do tipo de recurso, você poderá monitorar as alocações existentes. Para obter mais informações, consulte Monitorar o uso do CIDR por recurso.

> **Note**
>
> - Este tutorial pressupõe que você já tenha concluído as etapas em Criar um IPAM.
> - Cada etapa deste tutorial deve ser executada por uma das duas contas da AWS:
>   - A conta de administrador do IPAM. Neste tutorial, essa conta será chamada de conta IPAM.
>   - A conta da organização que é proprietária do CIDR de BYOIP. Neste tutorial, essa conta será chamada de conta de proprietário do CIDR de BYOIP.

Conteúdo

- Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM
- Etapa 2: obter o ID de escopo público do IPAM
- Etapa 3: criar um grupo do IPAM
- Etapa 4: compartilhar o grupo do IPAM usando o AWS RAM
- Etapa 5: transferir um CIDR IPv4 BYOIP existente para o IPAM
- Etapa 6: visualizar o CIDR no IPAM
- Etapa 7: limpeza

Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM

Para concluir este tutorial como um usuário da AWS, você pode usar os perfis nomeados da AWS CLI para alternar de um perfil do IAM para outro. Perfis nomeados são coleções de configurações e credenciais às quais você se refere ao usar a opção `--profile` com a AWS CLI. Para obter mais informações sobre como criar perfis do IAM e perfis nomeados para contas da AWS, consulte Uso de perfis do IAM na AWS CLI.

Crie uma função e um perfil nomeado para cada uma das três contas da AWS que você usará neste tutorial:

- Um perfil chamado `ipam-account` para a conta da AWS que é o administrador do IPAM.
- Um perfil chamado `byoip-owner-account` para a conta da AWS em sua organização que possui o CIDR de BYOIP.

Depois de criar os perfis do IAM e os perfis nomeados, volte para esta página e vá para a próxima etapa. Você notará, ao longo do restante deste tutorial, que os exemplos de comandos da AWS CLI usam a opção `--profile` com um dos perfis nomeados para indicar qual conta deve executar o comando.

Etapa 2: obter o ID de escopo público do IPAM

Siga as etapas nesta seção para obter o ID de escopo público do IPAM. Esta etapa deve ser executada pela conta do **`ipam-account`**.

Execute o comando a seguir para obter o ID do escopo público.

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

Na saída, você verá seu ID de escopo público. Observe os valores de `PublicDefaultScopeId`. Você precisará dele na próxima etapa.

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

Etapa 3: criar um grupo do IPAM

Siga as etapas nesta seção para criar um grupo do IPAM. Esta etapa deve ser executada pela conta do **`ipam-account`**. O grupo do IPAM criado deve ser um grupo de nível superior com a opção `--locale` correspondente à região AWS do CIDR de BYOIP. Você só pode transferir um BYOIP para um grupo do IPAM de nível superior.

> **Important**
>
> Ao criar o grupo, é necessário incluir `--aws-service ec2`. O serviço selecionado determina o serviço da AWS no qual o CIDR poderá ser publicado. No momento, a única opção é `ec2`, ou seja, os CIDRs alocados a partir desse grupo poderão ser publicados no serviço Amazon EC2 (para endereços IP elásticos) e no serviço Amazon VPC (para CIDRs associados a VPCs).

Para criar um grupo de endereços IPv4 para o CIDR de BYOIP transferido usando a AWS CLI

1. Execute o comando a seguir para criar um grupo do IPAM. Use o ID de escopo público do IPAM recuperado na etapa anterior.

   ```
   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
   ```

   Na saída, você verá `create-in-progress`, o que indica que a criação do grupo está em andamento.

   ```
   {
       "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. Execute o comando a seguir até ver um estado `create-complete` na saída.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

O exemplo a seguir mostra o estado do grupo. Você precisará desse OwnerId na próxima etapa.

```
{
    "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"
        }
```

```
    ]
}
```

Etapa 4: compartilhar o grupo do IPAM usando o AWS RAM

Siga as etapas desta seção para compartilhar um grupo do IPAM usando o AWS RAM para que outra conta da AWS possa transferir um CIDR IPV4 BYOIP existente para o grupo do IPAM e consiga usá-lo. Esta etapa deve ser executada pela conta do **`ipam-account`**.

Para compartilhar um grupo de endereços IPv4 usando a AWS CLI

1. Visualize as permissões do AWS RAM disponíveis para os grupos do IPAM. Você precisa de ambos os ARNs para concluir as etapas desta seção.

```
aws ram list-permissions --region us-east-1 --profile ipam-account --resource-type
 ec2:IpamPool
```

```
{
    "permissions": [
        {
           "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool",
           "version": "1",
           "defaultVersion": true,
           "name": "AWSRAMDefaultPermissionsIpamPool",
           "resourceType": "ec2:IpamPool",
           "status": "ATTACHABLE",
           "creationTime": "2022-06-30T13:04:29.335000-07:00",
           "lastUpdatedTime": "2022-06-30T13:04:29.335000-07:00",
           "isResourceTypeDefault": true
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMPermissionIpamPoolByoipCidrImport",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMPermissionIpamPoolByoipCidrImport",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:55.032000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:55.032000-07:00",
            "isResourceTypeDefault": false
```

```
        }
    ]
}
```

2. Crie um compartilhamento de recursos para permitir que a conta **byoip-owner-account** importe CIDRs BYOIP para o IPAM. O valor para `--resource-arns` é o ARN do grupo do IPAM criado na seção anterior. O valor para `--principals` é o ID da conta do proprietário do CIDR BYOIP. O valor para `--permission-arns` é o ARN da permissão `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. (Opcional) Se você quiser permitir que a conta **byoip-owner-account** aloque os CIDRs de endereço IP do grupo do IPAM para grupos IPv4 públicos após a conclusão da transferência, copie o ARN para `AWSRAMDefaultPermissionsIpamPool` e crie um segundo compartilhamento de recursos. O valor para `--resource-arns` é o ARN do

grupo do IPAM criado na seção anterior. O valor para `--principals` é o ID da conta do proprietário do CIDR BYOIP. O valor para `--permission-arns` é o ARN da permissão `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"

        }

}
```

Como resultado da criação do compartilhamento de recursos no RAM, a conta byoip-owner-account já pode mover CIDRs para o IPAM.

Etapa 5: transferir um CIDR IPv4 BYOIP existente para o IPAM

Siga as etapas nesta seção para transferir um CIDR IPv4 de BYOIP existente para o IPAM. Esta etapa deve ser executada pela conta do **`byoip-owner-account`**.

> **Important**
>
> Se você trouxer um intervalo de endereços IPv4 para a AWS, poderá usar todos os endereços IP do intervalo, incluindo o primeiro endereço (o endereço de rede) e o último endereço (o endereço de broadcast).

Para transferir o CIDR de BYOIP para o IPAM, o proprietário do CIDR de BYOIP deve ter estas permissões em sua política do IAM:

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> Você pode usar o Console de gerenciamento da AWS ou a AWS CLI para essa etapa.

AWS Management Console

Para transferir um CIDR BYOIP para o grupo do IPAM:

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/ como uma conta **`byoip-owner-account`**.
2. No painel de navegação, selecione Pools (Grupos).
3. Escolha o grupo de nível superior criado e compartilhado neste tutorial.
4. Escolha Ações > Transferir CIDR BYOIP.
5. Escolha Transferir CIDR BYOIP.
6. Escolha seu CIDR BYOIP.
7. Escolha Provisionar.

Command line

Use os comandos da AWS CLI a seguir para transferir um CIDR BYOIP para o grupo do IPAM usando a AWS CLI:

1. Execute o comando a seguir para transferir o CIDR. Verifique se o valor de `--region` é a região da AWS do CIDR de 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
```

   Na saída, você verá a provisão pendente do CIDR.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "pending-transfer"

    }

}
```

2. Certifique-se de que o CIDR tenha sido transferido. Execute o comando a seguir até ver um estado `complete-transfer` na saída.

```
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
```

   O exemplo de saída a seguir mostra o estado.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

Etapa 6: visualizar o CIDR no IPAM

Siga as etapas nesta seção para visualizar o CIDR no IPAM. Esta etapa deve ser executada pela conta do **`ipam-account`**.

Para visualizar o CIDR de BYOIP transferido no grupo do IPAM usando a AWS CLI

- Execute o comando a seguir para visualizar a alocação gerenciada no IPAM. Verifique se o valor de `--region` é a região da AWS do CIDR de BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

  A saída mostra a alocação no IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

Etapa 7: limpeza

Siga as etapas desta seção para remover os recursos que você criou neste tutorial. Esta etapa deve ser executada pela conta do **`ipam-account`**.

Para limpar os recursos criados neste tutorial usando a AWS CLI

1. Para excluir o recurso compartilhado do grupo do IPAM, execute o seguinte comando para obter o primeiro ARN do compartilhamento de recursos:

```
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. Copie o ARN do compartilhamento de recursos e use-o para excluir o compartilhamento de recursos do grupo do 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. Se você criou um compartilhamento de recursos adicional em Etapa 4: compartilhar o grupo do IPAM usando o AWS RAM, repita as duas etapas anteriores para obter o ARN do segundo compartilhamento de recursos para `PoolShare2` e excluir o segundo compartilhamento de recursos.
4. Execute o comando a seguir para obter o ID da alocação do CIDR de BYOIP. Verifique se o valor de `--region` corresponde à região da AWS do CIDR de BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

A saída mostra a alocação no 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. Remova o bloco CIDR do grupo público de endereços IPv4. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa precisa ser concluída pela conta do **`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. Visualize seus CIDRs de BYOIP novamente e verifique se não há mais endereços provisionados. Ao executar o comando nesta seção, o valor de `--region` deve corresponder à região do seu IPAM.

   Esta etapa precisa ser concluída pela conta do **`byoip-owner-account`**.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
```

   Na saída, você verá a contagem de endereços IP em seu grupo IPv4 público.

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
```

```
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

7. Execute o comando a seguir para excluir o grupo de nível superior.

```
aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
id ipam-pool-0a03d430ca3f5c035
```

Na saída, você pode ver o estado de exclusão.

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4",
        "AwsService": "ec2"
    }
}
```

Tutorial: Planejar o espaço de endereço IP da VPC para alocações IP de sub-rede

Complete este tutorial para planejar o espaço de endereço IP da VPC, alocar endereços de IP às sub-redes da VPC e monitorar as métricas relacionadas ao endereço IP no nível da sub-rede e da VPC.

> **Note**
>
> Este tutorial aborda a alocação de espaço de endereço IPv4 privado em um escopo de IPAM privado para VPCs e sub-redes. Você também pode concluir este tutorial usando um intervalo de CIDRs IPv6, criando a VPC com a opção de bloco CIDR IPv6 fornecido pela Amazon no console da VPC.

Planejar o espaço de endereço IP da VPC para sub-redes permite que você faça o seguinte:

- Elabore um plano e organize os endereços de IP da sua VPC para alocá-los a sub-redes: Pode-se dividir o espaço de endereços IP da VPC em blocos CIDR menores e provisionar esses blocos CIDR para sub-redes com diferentes necessidades comerciais, como a execução de cargas de trabalho em sub-redes de desenvolvimento ou produção.
- Simplifique as alocações de endereços de IP para sub-redes da VPC: Depois que o espaço de endereços da sua VPC estiver planejado e organizado, você pode optar por um comprimento de máscara de rede em vez de inserir manualmente um CIDR. Por exemplo, se um desenvolvedor estiver criando uma sub-rede para hospedar cargas de trabalho de desenvolvimento, ele precisará escolher um grupo e um comprimento de máscara de rede para a sub-rede, e o IPAM alocará automaticamente o bloco CIDR para a sua sub-rede.

O exemplo a seguir mostra a hierarquia da estrutura do grupo e dos recursos que você criará neste tutorial:

- Escopo privado
  - Grupo de planejamento de recursos (10.0.0.0/20)
    - Grupo de sub-redes de desenvolvimento 10.0.0.0/24)
      - Sub-redes de desenvolvimento (10.0.0.0/28)
    - Grupo de sub-redes de produção (10.0.0.1/24)
      - Sub-redes de produção (10.0.0.16/28)

> **Important**
>
> - O grupo de planejamento de recursos pode ser empregado para alocar CIDRs a sub-redes ou servir como um grupo primário no qual você pode criar subgrupos. Neste tutorial,

estamos utilizando o grupo de planejamento de recursos como um grupo principal para os subgrupos de sub-redes.

- Se a VPC possuir mais de um CIDR provisionado, você pode criar diversos grupos de planejamento de recursos; por exemplo, se uma VPC tiver dois CIDRs atribuídos, será possível criar dois grupos de planejamento de recursos, cada um para um CIDR específico. Cada CIDR pode ser atribuído a um grupo por vez.

Etapa 1: criar uma VPC

Conclua as etapas desta seção para criar uma VPC destinada ao planejamento de endereços de IP de sub-rede. Para obter mais informações sobre as permissões do IAM necessárias para criar VPCs, consulte exemplos de políticas da Amazon VPC no Guia do usuário da Amazon VPC.

> **Note**
>
> Você pode usar uma VPC existente em vez de criar uma nova, mas este tutorial se concentra no cenário em que a VPC é configurada com um bloco CIDR alocado manualmente, e não com um bloco CIDR alocado automaticamente pelo IPAM.

Para criar uma VPC

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. Escolha Criar VPC.
3. Insira um nome para a VPC, como tutorial-vpc.
4. Escolha IPv4 CIDR manual input (Entrada manual de CIDR IPv4) e insira um bloco CIDR IPv4. Neste tutorial, usamos 10.0.0.0/20.
5. Ignore a opção de adicionar um bloco CIDR IPv6.
6. Escolha Criar VPC.
7. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
8. No painel de navegação à esquerda, escolha Recursos.

9. Aguarde até que a VPC criada anteriormente apareça. Esse processo pode levar algum tempo e pode ser necessário atualizar a janela para visualizar as informações. A VPC deve ser descoberta pelo IPAM antes de continuar na próxima etapa.

Etapa 2: Criar um grupo de planejamento de recursos

Conclua as etapas nesta seção para criar um grupo de planejamento de recursos.

A criação de um grupo de planejamento de recursos

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado.
4. Selecione Criar.
5. Em Escopo do IPAM, deixe o escopo privado selecionado.
6. (Opcional) Adicionar uma Tag de nome para o grupo, por exemplo, “Grupo de planejamento de recursos”.
7. Em Tipo de origem, escolha Escopo do IPAM.
8. Em Planejamento de recursos, escolha Planejar espaço IP em uma VPC e escolha a VPC que você criou na etapa anterior. O VPC é o recurso usado para provisionar CIDRs para o grupo de planejamento de recursos.
9. Em CIDRs a serem provisionados, escolha o CIDR da VPC a ser provisionado para o grupo de recursos. O CIDR que você provisiona para o grupo de planejamento de recursos deve corresponder ao CIDR provisionado para a VPC. Neste tutorial, usamos 10.0.0.0/20.
10. Selecione Criar grupo.
11. Depois de criar o grupo, vá para a guia CIDR para verificar o estado do CIDR provisionado. Atualize a página e aguarde até que o estado do CIDR mude de Provisionamento pendente para Provisionado antes de prosseguir para a próxima etapa.

Etapa 3: Criar grupos de sub-redes

Conclua as etapas desta seção para criar dois grupos de sub-rede que serão utilizados para alocar espaço IP para as sub-redes.

A criação de grupos de sub-redes

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado.
4. Selecione Criar.
5. Em Escopo do IPAM, deixe o escopo privado selecionado.
6. (Opcional) Adicionar uma Tag de nome para o grupo, por exemplo, “dev-subnet-pool”.
7. Em Origem, selecione o grupo de IPAM e escolha o grupo de planejamento de recursos criado na Etapa 3. A família de endereços, as configurações de planejamento de recursos e a localidade são automaticamente herdadas do grupo de origem.
8. Na seção CIDRs a serem provisionados, selecione o CIDR a ser provisionado para o grupo de sub-rede. Neste tutorial, usamos 10.0.0.0/24.
9. Selecione Criar grupo.
10. Depois de criar o grupo, vá para a guia CIDR para verificar o estado do CIDR provisionado. Atualize a página e aguarde até que o estado do CIDR mude de Provisionamento pendente para Provisionado antes de prosseguir para a próxima etapa.
11. Repita esse processo para criar outra sub-rede chamada “prod-subnet-pool”.

Nesse ponto, se você quiser disponibilizar esse grupo de sub-redes para outras contas da AWS, poderá compartilhar o grupo de sub-redes. Para obter instruções sobre como fazer isso, consulte Compartilhar um grupo do IPAM usando o AWS RAM. Em seguida, volte aqui para concluir o tutorial.

Etapa 4: Criar sub-redes

Conclua estas etapas para criar duas sub-redes.

A criação de uma sub-rede

1. Usando a conta apropriada, abra o console VPC em https://console.aws.amazon.com/vpc/.
2. Escolha Sub-redes > Criar sub-rede.
3. Escolha a VPC que você criou no início deste tutorial.
4. Insira um nome para a sub-rede, como “tutorial-subnet”.

5. (Opcional) Escolha uma zona de disponibilidade.
6. Em Bloco IPv4 CIDR, escolha Bloco IPV4 CIDR alocado pelo IPAM e escolha o grupo de sub-rede dev e uma máscara de rede /28.
7. Escolha Criar sub-rede.
8. Repita esse processo para criar outra sub-rede. Desta vez, escolha o grupo de sub-rede prod e uma máscara de rede /28.
9. Volte ao console do IPAM e escolha Recursos no painel de navegação à esquerda.
10. Localize os grupos de sub-rede que foram criados e aguarde até que as sub-redes associadas estejam visíveis abaixo deles. Esse processo pode levar algum tempo e pode ser necessário atualizar a janela para visualizar as informações.

O tutorial está completo. Se necessário, você pode criar grupos de sub-rede adicionais ou iniciar instâncias do EC2 em uma das sub-redes existentes.

O IPAM gera métricas relacionadas ao uso de endereços IP em sub-redes. É possível configurar alarmes no CloudWatch com base na métrica "SubnetIPUsage", permitindo tomar medidas quando os limites de utilização de endereços IP são ultrapassados. Por exemplo, se uma sub-rede tiver um CIDR /24 (256 endereços IP) e você desejar ser notificado quando 80% dos IPs estiverem em uso, é possível configurar um alarme no CloudWatch para receber alertas quando esse limite for atingido. Para obter mais informações sobre como criar um alarme para o uso do IP da sub-rede, consulte Dica rápida para a criação de alarmes.

Etapa 5: limpeza

Conclua estas etapas para excluir os recursos criados neste tutorial.

Limpeza dos recursos

1. Use a conta de administrador do IPAM e abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Grupos.
3. Escolha o escopo privado.
4. Escolha o grupo de planejamento de recursos e escolha Ação > Excluir.
5. Selecione Excluir em cascata. O grupo de planejamento de recursos e os grupos de sub-rede serão excluídos. Isso não excluirá as sub-redes em si. Eles permanecerão com os CIDRs fornecidos a eles, embora os CIDRs não sejam mais de um grupo de IPAM.

6. Escolha Excluir.
7. Exclua as sub-redes.
8. Exclua a VPC.

A limpeza está completa.

Alocar endereços IP elásticos sequenciais de um grupo do IPAM

O IPAM permite que você provisione blocos IPv4 públicos de propriedade da Amazon para grupos do IPAM e aloque endereços IP elásticos sequenciais desses grupos para recursos da AWS.

Os endereços IP elásticos alocados de forma contígua são endereços IPv4 públicos que são alocados sequencialmente. Por exemplo, se a Amazon fornecer um bloco CIDR IPv4 público de `192.0.2.0/30` e você alocar os quatro endereços IPv4 públicos disponíveis desse bloco CIDR, um exemplo de quatro endereços IP elásticos sequenciais será `192.0.2.0`, `192.0.2.1`, `192.0.2.2` e `192.0.2.3`.

Os endereços IP elásticos alocados de forma contínua permitem que você simplifique as regras de segurança e rede das seguintes maneiras:

- Administração de segurança: o uso de endereços IPv4 sequenciais reduz a sobrecarga de gerenciamento do firewall. Você pode adicionar um prefixo inteiro com uma única regra e associar IPs do mesmo prefixo à medida que você escala, economizando tempo e esforço.
- Acesso corporativo: você pode simplificar o espaço de endereços compartilhado com seus clientes usando um bloco CIDR inteiro em vez de uma longa lista de endereços IPv4 públicos individuais. Isso evita a necessidade de ter de comunicar constantemente as mudanças de IP à medida que a aplicação escala na AWS.
- Gerenciamento simplificado de IPs: o uso de endereços IPv4 sequenciais simplifica o gerenciamento de IPs públicos para sua equipe de rede central, pois reduz a necessidade de rastrear IPs públicos individuais e, consequentemente, permite que eles se concentrem em um número limitado de prefixos IP.

Neste tutorial, você percorrerá as etapas necessárias para alocar endereços IP elásticos sequenciais de um grupo do IPAM. Você criará um grupo do IPAM com um bloco CIDR IPv4 público contíguo fornecido pela Amazon, alocará endereços IP elásticos do grupo e aprenderá a monitorar as alocações do grupo do IPAM.

Note

- Há cobranças associadas ao provisionamento de blocos CIDR IPv4 públicos de propriedade da Amazon. Para obter mais informações, consulte a guia Bloco IPv4 contíguo fornecido pela Amazon na página Preços da Amazon VPC.
- Este tutorial pressupõe que você queira criar um IPAM usando-o com uma única conta. Caso deseje compartilhar blocos IPv4 públicos contíguos de propriedade da Amazon entre contas, primeiro Integrar o IPAM a contas em uma organização da AWS Organizations e depois Compartilhar um grupo do IPAM usando o AWS RAM. Caso se integre ao AWS Organizations, você terá a opção de criar uma política de controle de serviços para evitar o desprovisionamento dos blocos IPv4 contíguos atribuídos ao grupo.
- Você não pode transferir endereços IP elásticos sequenciais alocados de um grupo do IPAM para outras contas da AWS. Em vez disso, o IPAM permite que você compartilhe grupos do IPAM entre contas da AWS integrando o IPAM com o AWS Organizations (conforme mencionado acima).
- Há limites no número de blocos CIDR IPv4 públicos de propriedade da Amazon que você pode provisionar e no tamanho. Para obter mais informações, consulte Cotas para o IPAM.

Conteúdo

- Etapa 1: criar um IPAM
- Etapa 2: criar um grupo do IPAM e provisionar um CIDR
- Etapa 3: alocar um endereço IP elástico do grupo
- Etapa 4: associar o endereço IP elástico a uma instância do EC2
- Etapa 5: rastrear e monitorar o uso do grupo
- Limpeza

Etapa 1: criar um IPAM

Conclua as etapas nesta seção para criar um IPAM.

AWS Management Console

Para criar um IPAM

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No Console de Gerenciamento da AWS, escolha a Região da AWS em que você deseja criar o IPAM. Crie o IPAM em sua principal região de operações.
3. Na página inicial do serviço, selecione Create IPAM (Criar IPAM).
4. Selecione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir que o IP Address Manager da Amazon VPC replique dados das contas de origem para a conta delegada do IPAM). Se você não selecionar essa opção, não poderá criar um IPAM.
5. Escolha um nível IPAM. Para obter mais informações sobre os recursos disponíveis em cada nível e os custos associados aos níveis, consulte a guia IPAM na página de preços do Amazon VPC.
6. Em Operating regions (Regiões operacionais), selecione as regiões da AWS nas quais esse IPAM pode gerenciar e descobrir recursos. A região da AWS na qual você está criando seu IPAM é selecionada como uma das regiões operacionais por padrão. Por exemplo, se estiver criando esse IPAM na região da AWS `us-east-1`, mas você deseja criar grupos do IPAM regionais posteriormente que forneçam CIDRs para VPCs em `us-west-2`, selecione `us-west-2` aqui. Se você esquecer uma região operacional, poderá retornar posteriormente e editar suas configurações de IPAM.

   > **Note**
   >
   > Se estiver criando um IPAM no Nível Gratuito, pode escolher várias regiões de operação para o seu IPAM, mas a única funcionalidade disponível em todas as regiões de operação será a Insights de IP público. Não será possível utilizar outras funcionalidades do Nível Gratuito, como BYOIP, em regiões de operação do IPAM. Essas funcionalidades só podem ser utilizadas na Região de origem do IPAM. Para utilizar todos os recursos do IPAM em todas as Regiões de operação, é necessário criar um IPAM no nível avançado.

7. Escolha Create IPAM (Criar IPAM).

Command line

Os comandos nesta seção são vinculados à Documentação de referência da AWS CLI. A documentação fornece descrições detalhadas das opções que você pode usar ao executar os comandos.

Crie o IPAM com o comando create-ipam:

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

Exemplo de resposta:

```
{
    "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"
    }
}
```

Você precisará do PublicDefaultScopeId na próxima etapa. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.

Etapa 2: criar um grupo do IPAM e provisionar um CIDR

Conclua as etapas desta seção para criar um grupo do IPAM do qual você alocará os endereços IP elásticos.

AWS Management Console

Para criar um grupo

1. Abra o console do IPAM em https://console.aws.amazon.com/ipam/.
2. No painel de navegação, selecione Pools (Grupos).
3. Escolha o escopo público. Para obter mais informações sobre escopos, consulte Como funciona o IPAM.
4. Selecione Criar.
5. (Opcional) Adicione uma Name tag (Etiqueta de nome) e uma Description (Descrição) para o grupo.
6. Em Tipo de origem, escolha Escopo do IPAM.
7. Em Address family (Família de endereços), escolha IPv4.
8. Em Planejamento de recursos, deixe a opção de Planejar espaço IP dentro do escopo selecionada.
9. Em Locale (Local), escolha o local do grupo. A localidade é a Região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. As opções disponíveis são provenientes das regiões operacionais que você escolheu ao criar seu IPAM.
10. Em Service (Serviço), escolha EC2 (EIP/VPC). O serviço que você seleciona determina o serviço da AWS no qual o CIDR será anunciado. Atualmente, a única opção é EC2 (EIP/VPC), o que significa que os CIDRs alocados desse grupo serão anunciados para o serviço do Amazon EC2 (para endereços IP elásticos).
11. Em Origem de IP público, escolha Propriedade da Amazon.
12. Em CIDR a provisionar, escolha Adicionar CIDR público de propriedade da Amazon. Escolha um comprimento de máscara de rede entre `/29` (oito endereços IP) e `/30` (quatro endereços IP). Você pode adicionar até dois CIDRs por padrão. Para obter mais informações sobre como aumentar os limites dos CIDRs IPv4 públicos contíguos fornecidos pela Amazon, consulte Cotas para o IPAM.
13. Desmarque a opção Definir as configurações da regra de alocação deste grupo.
14. (Opcional) Escolha Tags (Etiquetas) para o grupo.

15. Selecione Criar.

Certifique-se de que esse CIDR tenha sido provisionado antes de continuar. Você pode ver o estado do provisionamento na guia CIDRs na página de detalhes do grupo.

Command line

Para criar um grupo

1. Crie um grupo do IPAM com o comando create-ipam-pool. A localidade é a Região da AWS em que você quer disponibilizar esse grupo do IPAM para alocações. As opções disponíveis são provenientes das regiões operacionais que você escolheu ao criar seu 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
```

Exemplo de resposta com o estado `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. Verifique se o grupo foi criado com sucesso usando o comando describe-ipam-pools.

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

Exemplo de resposta com o estado `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. Provisione um CIDR para o grupo com o comando provision-ipam-pool-cidr. Escolha um `--netmask-length` entre `/29` (oito endereços IP) e `/30` (quatro endereços IP). Você pode adicionar até dois CIDRs por padrão. Para obter mais informações sobre como aumentar os limites dos CIDRs IPv4 públicos contíguos fornecidos pela Amazon, consulte Cotas para o IPAM.

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

Exemplo de resposta com o estado `pending-provision`:

```
{

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

4. Certifique-se de que esse CIDR tenha sido provisionado antes de continuar. Você pode exibir o estado do provisionamento usando o comando get-ipam-pool-cidrs.

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

Exemplo de resposta com o estado `provisioned`:

```
{

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

```
            "NetmaskLength": 29
        }
    ]
}
```

Etapa 3: alocar um endereço IP elástico do grupo

Conclua as etapas desta seção para alocar um endereço IP elástico do grupo.

AWS Management Console

Siga as etapas em Allocate an Elastic IP address no Guia do usuário do Amazon EC2 para alocar o endereço, mas observe o seguinte:

- Certifique-se de que a região da AWS em que você está no console do EC2 corresponda à opção de localidade que você escolheu ao criar o grupo na Etapa 2.
- Ao escolher o grupo de endereços, escolha a opção Alocar usando um grupo IPv4 do IPAM e depois o grupo que você criou na Etapa 1.

Command line

Aloque um endereço do grupo com o comando allocate-address. A `--region` que você usa deve corresponder à opção de `-locale` que você escolheu quando criou o grupo na Etapa 2. Inclua o ID do grupo do IPAM que você criou na Etapa 2 em `--ipam-pool-id`.

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

Exemplo de resposta:

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

Opcionalmente, você também pode escolher um `/32` específico em seu grupo do IPAM usando a opção `--address`.

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

Exemplo de resposta:

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

Para obter mais informações, consulte Allocate an Elastic IP address no Guia do usuário do Amazon EC2.

Etapa 4: associar o endereço IP elástico a uma instância do EC2

Conclua as etapas desta seção para associar um endereço IP elástico a uma instância do EC2.

AWS Management Console

Siga as etapas em Associar um endereço IP elástico no Guia do usuário do Amazon EC2 para alocar um endereço IP elástico do grupo do IPAM, mas observe o seguinte: quando você usa a opção Console de Gerenciamento da AWS, a região da AWS à qual você associa o endereço IP elástico deve corresponder à opção de localidade que você escolheu ao criar o grupo na Etapa 2.

Command line

Associe o endereço IP elástico a uma instância com o comando associate-address. A `--region` à qual você associa o endereço IP elástico deve corresponder à opção de `--locale` que você escolheu quando criou o grupo na Etapa 2.

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

Exemplo de resposta:

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

Para obter mais informações, consulte Associate an Elastic IP address with an instance or network interface no Guia do usuário do Amazon EC2.

Etapa 5: rastrear e monitorar o uso do grupo

Depois de alocar endereços IP elásticos do grupo do IPAM, você pode rastrear e monitorar as alocações do grupo do IPAM.

AWS Management Console

- Veja os detalhes do grupo do IPAM na guia Alocações no console do IPAM. Todos os endereços IP elásticos alocados do grupo do IPAM têm um Tipo de recurso de EIP.
- Use o Insights de IP público:
  - Em Tipos de IP público, filtre por EIPs de propriedade da Amazon. Isso mostra o número total de endereços IPv4 públicos alocados aos endereços IP elásticos de propriedade da Amazon. Caso filtre por essa medida e role até Endereços IP públicos na parte inferior da página, você verá os endereços IP elásticos que alocou.
  - Em Uso de EIPs, filtre por EIPs associados de propriedade da Amazon ou EIPs não associados de propriedade da Amazon. Isso mostra o número total de endereços IP elásticos que você alocou na sua conta da AWS e que associou ou não a uma instância do EC2, interface de rede ou recurso da AWS. Caso filtre por essa medida e role até Endereços IP públicos na parte inferior da página, você verá detalhes sobre os recursos filtrados.
  - Em Uso de IPs IPv4 contíguos de propriedade da Amazon, monitore o uso sequencial de endereços IPv4 públicos ao longo do tempo e os grupos IPv4 do IPAM de propriedade da Amazon.
- Use o Amazon CloudWatch para rastrear e monitorar métricas relacionadas aos blocos IPv4 públicos contíguos fornecidos pela Amazon que foram provisionados para grupos do IPAM. Para ver as métricas disponíveis específicas para blocos IPv4 contíguos, consulte Métricas de IPs públicos em Métricas do IPAM. Além de visualizar métricas, você pode criar alarmes no Amazon CloudWatch para notificá-lo quando os limites forem atingidos. A criação de alarmes e a configuração de notificações com o Amazon CloudWatch está fora do escopo deste tutorial.

Para obter mais informações, consulte Uso de alarmes do Amazon CloudWatch no Manual do usuário do Amazon CloudWatch.

Command line

- Exiba as alocações do grupo do IPAM com o comando get-ipam-pool-allocations. Todos os endereços IP elásticos alocados do grupo do IPAM têm um Tipo de recurso de eip.

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

Exemplo de resposta:

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

- Use o Amazon CloudWatch para rastrear e monitorar métricas relacionadas aos blocos IPv4 públicos contíguos fornecidos pela Amazon que foram provisionados para grupos do IPAM. Para ver as métricas disponíveis específicas para blocos IPv4 contíguos, consulte Métricas de IPs públicos em Métricas do IPAM. Além de visualizar métricas, você pode criar alarmes no Amazon CloudWatch para notificá-lo quando os limites forem atingidos. A criação de alarmes e a configuração de notificações com o Amazon CloudWatch está fora do escopo deste tutorial. Para obter mais informações, consulte Uso de alarmes do Amazon CloudWatch no Manual do usuário do Amazon CloudWatch.

O tutorial agora está completo. Você criou um grupo do IPAM com um bloco CIDR IPv4 público contíguo fornecido pela Amazon, alocou endereços IP elásticos do grupo e aprendeu a monitorar as

alocações de grupos do IPAM. Continue na próxima seção para excluir os recursos que você criou neste tutorial.

Limpeza

Siga as etapas nesta seção para limpar os recursos criados neste tutorial.

Etapa 1: desassociar o endereço IP elástico

Conclua as etapas em Disassociate an Elastic IP address no Guia do usuário do Amazon EC2 para desassociar o endereço IP elástico.

Etapa 2: liberar o endereço IP elástico

Conclua as etapas em Release an Elastic IP address no Guia do usuário do Amazon EC2 para liberar um endereço IP elástico do grupo IPv4 público.

Etapa 3: Desprovisionar o CIDR do grupo do IPAM

Conclua as etapas em Desprovisionar CIDRs de um grupo para desprovisionar o CIDR público de propriedade da Amazon do grupo do IPAM. Essa etapa é necessária para a exclusão do grupo. Haverá cobrança pelo bloco IPv4 contíguo fornecido pela Amazon até que essa etapa seja concluída.

Etapa 4: excluir o grupo do IPAM

Conclua as etapas em Excluir um grupo para excluir o grupo do IPAM.

Etapa 5: excluir o IPAM

Conclua as etapas em Excluir um IPAM para excluir o IPAM.

O tutorial de limpeza está completo.

Identificar e acessar o gerenciamento no IPAM

A AWS usa credenciais de segurança para identificar você e conceder acesso aos recursos da AWS. É possível usar atributos do AWS Identity and Access Management (IAM) para permitir que outros usuários, serviços e aplicações usem os atributos da AWS, totalmente ou de maneira limitada, sem compartilhar as credenciais de segurança.

Esta seção descreve as funções vinculadas ao serviço da AWS que são criadas especificamente para o IPAM e as políticas gerenciadas anexadas às funções vinculadas ao serviço do IPAM. Para obter mais informações sobre funções e políticas do AWS IAM, consulte Termos e conceitos de funções no Guia do usuário do IAM.

Para obter mais informações sobre o gerenciamento de identidade e de acesso para a VPC, consulte Identity and Access Management para a Amazon VPC no Guia do usuário da Amazon VPC.

Conteúdo

- Funções vinculadas ao serviço do IPAM
- Políticas do IPAM gerenciadas pela AWS
- Exemplo de política

Funções vinculadas ao serviço do IPAM

O IPAM faz uso de perfis vinculados ao serviço do AWS Identity and Access Management (IAM). Um perfilo vinculado ao serviço corresponde a um tipo exclusivo de perfil do IAM. Os perfis vinculados ao serviço são definidos previamente pelo IPAM e incluem todas as permissões necessárias para o serviço chamar outros serviços da AWS em seu nome.

Um perfil vinculado ao serviço simplifica a configuração do IPAM, eliminando a necessidade de adicionar manualmente as permissões necessárias. As permissões dos perfis vinculados ao serviço são definidas pelo IPAM e, a menos que seja indicado de outra maneira, somente o IPAM pode assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Permissões de perfil vinculado ao serviço

O IPAM usa a função AWSServiceRoleForIPAM vinculada ao serviço para chamar as ações na política gerenciada AWSIPAMServiceRolePolicy anexada. Para obter mais informações sobre as ações permitidas nessa política, consulte Políticas do IPAM gerenciadas pela AWS.

Além disso, uma política de confiança do IAM está anexada ao perfil vinculado ao serviço, permitindo que o serviço `ipam.amazonaws.com` assuma o perfil vinculado ao serviço.

Criar a função vinculada ao serviço

O IPAM monitora o uso de endereços IP em uma ou mais contas assumindo a função vinculada ao serviço em uma conta, descobrindo os recursos e seus respectivos CIDRs e integrando os recursos ao IPAM.

Há duas maneiras de a função vinculada ao serviço ser criada:

- Quando você integra com o AWS Organizations

  Se você Integrar o IPAM a contas em uma organização da AWS Organizations usando o console do IPAM ou usando o comando `enable-ipam-organization-admin-account` da AWS CLI, a função vinculada ao serviço AWSServiceRoleForIPAM será criada automaticamente em cada uma de suas contas de membro do AWS Organizations. Como resultado, os recursos em todas as contas de membros são detectáveis pelo IPAM.

  Important

  Para que o IPAM crie a função vinculada ao serviço em seu nome:

  - A conta de gerenciamento do AWS Organizations que permite a integração do IPAM com o AWS Organizations deve ter uma política do IAM anexada a ela que permita as seguintes ações:
    - `ec2:EnableIpamOrganizationAdminAccount`
    - `organizations:EnableAwsServiceAccess`
    - `organizations:RegisterDelegatedAdministrator`
    - `iam:CreateServiceLinkedRole`
  - A conta IPAM deve ter uma política do IAM anexada a ela que permita a ação `iam:CreateServiceLinkedRole`.

- Quando você cria um IPAM usando uma única conta da AWS

  Se você Usar o IPAM com uma única conta, a função vinculada ao serviço AWSServiceRoleForIPAM é criada automaticamente quando você cria um IPAM como essa conta.

  > **Important**
  >
  > Se você usar o IPAM com uma única conta da AWS, antes de criar o IPAM, você deverá garantir que a conta da AWS que usar para criar o IPAM tenha anexada a ela uma política do IAM que permita a ação `iam:CreateServiceLinkedRole`. Ao criar o IPAM, você cria automaticamente a função vinculada ao serviço AWSServiceRoleForIPAM. Para obter mais informações sobre como gerenciar políticas do IAM, consulte Editar a descrição de um perfil vinculado ao serviço no Guia do usuário do IAM.

Editar a função vinculada ao serviço

Não é possível editar o perfil vinculado ao serviço AWSServiceRoleForIPAM.

Excluir a função vinculada ao serviço

Se você não precisar mais usar o IPAM, é recomendável excluir a função vinculada ao serviço AWSServiceRoleForIPAM.

> **Note**
>
> Você pode excluir a função vinculada a serviço somente após excluir todos os recursos do IPAM em sua conta da AWS. Isso garante que você não remova o recurso de monitoramento do IPAM por engano.

Siga estas etapas para excluir o perfil vinculado ao serviço usando a AWS CLI:

1. Exclua seus recursos do IPAM usando deprovision-ipam-pool-cidr e delete-ipam. Para obter mais informações, consulte Desprovisionar CIDRs de um grupo e Excluir um IPAM.
2. Desative a conta do IPAM com disable-ipam-organization-admin-account.
3. Desative o serviço do IPAM com disable-aws-service-access usando a opção `--service-principal ipam.amazonaws.com`.

4. Exclua a função vinculada ao serviço: delete-service-linked-role. Quando você exclui a função vinculada ao serviço, a política gerenciada pelo IPAM também é excluída. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Políticas do IPAM gerenciadas pela AWS

Ao empregar o IPAM com uma única conta AWS e criar um IPAM, a política gerenciada AWSIPAMServiceRolePolicy é automaticamente gerada em sua conta IAM e associada à função vinculada ao serviço AWSServiceRoleForIPAM.

Se você habilitar a integração do IPAM com o AWS Organizations, a política gerenciada AWSIPAMServiceRolePolicy será criada automaticamente em sua conta do IAM e em cada uma das suas contas de membros do AWS Organizations. Além disso, a política gerenciada será anexada à função vinculada ao serviço AWSServiceRoleForIPAM.

Essa política gerenciada habilita o IPAM para fazer o seguinte:

- Monitorizar CIDRs associados a recursos de rede em todos os membros da sua AWS Organização.
- Armazenar métricas relacionadas ao IPAM no Amazon CloudWatch, como o espaço de endereços IP disponível em seus grupos do IPAM e o número de CIDRs de recursos que estão em conformidade com as regras de alocação.
- Modificar e ler listas de prefixos gerenciados.

O exemplo a seguir mostra os detalhes da política gerenciada que foi criada.

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"
                }
            }
        }
    ]
}
```

A primeira instrução no exemplo anterior habilita o IPAM a monitorar os CIDRs usados pela sua única conta da AWS ou pelos membros do seu AWS Organization.

A segunda instrução no exemplo anterior usa a chave de condição `cloudwatch:PutMetricData` para permitir que o IPAM armazene métricas do IPAM em seunamespace do Amazon CloudWatch `AWS/IPAM`. Essas métricas são usadas pelo Console de gerenciamento da AWS para exibir dados sobre as alocações em seus grupos e escopos do IPAM. Para obter mais informações, consulte Monitorar o uso do CIDR com o painel do IPAM.

Atualiza a política gerenciada pela AWS

Visualize detalhes sobre atualizações em políticas do IPAM gerenciadas pela AWS desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
AWSIPAMServiceRolePolicy	Ações adicionadas à política gerenciada AWSIPAMServiceRolePolicy (ec2:ModifyManagedPrefixList, ec2:DescribeManagedPrefixLists e ec2:GetManagedPrefixListEntries) para permitir que o IPAM modifique e leia listas de prefixos gerenciados.	31 de outubro de 2025
AWSIPAMServiceRolePolicy	Ações adicionadas à política gerenciada AWSIPAMServiceRolePolicy (`organizations:ListChildren`, `organizations:ListParents` e `organizations:DescribeOrganizationalUnit`) para permitir que o IPAM obtenha os detalhes das unidades organizacionais (UOs) no AWS Organizations para que os clientes possam usar o IPAM ao nível da UO.	21 de novembro de 2024

Alteração	Descrição	Data
AWSIPAMServiceRolePolicy	Ação incorporada à política gerenciada AWSIPAMSe rviceRolePolicy (`ec2:GetIp amDiscoveredPublic Addresses`) para conceder ao IPAM a capacidade de adquirir endereços IP públicos durante a identificação de recursos.	13 de novembro de 2023
AWSIPAMServiceRolePolicy	Inclusão de ações na política gerenciada AWSIPAMSe rviceRolePolicy (`ec2:Descr ibeAccountAttribut es` , `ec2:Descr ibeNetworkInterfac es` , `ec2:Descr ibeSecurityGroups` , `ec2:DescribeSecuri tyGroupRules` , `ec2:DescribeVpnCon nections` , `globalacc elerator:ListAccel erators` , e `globalacc elerator:ListByoip Cidrs`) para habilitar o IPAM a obter endereços IP públicos durante a identificação de recursos.	1º de novembro de 2023

Alteração	Descrição	Data
AWSIPAMServiceRolePolicy	Adição de duas ações (`ec2:GetIpamDiscoveredAccounts` e `ec2:GetIpamDiscoveredResourceCidrs`) à política gerenciada AWSIPAMServiceRolePolicy para possibilitar ao IPAM a obtenção das contas de AWS e dos CIDRs dos recursos monitorados durante a identificação de recursos.	25 de janeiro de 2023
O IPAM começou a monitorar alterações	O IPAM começou a monitorar as alterações nas políticas gerenciadas pela AWS.	2 de dezembro de 2021

Exemplo de política

O exemplo de política nesta seção contém todas as ações relevantes AWS Identity and Access Management (IAM) para o uso total do IPAM. Dependendo de como você está usando o IPAM, talvez não seja necessário incluir todas as ações do IAM. Para ter uma experiência completa usando o console do IPAM, talvez seja necessário incluir ações adicionais do IAM para serviços como AWS Organizations, AWS Resource Access Manager (AWS RAM) e Amazon CloudWatch.

JSON

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

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

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

Cotas para o IPAM

Esta seção lista as cotas relacionadas ao IPAM. O console do Service Quotas também fornece informações sobre as cotas do IPAM. É possível usar o console do Service Quotas para visualizar cotas padrão e solicitar aumentos de cota para cotas ajustáveis. Para obter mais informações, consulte Solicitar um aumento da cota no Guia do usuário do Service Quotas.

Nome	Padrão	Ajustável
Blocos CIDR IPV4 públicos contíguos fornecidos pela Amazon	2	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Comprimento da máscara de rede dos blocos CIDR IPv4 públicos contíguos fornecidos pela Amazon	/29	O tamanho aceitável é entre /29 e /30. Para solicitar um aumento, entre em contato com a Central de suporte da AWS, conforme descrito em AWS service quotas na Referência geral da AWS.
Comprimento da máscara de rede do bloco CIDR IPv6 fornecido pela Amazon	/52	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.

Nome	Padrão	Ajustável
Blocos CIDR IPv6 fornecidos pela Amazon por grupo regional	1	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Números de sistema autônomo (ASNs) que você pode trazer para o IPAM	5	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
CIDRs por grupo	50	Sim
Alvos habilitados por política do IPAM	100	Sim. Para solicitar um ajuste de cota, entre em contato com a Central de suporte da AWS, conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Administradores do IPAM por organização	1	Não
IPAMs por região	1	Não

Nome	Padrão	Ajustável
Políticas do IPAM por IPAM	10	Sim. Para solicitar um ajuste de cota, entre em contato com a Central de suporte da AWS, conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Regras de alocação de políticas do IPAM por par recurso-localidade*	10	Sim. Para solicitar um ajuste de cota, entre em contato com a Central de suporte da AWS, conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Exclusões de unidade organizacional por descoberta de recursos	10	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Profundidade do grupo (o número de grupos dentro dos grupos)	10	Sim
Grupos por escopo	50	Sim
Resolvidores de lista de prefixos por IPAM	10	Sim

Nome	Padrão	Ajustável
Destinos do resolvedor de lista de prefixos por resolvedor de lista de prefixos	50	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Regras por resolução de lista de prefixos	100	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Entradas CIDR por versão do resolvedor da lista de prefixos	1000	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.
Associações de descoberta de recursos por IPAM	5	Sim
Descobertas de recursos por região	1	Não
Métricas de utilização de recursos	50	Sim. Entre em contato com o AWS Support Center conforme descrito em Cotas de serviço da AWS na Referência geral da AWS.

Nome	Padrão	Ajustável
Escopos por IPAM	5	Sim. Ao criar um IPAM, um escopo público e um privado são criados para você. Se você quiser criar escopos adicionais, eles serão escopos privados. Não é possível criar escopos públicos adicionais.

* Par recurso/localidade: ao definir regras de alocação, você deve especificar um tipo de recurso (o recurso da AWS como EIPs, ALBs ou clusters RDS) e uma localidade (a região da AWS ou zona local em que a regra se aplica). As regras de alocação têm como escopo essa combinação de tipo de recurso e localidade. Por exemplo, se você estiver definindo uma política para EIPs na região us-east-1, será possível definir até 10 regras para esse par específico de recurso-localidade*.

Preços do IPAM

O Gerenciador de endereços IP (IPAM) da Amazon VPC é um serviço que ajuda você a gerenciar seu espaço de endereços IP nos recursos da AWS e nas redes on-premises. O IPAM fornece uma maneira centralizada de planejar, monitorar e controlar os endereços IP usados pelos recursos da AWS e on-premises.

Esta seção descreve como visualizar as informações relacionadas a preços e seus custos atuais de IPAM.

Conteúdo

- Visualizar informações sobre preços
- Veja seus custos e uso atuais usando o AWS Cost Explorer

Visualizar informações sobre preços

O IPAM oferece dois níveis: gratuito e avançado. Para obter mais informações sobre os atributos disponíveis em cada nível e os custos associados aos níveis, consulte a guia IPAM na página de preços do Amazon VPC.

Veja seus custos e uso atuais usando o AWS Cost Explorer

Ao usar o nível avançado do IPAM, você paga um preço por hora por endereço IP ativo gerenciado pelo IPAM. Se quiser visualizar e analisar seus custos e uso do IPAM, você pode usar o AWS Cost Explorer.

1. Abra o console de AWS Cost Management em https://console.aws.amazon.com/cost-management/home.
2. Inicie o Cost Explorer.
3. Filtre o uso do IPAM escolhendo o Tipo de uso e inserindo **`IPAddressManager`**.
4. Marque uma ou mais caixas de seleção. Cada um delas representa uma região diferente da AWS.
5. Clique em Aplicar.

Se, por exemplo, selecionar USE1-IPAddressManager-IP-Hours(Hrs) e us-east-1 for a região inicial do IPAM, você verá o número de horas de IP ativo cobradas pelo IPAM em todas a regiões e também o custo. Digamos que o uso em horas seja 18, isso significa que você poderia ter 1 endereço IP ativo por 18 horas, 3 endereços IP em 3 regiões diferentes por 6 horas ou qualquer outra combinação que totalize 18 horas.

Para obter mais informações sobre o AWS Cost Explorer, consulte Análise dos custos com o AWS Cost Explorer no Manual do usuário do AWS Cost Management.

Informações relacionadas

Embora o site de documentação técnica da AWS seja um recurso abrangente, há muitos outros lugares em que é possível encontrar informações sobre os serviços da AWS. Os whitepapers, estudos de caso, fóruns comunitários e blogs da AWS podem fornecer informações valiosas, exemplos do mundo real e perspectivas alternativas, além dos detalhes técnicos oficiais. Explorar essas fontes diversas pode proporcionar uma compreensão mais completa das ofertas da AWS.

Os seguintes recursos relacionados podem ajudar enquanto você trabalha com o Gerenciador de endereços IP da Amazon VPC:

- Práticas recomendadas do Amazon VPC IP Address Manager: um blog da AWS sobre as práticas recomendadas para planejar e criar um esquema de endereços escalável com o Amazon VPC IP Address Manager.
- Gerenciamento e auditoria de endereços de rede em grande escala com o Amazon VPC IP Address Manager: um blog da AWS que apresenta o Amazon VPC IP Address Manager e mostra como usar o serviço no console da AWS.
- Configure o acesso refinado aos seus recursos compartilhados usando o AWS Resource Access Manager: um blog da AWS que explica como compartilhar um grupo IPAM com as contas em uma unidade organizacional do AWS Organizations.
- Visualizar o gerenciamento e planejamento de endereços IP corporativos com o mapa do CIDR: um blog da AWS que explica como visualizar todo o cenário de IPv4 e IPv6 usando o mapa do CIDR do IPAM no console do IPAM.

Histórico de documentos do IPAM

A tabela a seguir descreve todas as versões do IPAM.

Recurso	Descrição	Data de lançamento
Traga seu próprio IP para o CloudFront usando o IPAM	Use o IPAM para gerenciar seus CIDRs BYOIP para serviços globais da AWS, começando com os serviços anycast do CloudFront.	21 de novembro de 2025
Definir a estratégia de alocação de IPv4 público com as políticas do IPAM	Agora você pode usar políticas do IPAM para definir regras que mapeiam serviços da AWS para pools do IPAM específicos, ajudando a definir a estratégia de alocação de IPv4 público.	19 de novembro de 2025
Integrar o IPAM à infraestrutura da Infoblox	Agora você pode integrar o IPAM com a infraestrutura da Infoblox, permitindo gerenciar endereços IP da AWS por meio de seus fluxos de trabalho existentes da Infoblox e, ao mesmo tempo, obter recursos nativos da nuvem da AWS. Essa integração está disponível para escopos privados e requer o nível avançado do IPAM.	7 de novembro de 2025
Automatizar atualizações da lista de prefixos	Agora é possível usar resolvedores de lista de prefixos IPAM para automatizar atualizações de lista de prefixos com base em CIDRs de grupo do IPAM.	31 de outubro de 2025
Gerenciar alarmes a partir da console do IPAM	Agora, é possível criar e gerenciar alarmes do Amazon CloudWatch diretamente do console do IPAM. Os alarmes relacionados ao IPAM aparecerão como barras de aviso e indicadores visuais quando estiverem nos estados INSUFFICIENT_DATA ou ALARM.	21 de agosto de 2025

Recurso	Descrição	Data de lançamento
Habilitar a distribuição de custos	Ao habilitar a distribuição de custos, você distribui as cobranças por endereços IP ativos para as contas que usam os endereços IP, e não para o proprietário do IPAM. Isso é útil para grandes organizações em que o administrador delegado do IPAM gerencia os endereços IP centralmente usando o IPAM e cada conta é responsável por seu próprio uso, eliminando a necessidade de cálculos de cobrança manuais.	1.º de maio de 2025
Excluir unidades organizacionais do IPAM	Se o IPAM for integrado ao AWS Organizations, você agora poderá excluir unidades organizacionais do IPAM. O IPAM não gerenciará os endereços IP de contas em exclusões de unidades organizacionais.	21 de novembro de 2024
Atualizações de política gerenciada pela AWS: atualização de uma política existente	A política AWSIPAMServiceRolePolicy existente foi atualizada.	21 de novembro de 2024
Alocar endereços IP elásticos sequenciais de um grupo do IPAM	O IPAM permite que você provisione blocos IPv4 públicos de propriedade da Amazon para grupos do IPAM e aloque endereços IP elásticos sequenciais desses grupos para recursos da AWS. Os endereços IP elásticos sequenciais permitem que você simplifique suas necessidades de listagem de permissões de rede e segurança.	28 de agosto de 2024

Recurso	Descrição	Data de lançamento
GUAs e ULAs IPv6 privados	Agora você pode provisionar intervalos de GUAs e ULAs IPv6 privados para um grupo do IPAM em um escopo privado. Endereços IPv6 privados só estão disponíveis no IPAM. Para obter mais informações sobre o endereçam ento IPv6 privado, consulte Endereços IPv6 privados no Manual do usuário da Amazon VPC.	8 de agosto de 2024
Níveis gratuitos e avançados do IPAM	Agora você pode escolher entre o nível gratuito e o nível avançado para seu IPAM.	17 de novembro de 2023
Insights sobre IPs públicos	Anteriormente, você só podia ver insights de IP públicos em uma única região. Agora você pode ver insights de IP públicos em todas as regiões. Além disso, agora você pode visualiza r informações sobre insights de IP públicos no Amazon CloudWatch.	17 de novembro de 2023
Planeje o espaço de endereço IP da VPC para alocações IP de sub-rede	Agora é possível empregar o IPAM para estruturar o espaço de endereço IP da sub-rede em uma VPC e supervisionar as métricas associadas ao endereço IP em níveis de sub-rede e VPC.	17 de novembro de 2023
Traga seu próprio ASN (BYOASN)	Agora, você tem a capacidade de trazer o seu próprio Número de Sistema Autônomo (ASN) para AWS.	17 de novembro de 2023
Atualizações de política gerenciada pela AWS: atualizaç ão de uma política existente	A política AWSIPAMServiceRolePolicy existente foi atualizada.	17 de novembro de 2023

Recurso	Descrição	Data de lançamento
Atualizações de política gerenciada pela AWS: atualização de uma política existente	A política AWSIPAMServiceRolePolicy existente foi atualizada.	1º de novembro de 2023
Métricas de utilização de recursos	O IPAM agora publica métricas de utilização de IPs para recursos que o IPAM monitora no Amazon CloudWatch.	2 de agosto de 2023
Insights sobre IPs públicos	Insights sobre IPs públicos mostra todos os endereços IPv4 públicos usados pelos serviços nesta região na sua conta. É possível usar esses insights para identificar o uso de endereços IPv4 públicos e ver recomendações para liberar endereços IP elásticos não utilizados.	28 de julho de 2023
Atualizações de política gerenciada pela AWS: atualização de uma política existente	A política AWSIPAMServiceRolePolicy existente foi atualizada.	25 de janeiro de 2023
Integrar o IPAM a contas fora de sua organização	Agora, você pode gerenciar endereços IP fora da sua organização usando uma só conta do IPAM e compartilhar grupos do IPAM com as contas de outros AWS Organizations.	25 de janeiro de 2023
Bloco CIDR IPv6 contíguo fornecido pela Amazon para grupos do IPAM	Ao criar um grupo do IPAM no escopo público, agora você pode provisionar um bloco CIDR IPv6 contíguo fornecido pela Amazon para o grupo. Para obter mais informações, consulte Criar grupos de endereços IPv6 no IPAM.	25 de janeiro de 2023

Recurso	Descrição	Data de lançamento
Lançamento inicial	Esta versão apresenta o Amazon VPC IP Address Manager.	2 de dezembro de 2021