



IP Address Manager

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: IP Address Manager

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

O que é o IPAM?	1
Como funciona o IPAM	2
Conceitos básicos do IPAM	4
Acessar o IPAM	4
Configurar permissões para seu IPAM	5
Integrar o IPAM a contas em uma organização da AWS Organizations	5
Integrar o IPAM a contas fora de sua organização	8
Usar o IPAM com uma única conta	11
Criar um IPAM	12
Planejar o provisionamento de endereços IP	14
Exemplo de planos de grupo do IPAM	16
Criar grupos de IPv4	18
Criar grupos de IPv6	27
Alocar CIDRs	35
Criar uma VPC que usa um CIDR de um grupo do IPAM	36
Alocar manualmente um CIDR a um grupo para reservar o espaço de endereços IP	36
Gerenciar o espaço de endereços IP no IPAM	38
Impor o uso do IPAM para a criação da VPC	38
Aplicar o IPAM ao criar VPCs	39
Aplique um grupo do IPAM ao criar VPCs	39
Aplique o IPAM para todas, exceto uma determinada lista de UOs	40
Compartilhar um grupo do IPAM usando o AWS RAM	41
Provisionar CIDRs para um grupo	43
Desprovisionar CIDRs de um grupo	45
Editar um grupo	46
Excluir um grupo	47
Trabalhar com descobertas de recursos	48
Criar uma descoberta de recursos	49
Visualizar detalhes da descoberta de recursos	50
Compartilhar uma descoberta de recursos	52
Associar uma descoberta de recursos a um IPAM	55
Desassociar uma descoberta de recursos	56
Excluir uma descoberta de recursos	57
Criar escopos adicionais	57

Mover CIDRs da VPC entre escopos	59
Alterar o estado de monitoramento dos CIDRs da VPC	60
Excluir um escopo	61
Liberar uma alocação	62
Criar um IPAM	65
Criar um nível de IPAM	65
Modificar regiões operacionais do IPAM	66
Excluir um IPAM	67
Rastrear uso de endereços IP no IPAM	70
Monitorar o uso do CIDR com o painel do IPAM	70
Monitorar o uso do CIDR por recurso	73
Monitorar o IPAM com o Amazon CloudWatch	77
Grupo e métricas de escopo do IPAM	77
Métricas de utilização de recursos	79
Ver histórico de endereços IP	84
Visualizar insights de IPs públicos	88
Tutoriais	93
Criar um IPAM e grupos usando o console	93
Pré-requisitos	94
Como o AWS Organizations se integra ao IPAM	94
Etapa 1: delegar um administrador do IPAM	95
Etapa 2: criar um IPAM	97
Etapa 3: criar um grupo do IPAM de nível superior	99
Etapa 4: criar grupos regionais do IPAM	104
Etapa 5: criar um grupo de desenvolvimento pré-produção	108
Etapa 6: compartilhar o grupo do IPAM	112
Etapa 7: criar uma VPC com um CIDR alocado em um grupo do IPAM	117
Etapa 8: limpeza	121
Criar um IPAM e grupos usando a AWS CLI	122
Etapa 1: habilitar o IPAM na sua organização	123
Etapa 2: criar um IPAM	124
Etapa 3: criar um grupo de endereços IPv4	126
Etapa 4: provisionar um CIDR para o grupo de nível superior	128
Etapa 5. Criar um grupo regional com o CIDR originado do grupo de nível superior	129
Etapa 6: provisionar um CIDR para o grupo regional	131
Etapa 7. Criar um compartilhamento do RAM para habilitar atribuições de IP nas contas	133

Etapa 8. Crie uma VPC	133
Etapa 9. Limpeza	134
Visualizar o histórico de endereços IP com a AWS CLI	135
Visão geral	135
Cenários	136
Traga o seu ASN para o IPAM	144
Pré-requisitos de integração para seu ASN	145
Etapas do tutorial	145
Trazer seus endereços IP para o IPAM	149
Console AWS e CLI	151
Somente AWS CLI	177
Transferir um CIDR IPv4 BYOIP para o IPAM	220
Etapa 1: criar perfis nomeados da AWS CLI e perfis do IAM	221
Etapa 2: obter o ID de escopo público do IPAM	222
Etapa 3: criar um grupo do IPAM	223
Etapa 4: compartilhar o grupo do IPAM usando o AWS RAM	225
Etapa 5: transferir um CIDR IPv4 BYOIP existente para o IPAM	227
Etapa 6: visualizar o CIDR no IPAM	230
Etapa 7: limpeza	230
Planeje o espaço de endereço IP da VPC para alocações IP de sub-rede	234
Etapa 1: Criar uma VPC	235
Etapa 2: Criar um grupo de planejamento de recursos	236
Etapa 3: Criar grupos de sub-redes	237
Etapa 4: Criar sub-redes	238
Etapa 5: limpeza	239
Identificar e acessar o gerenciamento no IPAM	240
Funções vinculadas ao serviço do IPAM	240
Permissões concedidas à função vinculada ao serviço	240
Criar a função vinculada ao serviço	241
Editar a função vinculada ao serviço	242
Excluir a função vinculada ao serviço	242
Políticas do IPAM gerenciadas	243
Atualiza a política gerenciada pela AWS	244
Exemplo de política	246
Cotas	249
Definição de preço	251

Visualizar informações sobre preços	251
Veja seus custos e uso atuais usando o AWS Cost Explorer	251
Informações relacionadas	252
Histórico do documento	253

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

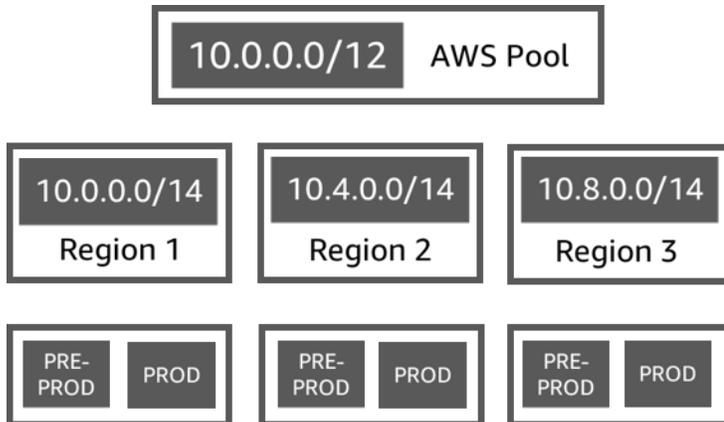
Este guia consiste nas seguintes seções:

- [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. Um IPAM contém dois escopos padrão. 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. 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 os CIDRs IPv4 privados, CIDRs IPv4/IPv6 públicos que você possui e espaço IPv6 público pertencente à Amazon.

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. 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.

Conteúdo

- [Acessar o IPAM](#)
- [Configurar permissões para seu IPAM](#)
- [Criar um IPAM](#)
- [Planejar o provisionamento de endereços IP](#)
- [Alocar CIDRs](#)

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 inclusive 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 documentação da AWS CLI que mostra como fazer a mesma coisa 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 permissões para seu IPAM](#).

Configurar permissões para seu IPAM

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 outras 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.

Important

- 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.

Note

Ao integrar ao AWS Organizations:

- 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 do IPAM deve ser uma conta membro do AWS Organizations. Não é possível utilizar a conta de gerenciamento do AWS Organizations como a conta do IPAM.
- 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. Escolha 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 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.

- 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](#) e [Compartilhar uma descoberta de recursos](#)). 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 usando AWS 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 próxima seção, uma função vinculada ao serviço é criada automaticamente para o serviço IPAM da Amazon VPC no AWS Identity and Access Management. 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 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.

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.

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](#).

Conteúdo

- [Exemplo de planos de grupo do IPAM](#)

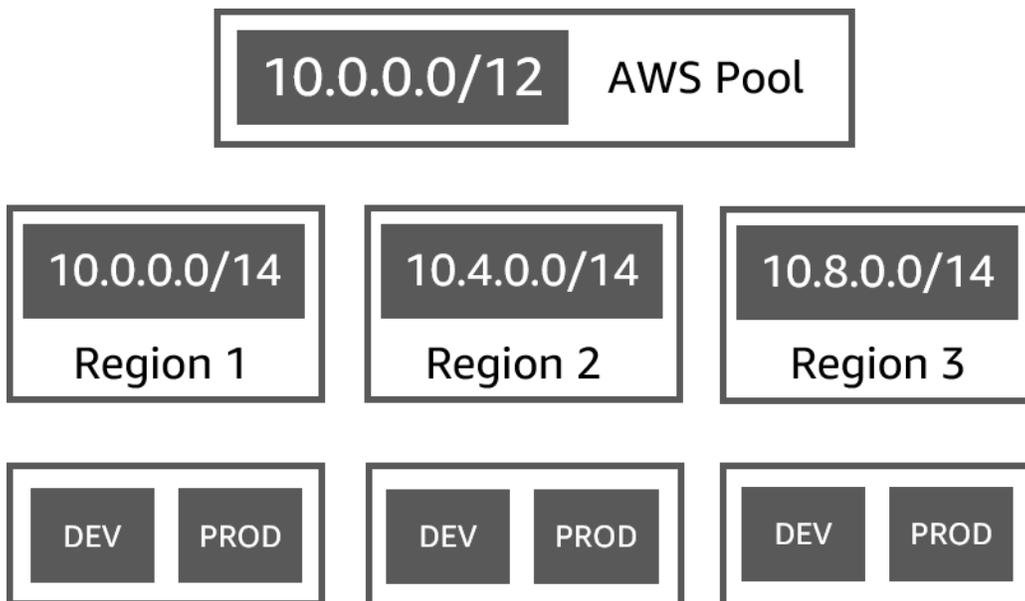
- [Criar grupos de IPv4](#)
- [Criar grupos de IPv6](#)

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.

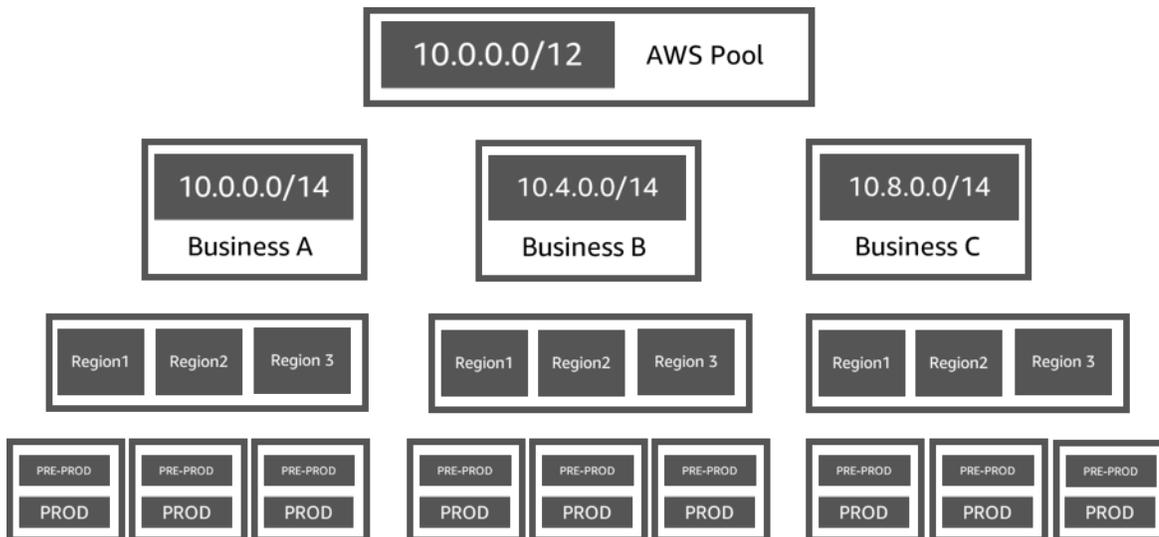
Grupos de IPv4 em várias regiões da AWS

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.



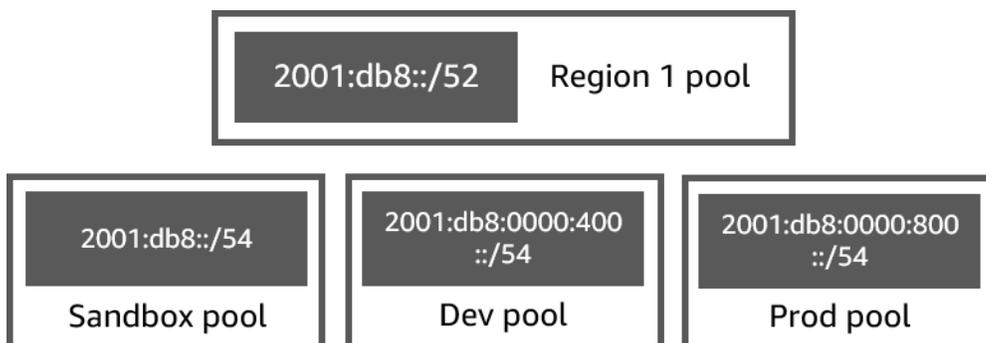
Grupos de IPv4 para várias linhas de negócios

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.



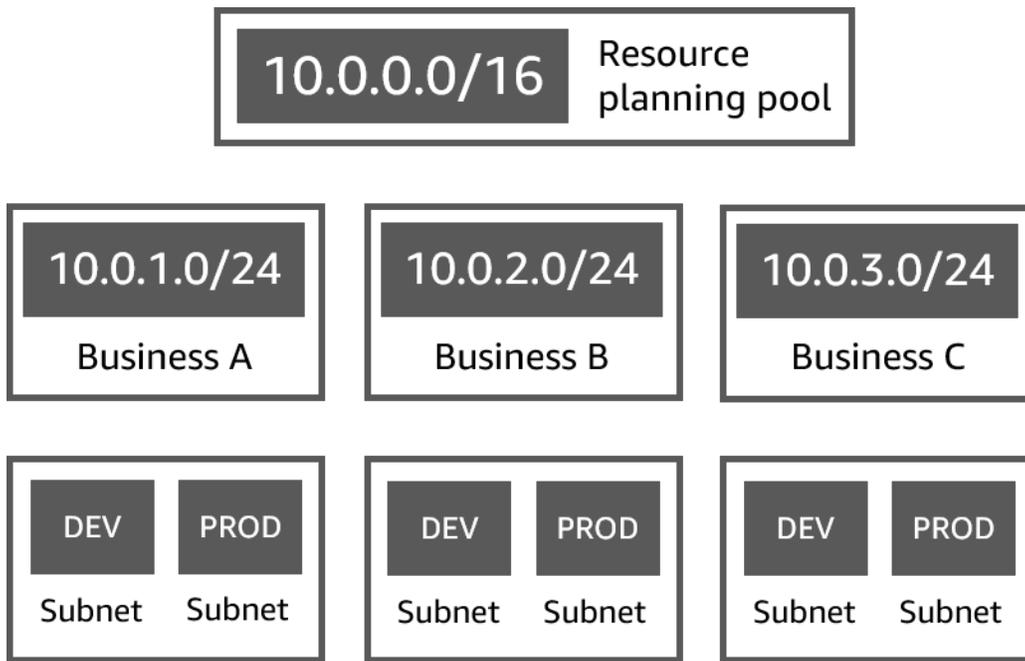
Grupos de IPv6 em uma região da AWS

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 de recursos para área restrita para testes, 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, um recurso ainda pode ser criado usando um CIDR maior que /24 desse grupo se o espaço estiver disponível, mas como isso viola uma regra de alocação no grupo, o IPAM sinaliza esse recurso como não compatível.

⚠ 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 ter 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 ter 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.

12. (Opcional) Escolha Tags (Etiquetas) para o grupo.

13. Selecione Criar.

14. Consulte [Criar um grupo regional de IPv4](#).

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.

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](#).

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. 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.

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](#).

9. (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.
10. 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.
11. (Opcional) Escolha Tags (Etiquetas) para o grupo.
12. Ao terminar de configurar o grupo, escolha Create pool (Criar grupo).
13. Consulte [Criar um grupo de desenvolvimento de IPv4](#).

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.

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](#).

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](#).

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.

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 IPv6

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.

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

Conteúdo

- [Criar um grupo regional de IPv6](#)
- [Criar um grupo de desenvolvimento de IPv6](#)

Criar um grupo regional de IPv6

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 público
 - 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](#).

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.

Important

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 seus próprios intervalos

de endereços IP IPv4 ou IPv6 para a AWS (BYOIP). Para ter 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 público. 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 que pode ser ou está sendo anunciado pela AWS na Internet.

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. A opção Permitir que os CIDRs neste grupo sejam anunciados publicamente é exibida. Por padrão, todos os CIDRs desse grupo poderão ser anunciados publicamente. Não é possível habilitar ou desabilitar essa opção.
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. 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. 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. 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 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. Na opção Fonte de IP público, escolha Pertencente à Amazon para que a AWS forneça 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 ter mais informações, consulte [Tutorial: trazer seus endereços IP para o IPAM](#).
12. Para grupos no escopo público que usam o BYOIP de origem de IP pública, você pode controlar se a AWS pode anunciar publicamente os CIDRs nesse grupo com a opção Permitir que os CIDRs deste grupo sejam anunciados publicamente. Por padrão, essa opção está habilitada. Desabilite essa opção se não quiser permitir que a AWS anuncie publicamente os CIDRs neste grupo.
13. (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, escolha Adicionar CIDR pertencente à Amazon e escolha o tamanho da máscara de rede entre /40 e /52 para o CIDR.

 Note

Observe o seguinte:

- 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](#).
- 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.

14. 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.

15. (Opcional) Escolha Tags (Etiquetas) para o grupo.

16. Selecione Criar.

17. Consulte [Criar um grupo de desenvolvimento de IPv6](#).

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.

Use os seguintes comandos da AWS CLI para criar ou editar um grupo regional de IPv6 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 de desenvolvimento de IPv6

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](#).

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 público
 - 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 o escopo público. 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 que pode ser ou está sendo anunciado pela AWS na Internet.

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 IPv6](#) 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](#).

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.

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

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

- [Criar 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](#)

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

Siga as etapas em [Criar 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 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.

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. 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

- [Impor o uso do IPAM para a criação da VPC](#)
- [Compartilhar um grupo do IPAM usando o AWS RAM](#)
- [Provisionar CIDRs para um grupo](#)
- [Desprovisionar CIDRs de um grupo](#)
- [Editar um grupo](#)
- [Excluir um grupo](#)
- [Trabalhar com descobertas de recursos](#)
- [Criar escopos adicionais](#)
- [Mover CIDRs da VPC entre escopos](#)
- [Alterar o estado de monitoramento dos CIDRs da VPC](#)
- [Excluir um escopo](#)
- [Liberar uma alocação](#)
- [Criar um IPAM](#)
- [Excluir um IPAM](#)

Impor o uso do IPAM para a criação da VPC

Note

Esta seção só se aplica a você se você tiver habilitado o IPAM para se integrar ao AWS Organizations. Para ter 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 em [Criar um SCP](#) no Guia do usuário do AWS Organizations e insira o seguinte texto no editor 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 [Anexar e desvincular políticas de controle de serviço](#) 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 em [Criar um SCP](#) no Guia do usuário do AWS Organizations e insira o seguinte texto no editor 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 [Anexar e desvincular políticas de controle de serviço](#) 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 exige que as UOs na organização, exceto para as UOs especificadas em `aws:PrincipalOrgPaths`, usem o IPAM para criar e expandir 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 em [Criar um SCP](#) no Guia do usuário do AWS Organizations e insira o seguinte texto no editor JSON:

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

```
"Condition": {
  "Null": {
    "ec2:Ipv4IpamPoolId": "true"
  },
  "ForAllValues:StringNotLike": {
    "aws:PrincipalOrgPaths": [
      "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/",
      "o-a1b2c3d4e5/r-ab12/ou-ab13-22222222/ou-ab13-33333333/"
    ]
  }
}
}]
}
```

2. 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 AWS Identity and Access Management.
3. Anexe a política à raiz da sua organização. Para obter mais informações, consulte [Anexar e desvincular políticas de controle de serviço](#) no Guia do usuário do AWS Organizations.

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 ter 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.

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 AWS RAM 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

Os comandos nesta seção estão vinculados à Documentação de referência da 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 [Criar uma VPC](#) no Guia do usuário da Amazon VPC.

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. Insira o CIDR que você quer adicionar e escolha Add new CIDR (Adicionar novo CIDR) para CIDRs adicionais.

 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 Request provisioning (Solicitar provisionamento).

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 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.

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](#)

Desprovisionar CIDRs de um grupo

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.

Important

Não é possível desprovisionar o CIDR se houver alocações no grupo. Para remover alocações, consulte [Liberar uma alocação](#).

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 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.

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

Siga as etapas nesta seção para editar um grupo do IPAM. Talvez você queira editar um grupo para alterar as regras de alocação no grupo. Para obter mais informações sobre etiquetas de alocação de custos, consulte [Criar um grupo de IPv4 de nível superior](#).

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. Escolha 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](#)

Excluir um grupo

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

Important

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.

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 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.

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](#).

Trabalhar com descobertas de recursos

A descoberta de recursos é um componente do IPAM que habilita o IPAM a gerenciar e monitorar recursos que pertencem à conta proprietária. 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.

Conteúdo

- [Criar uma descoberta de recursos](#)
- [Visualizar detalhes da descoberta de recursos](#)
- [Compartilhar uma descoberta de recursos](#)
- [Associar uma descoberta de recursos a um IPAM](#)
- [Desassociar uma descoberta de recursos](#)

- [Excluir uma descoberta de recursos](#)

Criar uma descoberta de recursos

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 atributo 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 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.

- Criar uma descoberta de recursos: [create-ipam-resource-discovery](#)

Visualizar detalhes da descoberta de recursos

Esta seção descreve como visualizar os detalhes para uma descoberta de recursos. Isso inclui os CIDRs de recursos e os status de descoberta das contas monitoradas durante sua descoberta 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.
- Uso de IP: o percentual de espaço de endereços 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 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.

- Exibir detalhes da descoberta de recursos: [describe-ipam-resource-discovery](#)

Compartilhar uma descoberta de recursos

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 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 ter mais informações, consulte [Associar uma descoberta de recursos a um 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.

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 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.

- 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 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.

- 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 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.

- Para excluir uma descoberta de recursos: [delete-ipam-resource-discovery](#)

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 privados, os CIDRs de 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 ter 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 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.

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](#)

Mover CIDRs da VPC entre escopos

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](#)

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 ter mais informações, consulte [Preços do IPAM](#).
- Se um CIDR for ignorado, você ainda poderá visualizar o histórico dos endereços IP no CIDR. Para ter 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](#)

Excluir um escopo

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

Important

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 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.

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](#).

Liberar uma alocação

Siga as etapas nesta seção para liberar uma alocação de CIDR de um grupo do IPAM. Uma alocação é uma atribuição CIDR de um grupo do IPAM para outro recurso ou grupo do IPAM.

Se você estiver planejando excluir um grupo, talvez seja necessário liberar uma alocação de grupo. 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 ter 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. Leva alguns minutos para que o CIDR fique disponível para alocações futuras. 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.
7. Escolha Actions (Ações) > Release custom allocation (Liberar alocação personalizada).
8. Escolha Deallocate CIDR (Desalocar CIDR).

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.

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](#). Para excluir o grupo após liberar alocações, primeiro é necessário [Desprovisionar CIDRs de um grupo](#).

Criar um IPAM

Siga as etapas nesta seção para modificar um IPAM.

Conteúdo

- [Criar um nível de IPAM](#)
- [Modificar regiões operacionais do IPAM](#)

Criar um nível de IPAM

Siga as etapas nesta seção para modificar um nível de IPAM. O IPAM oferece dois níveis: nível gratuito e nível avançado. 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](#).

Important

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

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.

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

Siga os passos desta seção para modificar as regiões de funcionamento 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.

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 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.

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](#)

Excluir um IPAM

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](#).

Important

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 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 opção. 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 ter mais informações, consulte [Liberar uma alocação](#).
 - Desprovisione os CIDRs provisionados para grupos dentro do IPAM. Para ter mais informações, consulte [Desprovisionar CIDRs de um grupo](#).
 - Exclua quaisquer escopos não padrão adicionais. Para ter mais informações, consulte [Excluir um escopo](#).
 - Exclua seus grupos do IPAM. Para ter mais informações, consulte [Excluir um grupo](#).

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

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.

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](#).

Rastrear uso de endereços IP no IPAM

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.

Siga as etapas nesta seção para rastrear o uso de endereços IP com o 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

Siga as etapas desta seção para acessar o painel do IPAM e exibir o status de todos os CIDRs em um escopo do IPAM específico.

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](#).
- **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](#).
- **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

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.

- **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:
 - VPCs
 - Grupos IPv4 públicos

Important

Os grupos IPv4 públicos e os grupos do IPAM são gerenciados por recursos distintos na AWS. Os 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.

- **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:
 - VPCs
 - Grupos IPv4 públicos
 - Sub-redes VPC

- Endereços IP elásticos

As etapas a seguir mostram como monitorar o uso do CIDR e a conformidade com regras de alocação por recurso.

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 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. 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.

5. 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.
 - Uso de IP: para recursos que são VPCs, esse valor é a porcentagem 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).
 - 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.
6. 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 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.

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.

Conteúdo

- [Grupo e métricas de escopo do IPAM](#)
- [Métricas de utilização de recursos](#)

Grupo e métricas de escopo do IPAM

O IPAM publica dados sobre seus grupos e 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 de grupo do 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 .

Nome da métrica	Descrição
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.
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

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 atualmente estão associados a recursos gerenciáveis, mas não são gerenciados pelo IPAM.

As dimensões que você pode usar para filtrar métricas do IPAM são listadas abaixo.

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

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.
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 instâncias 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.

ℹ 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 ter 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 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.

- 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 for 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 atributo
 - 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

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, Amazon RDS ou Amazon Workspaces.

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.

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.
- 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.
- 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

- [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](#)

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

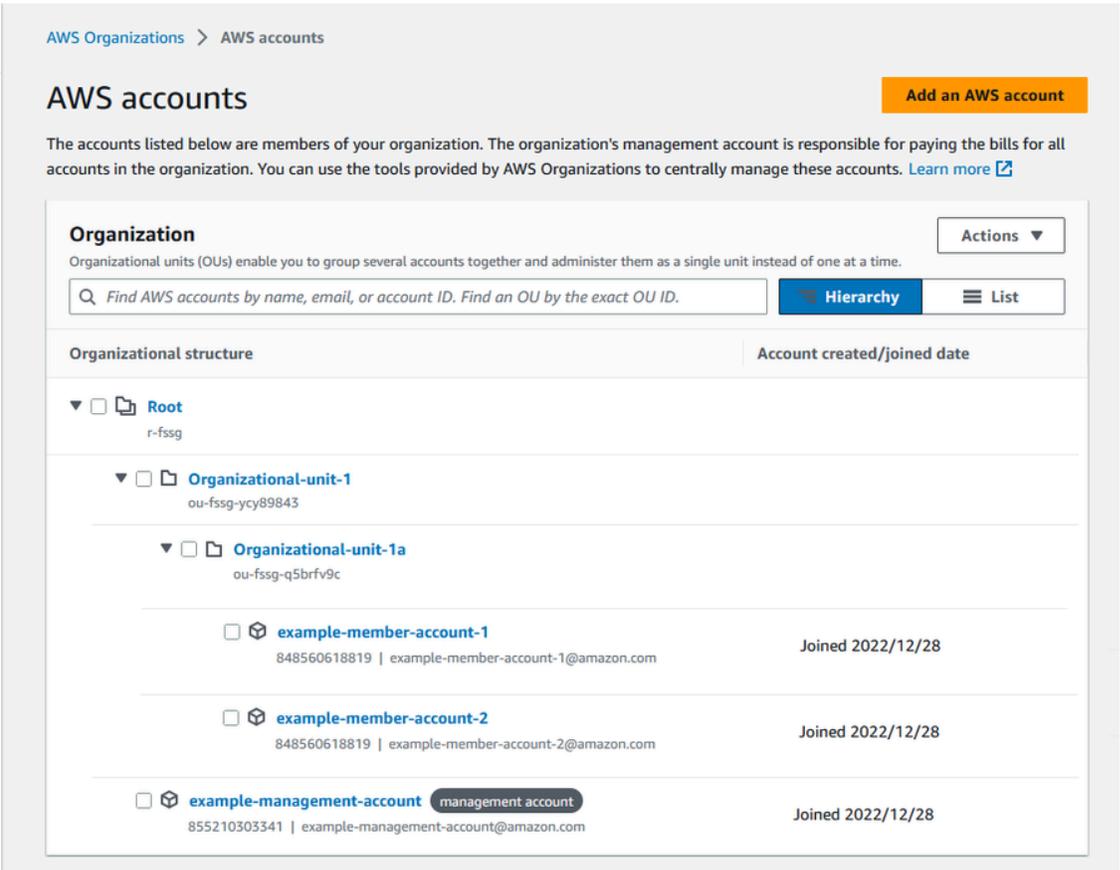
Antes de começar, é preciso ter configurado uma conta do AWS Organizations com ao menos uma conta de membro. Para obter instruções, consulte [Criar e gerenciar uma organização](#) no Guia do usuário do AWS Organizations.

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.



AWS Organizations ×

AWS Organizations > AWS accounts

AWS accounts Add an AWS account

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

Organization Actions

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

Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID. Hierarchy List

Organizational structure Account created/joined date

Organizational structure	Account created/joined date
Root r-fssg	
Organizational-unit-1 ou-fssg-ycy89843	
Organizational-unit-1a ou-fssg-q5brfv9c	
example-member-account-1 848560618819 example-member-account-1@amazon.com	Joined 2022/12/28
example-member-account-2 848560618819 example-member-account-2@amazon.com	Joined 2022/12/28
example-management-account 855210303341 example-management-account@amazon.com	Joined 2022/12/28

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 ter 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 em que você deseja trabalhar com o IPAM.
3. No painel de navegação, selecione Organization settings (Configurações da organização).
4. Escolha 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.

The screenshot shows the 'Settings' page for Amazon VPC IP Address Manager. The breadcrumb navigation is 'Amazon VPC IP Address Manager > Settings > Edit'. The main heading is 'Settings' with an 'Info' link. Below this is a section titled 'Delegated administrator'. Underneath, there is a sub-section 'Delegated administrator account' with a descriptive text: 'The account to be delegated as the IPAM administrator for your organization. To monitor resources across your organization, the IPAM must be created in the delegated administrator's account.' Below this text is a text input field with the placeholder text 'Enter an account ID for the IPAM administrator'. Further down is a sub-section 'Service access' with the text: 'When you delegate an IPAM administrator, you grant Amazon VPC IP Address Manager permission to describe resources on your behalf.' Below this text is a 'View details' button. At the bottom right of the form are two buttons: 'Cancel' and 'Save changes'.

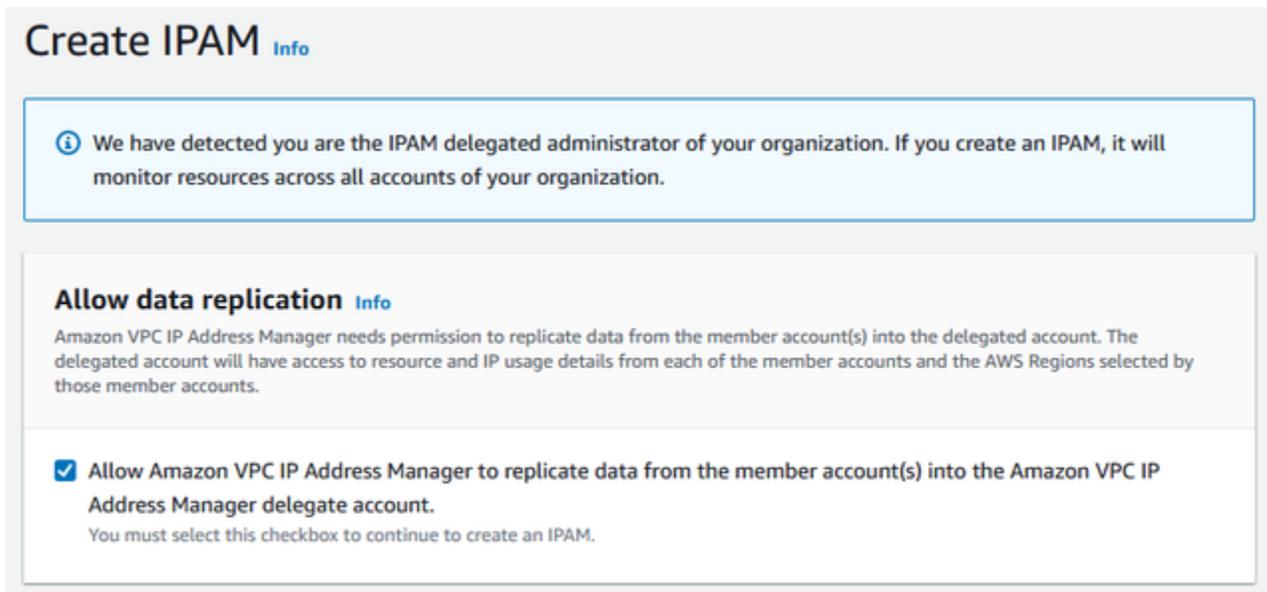
6. Escolha Salvar alterações. As informações do administrador delegado são preenchidas com detalhes relacionados à conta do membro.

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 ter 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.



Create IPAM [Info](#)

ⓘ We have detected you are the IPAM delegated administrator of your organization. If you create an IPAM, it will monitor resources across all accounts of your organization.

Allow data replication [Info](#)

Amazon VPC IP Address Manager needs permission to replicate data from the member account(s) into the delegated account. The delegated account will have access to resource and IP usage details from each of the member accounts and the AWS Regions selected by those member accounts.

Allow Amazon VPC IP Address Manager to replicate data from the member account(s) into the Amazon VPC IP Address Manager delegate account.

You must select this checkbox to continue to create an 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.

IPAM settings [Info](#)

Name tag - *optional*

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

Description - *optional*

Write a brief description for the IPAM.

Operating Regions

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



Default resources will be created

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

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

6. Escolha Create IPAM (Criar IPAM).

✔ Successfully created IPAM ipam-005f921c17ebd5107✕

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

DemoIPAM (ipam-005f921c17ebd5107) Info

Edit Delete

IPAM details

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

Operating Regions | Associated discoveries | Tags

Operating Regions (3) Info

< 1 > ⚙

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

Etapa 3: criar um grupo do IPAM de nível superior

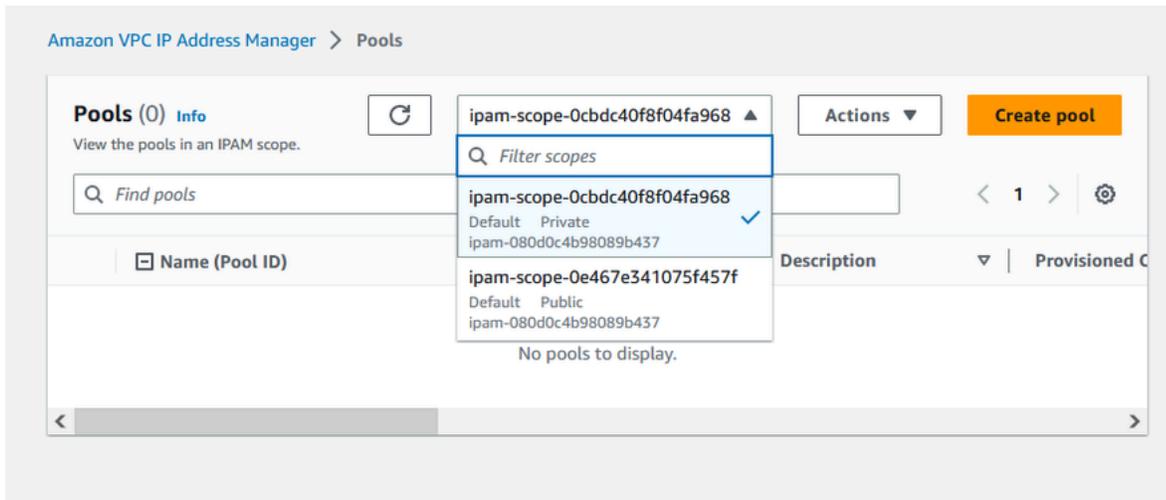
Neste tutorial, você cria uma hierarquia de grupos iniciando pelo grupo do IPAM de nível superior. Nas etapas seguintes, você criará um par de grupos regionais e um grupo de desenvolvimento de pré-produção em um dos grupos regionais.

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.

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

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

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

Description - optional
Write a brief description for the pool.

Pool hierarchy [Info](#)

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

Address family
Select the address family for this pool.

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

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

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

CIDRs to provision [Info](#)

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

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/16	65K IPs	Remove
< > ^ v		

Add new CIDR

- 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.

Allocation rule settings - *optional* [Info](#)



AWS best practice

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

Configure this pool's allocation rule settings

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

Sent request to provision 10.0.0.0/16

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

Global pool (ipam-pool-06fb4cace4bc1e551)

Pool summary

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

Pool details | Monitoring | IP space visualization | **CIDRs** | Allocations | Resources | Compliance | Reso

CIDRs (1) Info

Deprovision CIDRs | Provision CIDR

Filter CIDRs

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

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

✔ Sent request to provision 10.0.0.0/16✕

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

Global pool (ipam-pool-06fb4cace4bc1e551) ↻ Actions ▾

Pool summary

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

< Pool detailsMonitoringIP space visualizationCIDRsAllocationsResourcesComplianceResc >

CIDRs (1) Info

Filter CIDRsDeprovision CIDRsProvision CIDR

<input type="checkbox"/>	CIDR	CIDR ID	State
<input type="checkbox"/>	10.0.0.0/16	ipam-pool-cidr-0657f970d119e40899...	✔ Provisioned

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

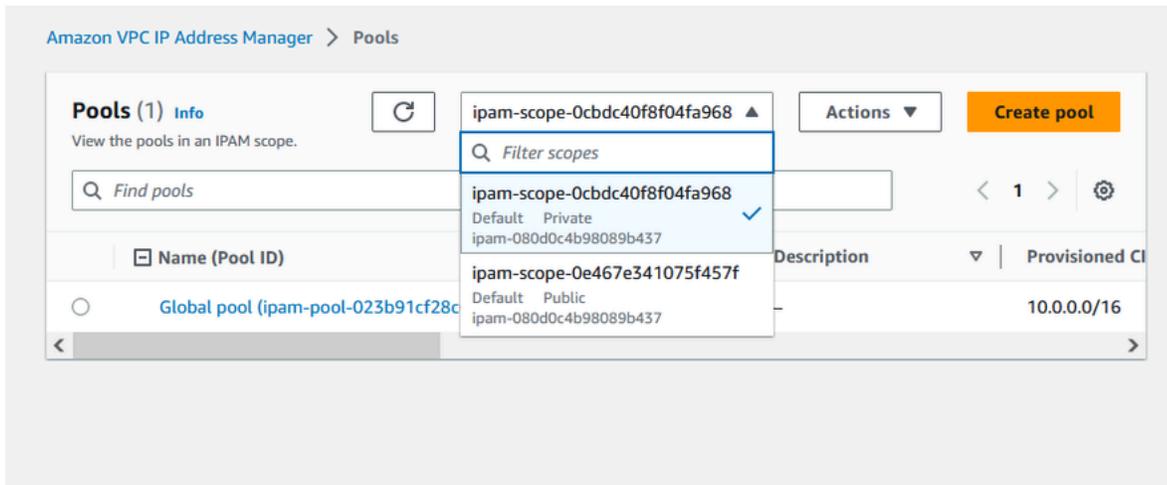
Etapa 4: criar grupos regionais do IPAM

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.

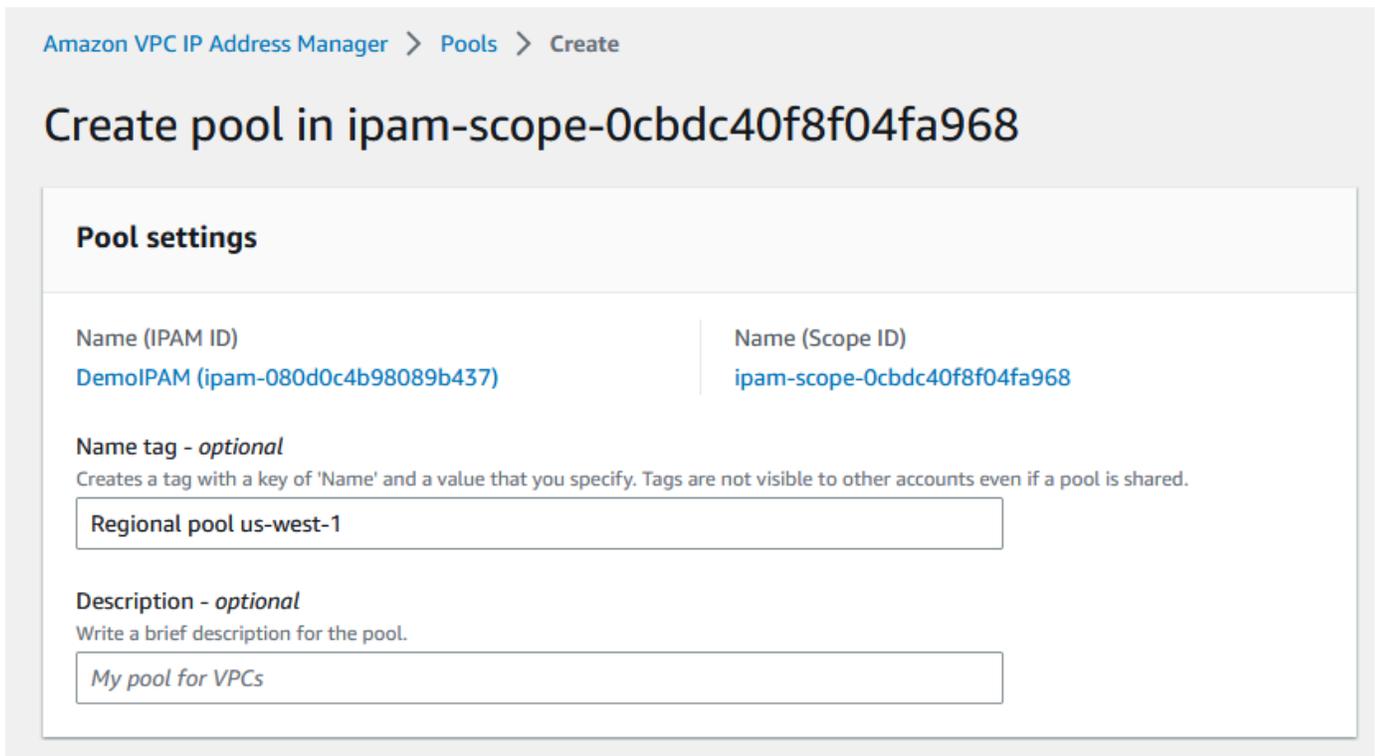
Para criar um grupo regional

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.

Pool hierarchy [Info](#)

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

Global pool (ipam-pool-023b91cf28c61a0fb) ▼

▼ **Source pool summary**

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

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

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

US West (N. California) - us-west-1 ▼

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

8. 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.

CIDRs to provision [Info](#)

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

IP space visualization (source pool)

Zoom Overlapping New allocation Allocated Available

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



CIDR

Enter a CIDR to be provisioned.

16K IPs

< > ^ v

- 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.

Allocation rule settings - *optional* [Info](#)

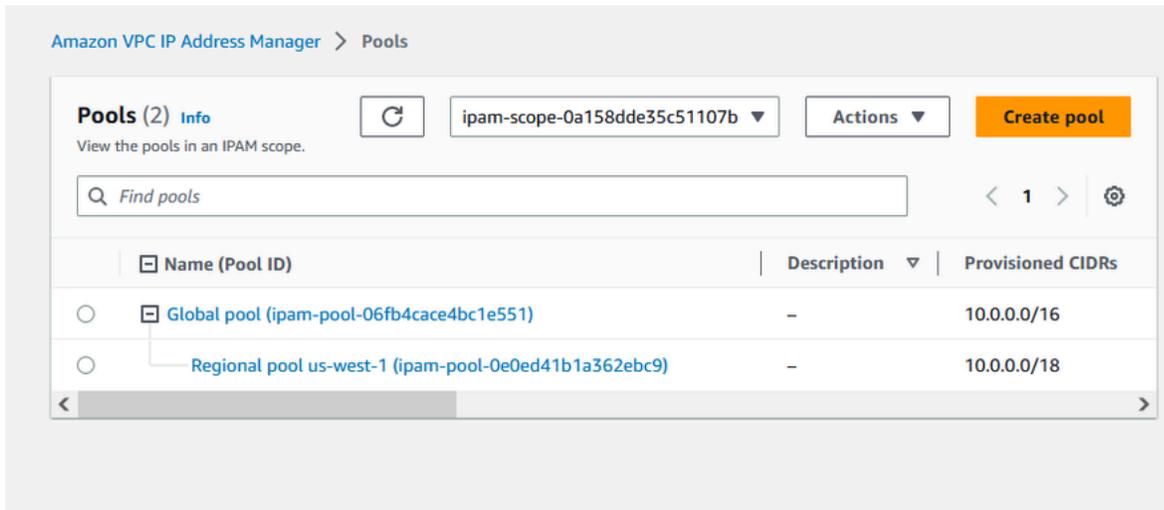


AWS best practice

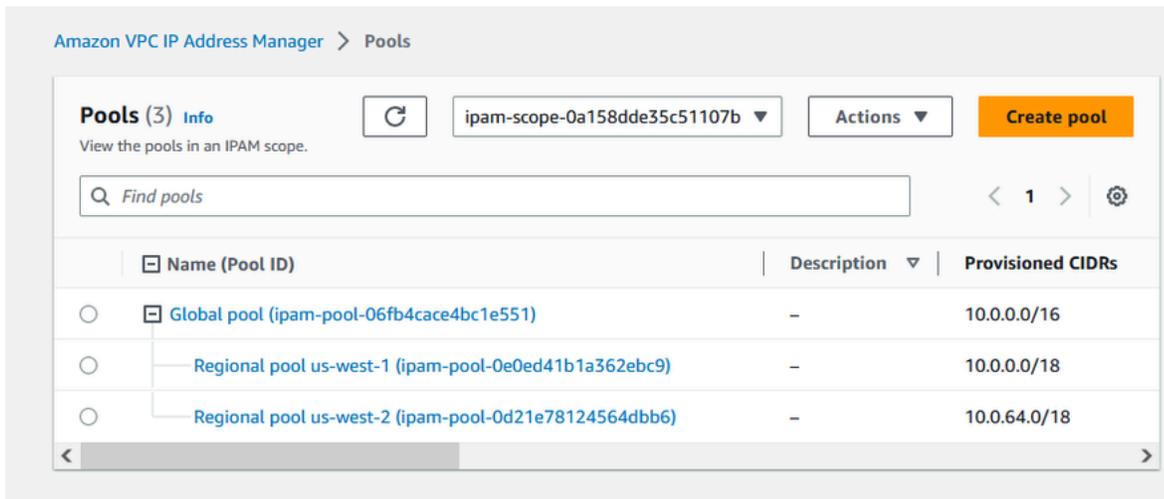
We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize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

Configure this pool's allocation rule settings

- Selecione Criar.
- 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.

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

Name (IPAM ID)

DemoIPAM (ipam-080d0c4b98089b437)

Name (Scope ID)

ipam-scope-0cbdc40f8f04fa968

Name tag - *optional*

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

Description - *optional*

Write a brief description for the pool.

Pool hierarchy [Info](#)

Source pool

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

▼ Source pool summary

Name (Pool ID)

Regional pool us-west-1 (ipam-pool-03b74e706bb0df4ab)

Description

-

Provisioned CIDRs

10.0.0.0/18

Locale

us-west-1

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

CIDRs to provision [Info](#)

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

IP space visualization (source pool)

Zoom Overlapping New allocation Allocated Available

10.0.0.0/18 (100% available → 75% available after allocations)

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/20 4K IPs Remove

< > ^ v

Add specific CIDR Add CIDR by size

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.

Allocation rule settings - *optional* [Info](#)



AWS best practice

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

Configure this pool's allocation rule settings

CIDR management

Automatically import discovered resources

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

- Allow automatic import
- Don't allow

Netmask compliancy

Minimum netmask length

The minimum netmask length for allocating resources within the pool.

/24 (256 IPs)

Default netmask length

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

/24 (256 IPs)

Maximum netmask length

The maximum netmask length for allocating resources within the pool.

/24 (256 IPs)

Tag compliancy

Tagging requirements

Add tagging requirements for resources in this pool.

Key

environment



Value - *optional*

pre-prod



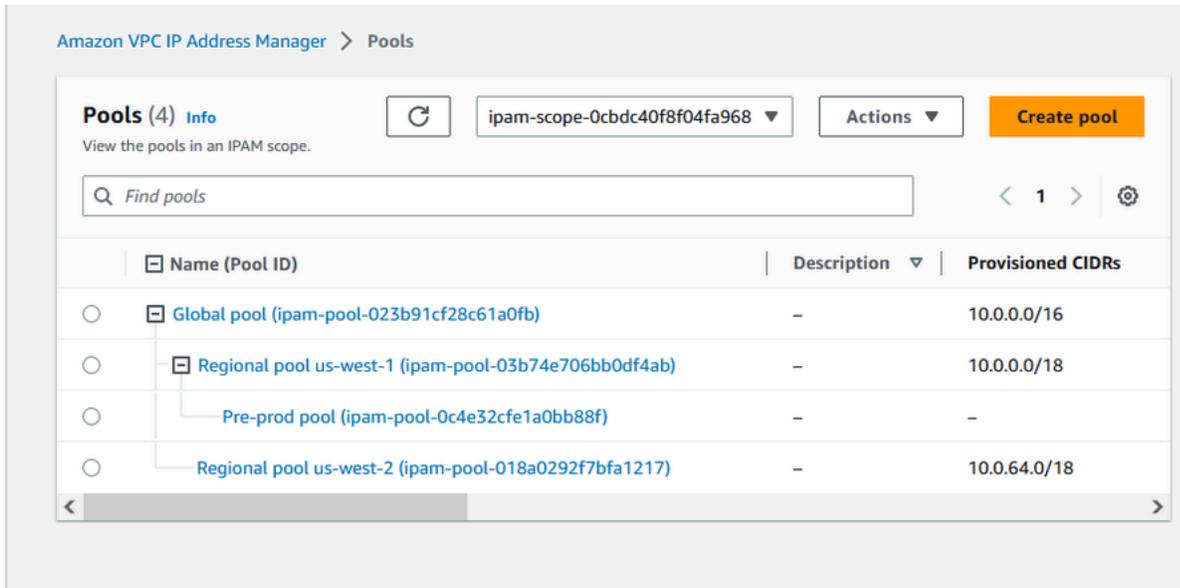
Remove

Add new required tag

You can add up to 49 more tags.

4. 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:

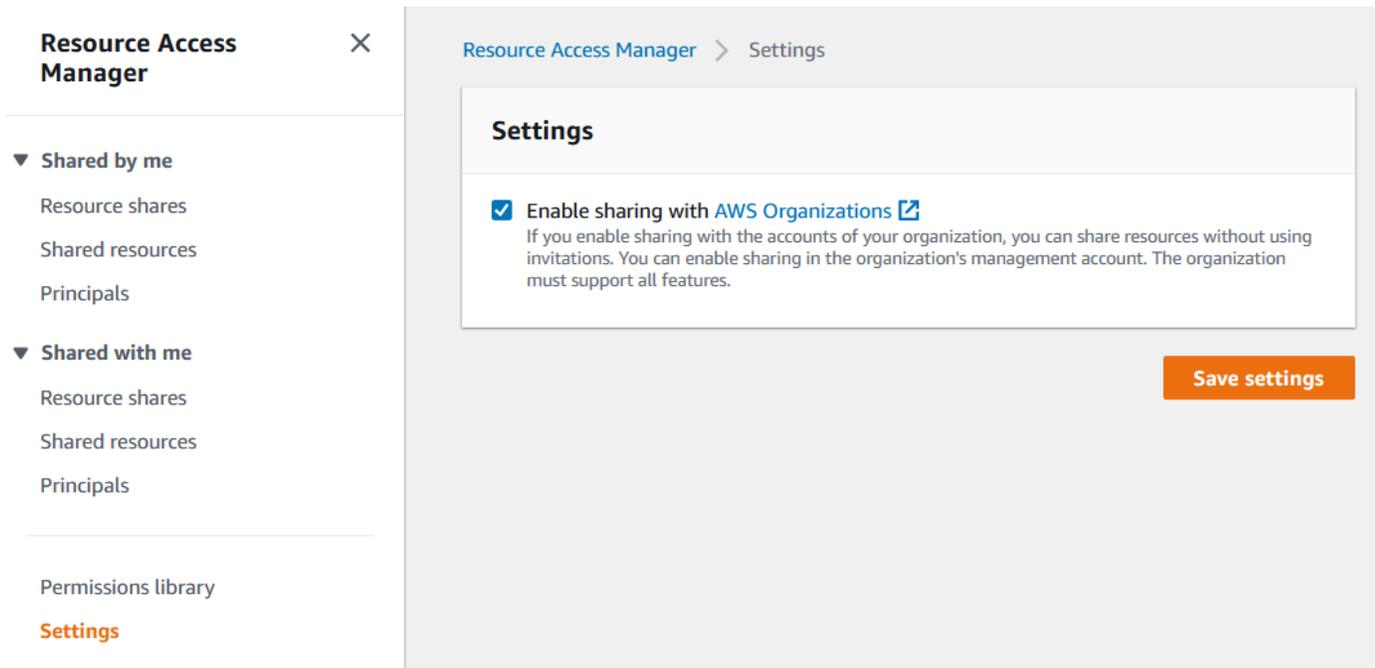
- [Etapa 6.1. Habilitar o compartilhamento de recursos no AWS RAM](#): esta etapa deve ser realizada pela conta de gerenciamento do AWS Organizations.
- [Etapa 6.2. Compartilhar um grupo do IPAM usando o AWS RAM](#): esta etapa deve ser realizada pelo administrador do IPAM.

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).

Sent request to provision 10.0.0.0/20

Amazon VPC IP Address Manager > Pools > ipam-pool-07bdd12d7c94e4693

Pre-prod pool (ipam-pool-07bdd12d7c94e4693)

Pool summary

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

Pool details | Monitoring | IP space visualization | CIDRs | Allocations | Resources | Compliancy | **Resource sharing** | Tags

Resource sharing Info

Filter resource shares

1

Resource share ARN	Status	Created at
No shares This resource is not part of any resource share.		

Create resource share

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.

Specify resource share details

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

Resource share name

Name

Provide a descriptive name for the resource share.

Resources - optional

Choose the resources to add to the resource share.

Select resource type

< 1 > ⚙

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

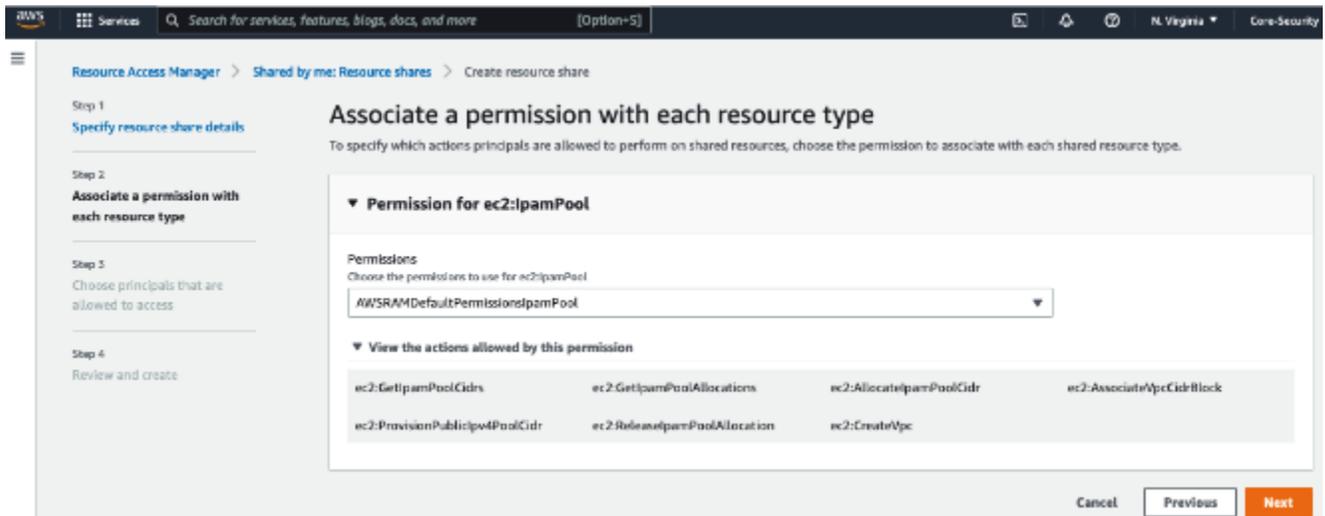
Selected resources (1)

Deselect

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

9. 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.

Grant access to principals

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

Principals - *optional*

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

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

Principals

You can add multiple principals of different types.

Organizational unit (OU) ▼

ou-fssg-q5brfv9c

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

Add

▼ Selected principals (0)

Deselect

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

<input type="checkbox"/>	Principal ID	Type
--------------------------	--------------	------

No selected principals.

Cancel

Previous

Next

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. Usando a conta de membro, abra o console da VPC em <https://console.aws.amazon.com/vpc/> como a conta de membro que você usará como 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.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

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

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

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

Example VPC

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

IPv4 IPAM pool

ipam-pool-0c4e32cfe1a0bb88f
us-west-1

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

Netmask

/24 (allowed maximum) 256 IPs

- Para fins de demonstração, em Tags, não adicione nenhuma tag adicional no momento. Ao criar o grupo de pré-produção (em [5. Criar um grupo de desenvolvimento de 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.
- Escolha Criar VPC.
- 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.

⊗ **There was an error creating your VPC**✕

The resource is missing one or more of the resource tags required by the IPAM pool.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

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

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

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

Example VPC

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

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

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

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

Add new tag

You can add 48 more tags.

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

✔ You successfully created vpc-07701f4fcc6549b8d / Example VPC

VPC > Your VPCs > vpc-07701f4fcc6549b8d

vpc-07701f4fcc6549b8d / Example VPC

Actions ▼

Details [Info](#)

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

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 AWS 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 obter 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.

Delete IPAM DemoIPAM (ipam-080d0c4b98089b437) ✕

Deleting this IPAM will permanently remove it. To confirm deletion, type *delete* in the field.

Cascade delete
Enables you to quickly delete an IPAM, private scopes, pools in private scopes, and any allocations in the pools in private scopes. You cannot delete the IPAM with this option if there is a pool in your public scope. No VPC resources will be deleted.

Cancel Delete

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](#). Com o uso de cada uma das contas de membro do AWS Organizations, faça login no IAM e exclua o perfil vinculado ao serviço AWSServiceRoleForIPAM em cada conta de membro.
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 ter 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 111111111111
```

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 via Internet pública. O escopo privado é destinado a endereços IP que não serão acessados via 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 `--local` 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 `None` será adotado. 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 ter 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.

ℹ 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, das 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 **10.2.1.155/32** atualmente?

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 **10.2.1.0/24** atualmente?

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-0864c82a42f5bffd",
      "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 **54.0.0.9/32** atualmente?

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) possibilita anunciar os endereços IP que você trouxe para a AWS com seu próprio ASN público, em vez de utilizar o 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. Você pode usar a chave privada que criou quando trouxe o intervalo CIDR de endereços IP para a AWS ou criar uma nova chave privada conforme descrito em [Criar uma chave privada e gerar um certificado X.509](#) no Guia do usuário do EC2.
- Ao trazer um intervalo de endereços IP para a AWS com o [Tutorial: trazer seus endereços IP para o IPAM](#), você [cria um certificado X.509](#) e [carrega o certificado X.509 no registro RDAP em seu 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.

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. Sem o IPAM, você precisa integrar seus IPs públicos a cada região da AWS.

Important

- Antes de começar este tutorial, conclua as etapas em [Pré-requisitos de integração para seu intervalo de endereços BYOIP](#) no Guia do usuário do Amazon EC2 para instâncias Linux.

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.

- 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 o Console de Gerenciamento da AWS e a AWS CLI](#)
- [Traga seu próprio CIDR IPv4 público para o IPAM usando somente a AWS CLI](#)

Traga seu próprio CIDR IPv4 público para o IPAM usando o Console de Gerenciamento da AWS e a AWS CLI

Siga estas etapas para trazer um CIDR IPv4 ou IPv6 para o IPAM usando o Console de Gerenciamento da AWS e a AWS CLI.

Important

- Antes de começar este tutorial, conclua as etapas em [Pré-requisitos de integração para seu intervalo de endereços BYOIP](#) no Guia do usuário do Amazon EC2 para instâncias Linux.

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.

- 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

- Você não pode provisionar ou anunciar intervalos de endereços BYOIP em Zonas locais no momento.
- 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: Compartilhar o grupo regional](#)
- [Etapa 5: criar um grupo IPv4 público](#)
- [Etapa 6: provisionar o CIDR IPv4 público para seu grupo IPv4 público](#)
- [Etapa 7: criar um endereço IP elástico do grupo IPv4 público](#)
- [Etapa 8: associar um endereço IP elástico a uma instância do EC2](#)

- [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 [Como usar um perfil do IAM na AWS CLI](#) no Guia do usuário do AWS Identity and Access Management.

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 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.

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 do IP público, escolha uma das opções a seguir:
 - BYOIP: você está trazendo seu próprio intervalo de endereços IPv4 ou IPv6 (BYOIP) para esse grupo.
 - Pertencente à Amazon: você deseja que a Amazon provisione um intervalo de endereços IPv6 para esse grupo.
11. Execute um destes procedimentos:

- Se tiver escolhido BYOIP na etapa anterior, em CIDRs a provisionar, escolha o CIDR que será provisionado para o grupo. 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. Você deve incluir o CIDR, a mensagem BYOIP e a assinatura do certificado na solicitação para que possamos verificar se o espaço público lhe pertence. Para obter uma lista de pré-requisitos para BYOIP, inclusive como obter essa mensagem BYOIP e assinatura de certificado, consulte [Traga seu próprio CIDR IPv4 público para o IPAM usando o Console de Gerenciamento da AWS e a AWS CLI](#).

 Important

Pode levar até uma semana para que o CIDR do BYOIP seja provisionado.

- Se tiver escolhido Pertencente à Amazon, em Comprimento da máscara de rede, escolha um comprimento de máscara de rede entre /40 e /52. O padrão é/52.
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. Observe que pode levar até uma semana para que o CIDR do BYOIP seja provisionado.

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 `Local` 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) 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 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. 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. Observe que, ao provisionar um CIDR 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.
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. Compartilhar o grupo regional

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

4.1. 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.

4.2. 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` 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`.

Etapa 5: criar um grupo IPv4 público

Criar um grupo IPv4 público é uma etapa necessária para trazer um endereço IPv4 público para a AWS para ser gerenciado com o IPAM. Essa etapa deve ser executada pela conta de membro que provisionará um endereço IP elástico.

Important

- 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. Os 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 `Local` 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 6: provisionar o CIDR IPv4 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 `Local` 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 prefixo IPv4 menos específico que você pode incluir 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.

Important

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 7: criar um endereço IP elástico do grupo IPv4 público

Siga as etapas em [Allocate an Elastic IP address](#) (Alocar um endereço IP elástico) no Guia do usuário do Amazon EC2 para instâncias do Linux para criar 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 **Local** 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`.

Etapa 8: associar um endereço IP elástico a uma instância do EC2

Conclua as etapas em [Associate an Elastic IP address with an instance or network interface](#) (Associar um endereço IP elástico a uma instância ou interface de rede) no Guia do usuário do Amazon EC2 para instâncias do Linux para associar o EIP a uma instância do EC2. Ao abrir o EC2 no Console de Gerenciamento da AWS, a região da AWS em que você associa a EIP deve corresponder à opção Local escolhida ao criar o grupo que será usado para o CIDR de BYOIP. Neste tutorial, esse é o seu grupo regional.

Esta etapa deve ser executada pela conta de membro. Se você estiver usando a AWS CLI, use a opção `--profile member-account`.

Etapa 9: 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.

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 10: 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 [Disassociate an Elastic IP address](#) (Dissociar um endereço IP elástico) no Guia do usuário do Amazon EC2 para instâncias do Linux para desassociar o 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 Local 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 [Release an Elastic IP address](#) (Liberar um endereço IP elástico) no Guia do usuário do Amazon EC2 para instâncias do Linux 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 Local escolhida ao criar o grupo que será usado para o CIDR de BYOIP.

Etapa 4: 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 a seguir para liberar o último endereço IP no CIDR do grupo IPv4 público. Insira o endereço IP com uma máscara de rede de /32.

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

Na saída, você verá o CIDR desprovisionado.

```
{
  "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
  "DeprovisionedAddresses": [
    "130.137.245.255"
  ]
}
```

Important

Você deve executar novamente esse comando para cada endereço IP no intervalo do CIDR. Se o seu CIDR for um /24, você terá que executar esse comando para desprovisionar cada um dos 256 endereços IP no CIDR /24.

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 5: 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 `Local` 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).

Etapa 6: excluir qualquer compartilhamento do RAM e desabilite 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 7: 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 8: 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.

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.

Important

- Você não pode provisionar ou anunciar intervalos de endereços BYOIP em Zonas locais no momento.
- 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 do IPAM de nível superior com um grupo regional dentro dele, e vamos alocar espaço para um recurso (um endereço IP elástico) 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.

Ao escolher IPv6, você verá uma opção de alternância que permite controlar se a AWS pode anunciar publicamente os CIDRs nesse grupo. Deixe essa opção habilitada.

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. Confirme se a opção Allow CIDRs in this pool to be publicly advertisable (Permitir que os CIDRs neste grupo sejam anunciados publicamente) está selecionada.
10. 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.

11. Em Fonte de IP público, a opção BYOIP é selecionada por padrão.
12. 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. Você deve incluir o CIDR, a mensagem BYOIP e a assinatura do certificado na solicitação para que possamos verificar se o espaço público lhe pertence. Para obter uma lista de pré-requisitos para BYOIP, inclusive como obter essa mensagem BYOIP e assinatura de certificado, consulte [Traga](#)

[seu próprio CIDR IPv4 público para o IPAM usando o Console de Gerenciamento da AWS e a AWS CLI.](#)

 Important

Pode levar até uma semana para que o CIDR do BYOIP seja provisionado.

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. Observe que pode levar até uma semana para que o CIDR do BYOIP seja provisionado.

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](#).

- 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.

- 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).
- 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.
- 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).

4.1. 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.

4.2. 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` 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`.

Etapa 4: criar uma VPC

Conclua as etapas em [Criar 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 `Local` 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 em [Excluir uma VPC](#) no Guia do usuário da Amazon VPC para excluir uma 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 Local 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 de gerenciamento, 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 os compartilhamentos 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.

Traga seu próprio CIDR IPv4 público para o IPAM usando somente a AWS CLI

Siga estas etapas para trazer um CIDR IPv4 ou IPv6 para o IPAM usando apenas a AWS CLI.

Important

- Antes de começar este tutorial, conclua as etapas em [Pré-requisitos de integração para seu intervalo de endereços BYOIP](#) no Guia do usuário do Amazon EC2 para instâncias Linux.

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.

- 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

- Você não pode provisionar ou anunciar intervalos de endereços BYOIP em Zonas locais no momento.
- 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: Compartilhar o grupo regional](#)
- [Etapa 8: criar um grupo IPv4 público](#)
- [Etapa 9: provisionar o CIDR IPv4 público para seu grupo IPv4 público](#)
- [Etapa 10: criar um endereço IP elástico do grupo IPv4 público](#)
- [Etapa 11: anunciar o CIDR](#)
- [Etapa 12: 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 [Como usar um perfil do IAM na AWS CLI](#) no Guia do usuário do AWS Identity and Access Management.

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. Você deve incluir o CIDR, a mensagem BYOIP e a assinatura do certificado na solicitação para que possamos verificar se o espaço público lhe pertence. Para obter uma lista de pré-requisitos para BYOIP, inclusive como obter essa mensagem BYOIP e assinatura de certificado, consulte [Traga seu próprio CIDR IPv4 público para o IPAM usando somente a AWS CLI](#).

Esta etapa deve ser realizada pela conta do IPAM.

Important

Você só precisa adicionar `--cidr-authorization-context` ao provisionar o CIDR de BYOIP para o grupo de nível superior. Para o grupo regional dentro do grupo de nível superior, você pode omitir a opção `--cidr-authorization-context`. 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. Execute o comando a seguir para provisionar o CIDR.

```

aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --cidr-authorization-
context Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrxnGM~cvGx~KCIsmAu0P7EN07VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRY0dRaNx8yt-uoZWzxc2yIhWngy-

```

```
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXE1T5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-  
oS9AZ1afBbrFxrjFWRCTJhc7Cg3ASbR0-VWNci-  
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --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

Pode levar até uma semana para que o CIDR do BYOIP seja provisionado.

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 do grupo de nível superior. `--locale` é necessária no grupo e deve ser uma das regiões operacionais que você configurou ao criar o 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.

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. Observe que, ao provisionar um CIDR 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.

Esta etapa deve ser realizadas 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. Compartilhar o grupo regional

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

4.1. 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.

4.2. 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` 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`.

Etapa 8: criar um grupo IPv4 público

Criar um grupo IPv4 público é uma etapa necessária para trazer um endereço IPv4 público para a AWS para ser gerenciado com o IPAM. Normalmente, esta etapa seria realizada por uma conta da AWS diferente que deseja provisionar um endereço IP elástico.

Esta etapa deve ser realizadas pela conta de membro.

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 9: provisionar o CIDR IPv4 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.

Esta etapa deve ser realizadas 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 10: 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"
    }
  ]
}
```

Etapa 11: 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 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 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 12: 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 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 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": []
  }
]
}

```

5. Libere o último endereço IP no CIDR do grupo IPv4 público. Insira o endereço IP com uma máscara de rede de /32. Você deve executar novamente esse comando para cada endereço IP no intervalo do CIDR. Se o seu CIDR for um /24, você terá que executar esse comando para desprovisionar cada um dos 256 endereços IP no CIDR /24. 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 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.255/32 --profile member-account
```

Na saída, você verá o CIDR desprovisionado.

```

{
  "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
  "DeprovisionedAddresses": [
    "130.137.245.255"
  ]
}

```

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 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": []
    }
  ]
}
```

7. 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 corresponder à opção `--locale` inserida ao criar o grupo 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-0d8f3646b61ca5987 --profile ipam-account
```

A saída mostra a alocação no IPAM.

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

8. 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"
  }
}
```

9. Exclua os compartimentos 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 compartimentos 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`.

10. 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"  
  }  
}
```

11. 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"
  }
}
```

12. 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"
  }
}
```

13. 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"  
  }  
],  
}
```

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.

Important

- Você não pode provisionar ou anunciar intervalos de endereços BYOIP em Zonas locais no momento.
- 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](#)
- [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 [Como usar um perfil do IAM na AWS CLI](#) no Guia do usuário do AWS Identity and Access Management.

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.

```
{  
  "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 de 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. Você deve incluir o CIDR, a mensagem BYOIP e a assinatura do certificado na solicitação para que possamos verificar se o espaço público lhe pertence. Para obter uma lista de pré-requisitos para BYOIP, inclusive como obter essa mensagem BYOIP e assinatura de certificado, consulte [Traga seu próprio CIDR IPv4 público para o IPAM usando somente a AWS CLI](#).

Você só precisa adicionar `--cidr-authorization-context` ao provisionar o CIDR de BYOIP para o grupo de nível superior. Para o grupo regional dentro do grupo de nível superior, você pode omitir a opção `--cidr-authorization-context`.

Esta etapa deve ser realizadas pela conta do IPAM.

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-  
pool1-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --cidr-authorization-  
context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|  
SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-  
CR7HqMwzcgdS9R1pBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxFnp7RAJDvF1mBwxmSgH~C  
Vp6L0N3y00Xmp4JENB9uM7sM1u6oeoutGyyhXFeYPz1GSRdcdfKNKaimvPCqVsxGN5AwSi1KQ8byNqoa~G3dvs8ueSa  
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --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

Pode levar até uma semana para que o CIDR do BYOIP seja provisionado.

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 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-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).

4.1. 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.

4.2. 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` 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`.

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 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`.

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 realizada 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"  
      }  
    ]  
  }  
}
```

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 ter mais informações, consulte [Monitorar o uso do CIDR por recurso](#).

Important

- 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 [Como usar um perfil do IAM na AWS CLI](#) no Guia do usuário do AWS Identity and Access Management.

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 trazer 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`

ℹ Note

Você pode usar o AWS Management Console 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. Libere o último endereço IP no CIDR do grupo IPv4 público. Insira o endereço IP com uma máscara de rede de /32. Você deve executar novamente esse comando para cada endereço IP no intervalo do CIDR. Se o seu CIDR for um /24, você terá que executar esse comando para desprovisionar cada um dos 256 endereços IP no CIDR /24. 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 130.137.249.255/32
```

Na saída, você verá o CIDR desprovisionado.

```
{
  "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
  "DeprovisionedAddresses": [
    "130.137.249.255"
  ]
}
```

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 o escopo público e um intervalo IPv6 CIDR, criando a VPC com a opção de bloco IPv6 CIDR fornecida 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.

Identificar e acessar o gerenciamento no IPAM

O AWS usa credenciais de segurança para identificar você e conceder acesso aos seus recursos do AWS. Você pode usar recursos do AWS Identity and Access Management (IAM) para permitir que outros usuários, serviços e aplicações usem seus recursos do AWS, totalmente ou de maneira limitada, sem compartilhar suas 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 acesso da VPC, consulte [Gerenciamento de identidade e acesso da 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

Funções vinculadas ao serviço no AWS Identity and Access Management (IAM) habilitam os serviços da AWS a chamar outros serviços da AWS em seu nome. Para obter mais informações sobre funções vinculadas a serviços, consulte [Usar funções vinculadas a serviços](#) no Guia do usuário do IAM.

Atualmente, há apenas uma função vinculada ao serviço do IPAM: AWSServiceRoleForIPAM.

Permissões concedidas à função vinculada 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](#).

Há uma política confiável do IAM, também anexada à [função vinculada ao serviço](#), que permite que o serviço da `ipam.amazonaws.com` assuma a função vinculada 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 uma política do IAM, consulte [Edição de políticas do IAM](#) no Guia do usuário do IAM.

Editar a função vinculada ao serviço

Não é possível editar a função vinculada 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 a função vinculada ao serviço por meio da 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.

O exemplo a seguir mostra os detalhes da política gerenciada que foi criada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAMDiscoveryDescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
```

```

        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*"
},
{
    "Sid": "CloudWatchMetricsPublishActions",
    "Effect": "Allow",
    "Action": "cloudwatch:PutMetricData",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": "AWS/IPAM"
        }
    }
}
]
}

```

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 seu [namespace 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 ter 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	Ação incorporada à política gerenciada AWSIPAMSe	13 de novembro de 2023

Alteração	Descrição	Data
	erviceRolePolicy (ec2:GetIpamDiscoveredPublicAddresses) para conceder ao IPAM a capacidade de adquirir endereços IP públicos durante a identificação de recursos.	
AWSIPAMServiceRolePolicy	Inclusão de ações na política gerenciada AWSIPAMServiceRolePolicy (ec2:DescribeAccountAttributes , ec2:DescribeNetworkInterfaces , ec2:DescribeSecurityGroups , ec2:DescribeSecurityGroupRules , ec2:DescribeVpnConnections , globalaccelerator:ListAccelerators , e globalaccelerator:ListByoipCidrs) para habilitar o IPAM a obter endereços IP públicos durante a identificação de recursos.	1.º 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 (RAM) e Amazon CloudWatch.

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

```

```

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

```

```
}  
  ]  
}
```

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
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.
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
Administradores do IPAM por organização	1	Não

Nome	Padrão	Ajustável
IPAMs por região	1	Não
Profundidade do grupo (o número de grupos dentro dos grupos)	10	Sim
Grupos por escopo	50	Sim
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.
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.

Preços do IPAM

Esta seção descreve como visualizar as informações relacionadas a preços e seus custos atuais de IPAM.

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 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, você selecionar USE1-IPAddressManager-IP-Hours(Hrs), verá o número de horas de IP ativo cobradas pelo IPAM na região us-east-1 e o custo. Caso o uso em horas for 18, isso significa que você poderá ter 1 endereço IP ativo por 18 horas, 3 endereços IP ativos por 6 horas ou qualquer combinação que resulte em 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

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

- [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.

Histórico de documentos do IPAM

A tabela a seguir descreve todas as versões do IPAM.

Atributo	Descrição	Data de lançamento
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 visualizar 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: atualização de uma política existente	A política AWSIPAMServiceRolePolicy existente foi atualizada.	17 de novembro de 2023
Atualizações de política gerenciada pela AWS: atualização	A política AWSIPAMServiceRolePolicy existente foi atualizada.	1.º de novembro de 2023

Atributo	Descrição	Data de lançamento
Atualização de uma política existente		
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 ter mais informações, consulte Criar grupos de IPv6 .	25 de janeiro de 2023
Lançamento inicial	Esta versão apresenta o Amazon VPC IP Address Manager.	2 de dezembro de 2021