Manajer Alamat IP

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: Manajer Alamat IP

Table of Contents

Apa itu IPAM? 1
Cara kerja IPAM 2
Memulai dengan IPAM 4
Akses IPAM 4
Konfigurasikan izin untuk IPAM Anda 5
Integrasikan IPAM dengan akun di Organisasi AWS 5
Integrasikan IPAM dengan akun di luar organisasi 8
Gunakan IPAM dengan satu akun 11
Buat IPAM 11
Merencanakan penyediaan alamat IP 14
Contoh rencana kolam IPAM 15
Buat kolam IPv4 17
Buat kolam IPv6 27
Alokasikan CIDR 34
Buat VPC yang menggunakan CIDR kolam IPAM 35
Secara manual mengalokasikan CIDR ke pool untuk memesan ruang alamat IP 35
Mengelola ruang alamat IP di IPAM 37
Terapkan penggunaan IPAM untuk pembuatan VPC 37
Terapkan IPAM saat membuat VPC 38
Menegakkan kolam IPAM saat membuat VPC 38
Terapkan IPAM untuk semua kecuali daftar OU yang diberikan 39
Membagikan kumpulan IPAM menggunakanAWS RAM 40
Menyediakan CIDR ke kolam 42
Deprovision CIDR dari kolam 44
Mengedit kolam yang lebih baik. 45
Menghapus kolam kolam kolam kolam kolam kolam renang 46
Bekerja dengan penemuan sumber daya 47
Buat penemuan sumber daya 48
Lihat detail penemuan sumber daya 49
Bagikan penemuan sumber daya 51
Kaitkan penemuan sumber daya dengan IPAM 53
Putuskan penemuan sumber daya 54
Hapus penemuan sumber daya 55
Buat cakupan tambahan 56

Memindahkan CIDR VPC antar cakupan 57
Ubah status pemantauan CIDR VPC 59
Menghapus cakupan 60
Rilis alokasi yang berbeda. 61
Memodifikasi IPAM 63
Ubah tingkat IPAM 63
Ubah Wilayah operasi IPAM 65
Menghapus IPAM 65
Melacak penggunaan alamat IP di IPAM 68
Memantau penggunaan CIDR dengan dasbor IPAM 68
Pantau penggunaan CIDR berdasarkan sumber daya 71
Pantau IPAM dengan Amazon CloudWatch 75
Metrik kolam dan cakupan IPAM 75
Metrik pemanfaatan sumber daya 77
Lihat riwayat alamat IP 82
Lihat wawasan IP publik 86
Tutorial 91
Buat IPAM dan kolam menggunakan konsol 91
Prasyarat 92
Bagaimana AWS Organizations terintegrasi dengan IPAM 92
Langkah 1: Delegasikan administrator IPAM 94
Langkah 2: Buat IPAM 95
Langkah 3: Buat kolam IPAM tingkat atas 98
Langkah 4: Buat kolam IPAM Regional 103
Langkah 5: Buat kumpulan pengembangan pra-produksi 107
Langkah 6: Bagikan kolam IPAM 111
Langkah 7: Buat VPC dengan CIDR yang dialokasikan dari kolam IPAM 116
Langkah 8: Pembersihan 120
Buat IPAM dan pool menggunakanAWS CLI 122
Langkah 1: Aktifkan IPAM di organisasi 123
Langkah 2: Buat IPAM 123
Langkah 3: Buat kolam alamat IPv4 125
Langkah 4: Menyediakan CIDR pada pool tingkat atas 127
Langkah 5. Buat kolam Regional dengan CIDR yang bersumber dari kolam renang tingkat atas 128
Langkah 6: Menyediakan CIDR ke kolam Regional 130

Langkah 7. Buat berbagi RAM untuk mengaktifkan penetapan IP di seluruh akun 132
Langkah 8. Buat VPC 132
Langkah 9. Pembersihan 133
Lihat riwayat alamat IP menggunakanAWS CLI 134
Gambaran Umum 134
Skenario 135
Bawa ASN Anda ke IPAM 143
Prasyarat orientasi untuk ASN Anda 144
Langkah-langkah tutorial 144
Bawa alamat IP Anda ke IPAM 148
AWS konsol dan CLI 150
AWS Hanya CLI 175
Transfer BYOIP IPv4 CIDR ke IPAM 219
Langkah 1: Buat profil AWS CLI bernama dan peran IAM 220
Langkah 2: Dapatkan ID ruang lingkup publik IPAM Anda 220
Langkah 3: Buat kolam IPAM 221
Langkah 4: Bagikan kolam IPAM menggunakan AWS RAM 223
Langkah 5: Transfer CIDR BYOIP IPV4 yang ada ke IPAM 226
Langkah 6: Lihat CIDR di IPAM 228
Langkah 7: Pembersihan 229
Rencanakan ruang alamat IP VPC untuk alokasi IP subnet 232
Langkah 1: Buat VPC 233
Langkah 2: Buat kolam perencanaan sumber daya 234
Langkah 3: Buat subnet pool 235
Langkah 4: Buat subnet 236
Langkah 5: Pembersihan 237
Identity and access management di IPAM 238
Peran tertaut layanan untuk IPAM 238
Izin yang diberikan kepada peran yang ditautkan dengan layanan 238
Membuat peran tertaut layanan 239
Mengedit peran tertaut layanan 240
Hapus peran tertaut layanan 240
Kebijakan terkelola untuk IPAM 241
Pembaruan kebijakan AWS terkelola 242
Contoh kebijakan 244
Quotas 247

Harga 249
Lihat informasi harga 249
Lihat biaya dan penggunaan Anda saat ini AWS Cost Explorer 249
Informasi terkait 250
Riwayat dokumen 251
..... ccliii

Apa itu IPAM?

Amazon VPC IP Address Manager (IPAM) adalah fitur VPC yang memudahkan Anda merencanakan, melacak, dan memantau alamat IP untukAWS beban kerja Anda. Anda dapat menggunakan alur kerja otomatis IPAM untuk mengelola alamat IP dengan lebih efisien.

Anda dapat melakukan hal berikut:

- Mengatur ruang alamat IP ke domain routing dan keamanan
- Pantau ruang alamat IP yang digunakan dan pantau sumber daya yang menggunakan ruang sesuai aturan bisnis
- Melihat riwayat penetapan alamat IP di organisasi Anda
- Secara otomatis mengalokasikan CIDR ke VPC menggunakan aturan bisnis tertentu
- Memecahkan masalah konektivitas jaringan
- Memungkinkan berbagi lintas wilayah dan berbagi lintas akun dari alamat Bawa Anda sendiri (BYOIP)
- Menyediakan blok CIDR IPv6 bersebelahan yang disediakan Amazon ke kolam untuk pembuatan VPC

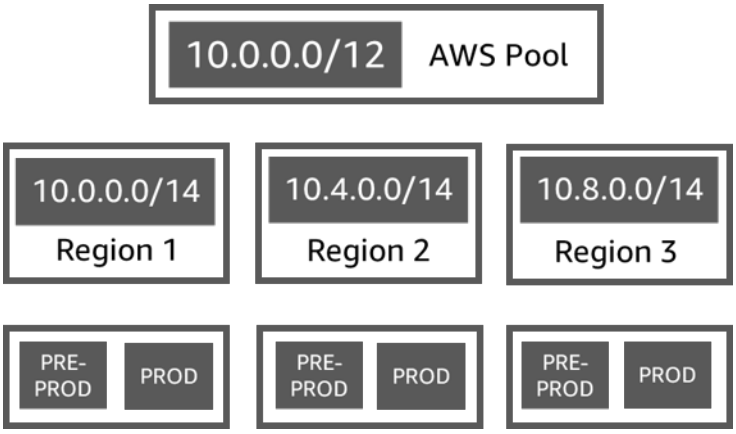
Panduan ini terdiri dari bagian berikut:

- Cara kerja IPAM: Konsep dan terminologi IPAM.
- Memulai dengan IPAM: Langkah-langkah untuk mengaktifkan manajemen alamat IP di seluruh perusahaan denganAWS Organizations, membuat IPAM, dan merencanakan penggunaan alamat IP.
- Mengelola ruang alamat IP di IPAM: Langkah-langkah untuk mengelola IPAM, cakupan, pool, dan alokasi Anda.
- Melacak penggunaan alamat IP di IPAM: Langkah-langkah untuk memantau dan melacak penggunaan alamat IP dengan IPAM.
- Tutorial untuk Manajer Alamat IP VPC Amazon: step-by-step Tutorial terperinci untuk membuat IPAM dan pool, mengalokasikan VPC CIDR, dan membawa CIDR alamat IP publik Anda sendiri ke IPAM.

Cara kerja IPAM

Topik ini menjelaskan beberapa konsep utama untuk membantu Anda memulai IPAM.

Diagram berikut menunjukkan hierarki kolam IPAM untuk beberapaAWS Wilayah dalam kolam IPAM tingkat atas. Setiap kolamAWS Regional memiliki dua kolam pengembangan IPAM di dalamnya, satu kolam untuk pra-produksi dan satu sumber daya produksi kolam. Untuk informasi selengkapnya tentang konsep IPAM, lihat deskripsi di bawah diagram.



Untuk menggunakan Amazon VPC IP Address Manager, Anda terlebih dahulu membuat IPAM.

Saat Anda membuat IPAM, Anda memilihAWS Wilayah mana untuk membuatnya. Ketika Anda membuat IPAM,AWS VPC IPAM secara otomatis membuat dua cakupan untuk IPAM. Cakupan, bersama dengan kumpulan dan alokasi, adalah komponen kunci IPAM Anda.

- Ruang lingkup adalah wadah tingkat tertinggi dalam IPAM. IPAM berisi dua cakupan default. Setiap ruang lingkup mewakili ruang IP untuk satu jaringan. Ruang lingkup pribadi ditujukan untuk semua ruang pribadi. Ruang lingkup publik ditujukan untuk semua ruang publik. Cakupan memungkinkan Anda untuk menggunakan kembali alamat IP di beberapa jaringan yang tidak terhubung tanpa menyebabkan tumpang tindih alamat IP atau konflik. Dalam lingkup, Anda membuat kolam IPAM.
- Kolam renang adalah kumpulan rentang alamat IP yang berdekatan (atau CIDR). Kumpulan IPAM memungkinkan Anda mengatur alamat IP sesuai dengan kebutuhan perutean dan keamanan Anda. Anda dapat memiliki beberapa kolam renang dalam kolam tingkat atas. Misalnya, jika Anda memiliki kebutuhan perutean dan keamanan terpisah untuk aplikasi pengembangan dan produksi, Anda dapat membuat kumpulan untuk masing-masing. Dalam kumpulan IPAM, Anda mengalokasikan CIDR keAWS sumber daya.

- Alokasi adalah tugas CIDR dari kumpulan IPAM ke sumber daya lain atau kumpulan IPAM. Saat Anda membuat VPC dan memilih kumpulan IPAM untuk CIDR VPC, CIDR dialokasikan dari CIDR yang disediakan ke kolam IPAM. Anda dapat memantau dan mengelola alokasi dengan IPAM.

IPAM dapat mengelola dan memantau CIDR IPv4 pribadi, CIDR IPv4/IPv6 publik yang Anda miliki, dan ruang IPv6 publik milik Amazon.

Untuk memulai dan membuat IPAM, lihatMemulai dengan IPAM.

Memulai dengan IPAM

Ikuti langkah-langkah dalam bagian ini untuk mulai menggunakan IPAM. Anda akan mulai dengan mengakses IPAM dan memutuskan apakah Anda ingin mendelegasikan akun IPAM. Pada akhir bagian ini, Anda akan membuat IPAM, membuat beberapa kumpulan alamat IP, dan mengalokasikan CIDR di kolam ke VPC.

Konten

- Akses IPAM
- Konfigurasikan izin untuk IPAM Anda
- Buat IPAM
- Merencanakan penyediaan alamat IP
- Alokasikan CIDR

Akses IPAM

Seperti halnyaAWS layanan lain, Anda dapat membuat, mengakses, dan mengelola IPAM Anda menggunakan metode berikut:

- AWSManagement Console: Menyediakan antarmuka web yang dapat Anda gunakan untuk membuat dan mengelola IPAM Anda. Lihat https://console.aws.amazon.com/ipam/.
- AWSCommand Line Interface (AWSCLI): MenyediakanAWS AWSCLI didukung di Windows, macOS, dan Linux. Untuk mendapatkanAWS CLI, lihat AWS Command Line Interface.
- AWSSDK: Menyediakan API khusus bahasa. AWSSDK menangani banyak Untuk informasi selengkapnya, lihat SDK AWS.
- Kueri: Menyediakan tindakan API Kueri yang Anda hubungi menggunakan permintaan HTTPS. Menggunakan API Kueri merupakan cara paling langsung untuk mengakses IPAM. Namun, Anda mengharuskan aplikasi Anda menangani detail tingkat rendah seperti membuat hash untuk menandatangani permintaan, dan menangani kesalahan. Untuk informasi selengkapnya, lihat Aksi Amazon EC2 API.

Panduan ini terutama berfokus pada penggunaanAWS Management Console untuk membuat, mengakses, dan mengelola IPAM Anda. Dalam setiap deskripsi tentang cara menyelesaikan proses

di konsol, kami menyertakan tautan ke dokumentasiAWS CLI yang menunjukkan kepada Anda bagaimana melakukan hal yang sama dengan menggunakanAWS CLI.

Jika Anda adalah pengguna IPAM pertama kali, tinjauCara kerja IPAM untuk mempelajari peran IPAM di Amazon VPC dan kemudian lanjutkan dengan instruksi di dalamnyaKonfigurasikan izin untuk IPAM Anda.

Konfigurasikan izin untuk IPAM Anda

Sebelum Anda mulai menggunakan IPAM, Anda harus memilih salah satu opsi di bagian ini untuk mengaktifkan IPAM untuk memantau CIDR yang terkait dengan sumber daya jaringan EC2 dan menyimpan metrik:

- Untuk mengaktifkan IPAM berintegrasi dengan AWS Organizations mengaktifkan layanan Amazon VPC IPAM mengelola dan memantau sumber daya jaringan yang dibuat oleh semua akun anggota AWS Organizations, lihat. Integrasikan IPAM dengan akun di Organisasi AWS
- Setelah Anda berintegrasi denganAWS Organizations, untuk mengintegrasikan IPAM dengan akun di luar organisasi Anda, lihatIntegrasikan IPAM dengan akun di luar organisasi.
- Untuk menggunakan satu AWS akun dengan IPAM dan mengaktifkan layanan Amazon VPC IPAM untuk mengelola dan memantau sumber daya jaringan yang Anda buat dengan satu akun, lihat. Gunakan IPAM dengan satu akun

Jika Anda tidak memilih salah satu opsi ini, Anda masih dapat membuat sumber daya IPAM, seperti kolam, tetapi Anda tidak akan melihat metrik di dasbor Anda dan Anda tidak akan dapat memantau status sumber daya.

Konten

- Integrasikan IPAM dengan akun di Organisasi AWS
- Integrasikan IPAM dengan akun di luar organisasi
- Gunakan IPAM dengan satu akun

Integrasikan IPAM dengan akun di Organisasi AWS

Secara opsional, Anda dapat mengikuti langkah-langkah di bagian ini untuk mengintegrasikan IPAM dengan AWS Organizations dan mendelegasikan akun anggota sebagai akun IPAM.

Akun IPAM bertanggung jawab untuk membuat IPAM dan menggunakannya untuk mengelola dan memantau penggunaan alamat IP.

Mengintegrasikan IPAM dengan AWS Organizations dan mendelegasikan admin IPAM memiliki manfaat sebagai berikut:

- Bagikan kumpulan IPAM Anda dengan organisasi Anda: Saat Anda mendelegasikan akun IPAM, IPAM memungkinkan akun anggota Organizations lain di AWS organisasi untuk mengalokasikan CIDR dari kumpulan IPAM yang dibagikan menggunakan Resource Access Manager (RAM). AWS Untuk informasi selengkapnya tentang menyiapkan organisasi, lihat Apa itu AWS Organizations? dalam Panduan Pengguna AWS Organizations.
- Pantau penggunaan alamat IP di organisasi Anda: Saat Anda mendelegasikan akun IPAM, Anda memberikan izin IPAM untuk memantau penggunaan IP di semua akun Anda. Akibatnya, IPAM secara otomatis mengimpor CIDR yang digunakan oleh VPC yang ada di seluruh akun anggota AWS Organizations lainnya ke IPAM.

Jika Anda tidak mendelegasikan akun anggota AWS Organizations sebagai akun IPAM, IPAM akan memantau sumber daya hanya di AWS akun yang Anda gunakan untuk membuat IPAM.

Important

- Anda harus mengaktifkan integrasi dengan AWS Organizations dengan menggunakan IPAM di konsol AWS manajemen atau perintah enable-ipam-organization-admin-account CLI AWS . Ini memastikan bahwa peran `AWSServiceRoleForIPAM` terkait layanan dibuat. Jika Anda mengaktifkan akses tepercaya dengan AWS Organizations menggunakan konsol AWS Organizations atau perintah register-delegated-administrator AWS CLI, peran `AWSServiceRoleForIPAM` terkait layanan tidak dibuat, dan Anda tidak dapat mengelola atau memantau sumber daya dalam organisasi Anda.

Note

Saat berintegrasi dengan AWS Organizations:

- IPAM menagih Anda untuk setiap alamat IP aktif yang dipantau di akun anggota organisasi Anda. Untuk informasi selengkapnya tentang harga, lihat harga IPAM.

- Anda harus memiliki akun di AWS Organizations dan akun manajemen yang disiapkan dengan satu atau beberapa akun anggota. Untuk informasi selengkapnya tentang jenis akun, lihat Terminologi dan konsep di Panduan Pengguna AWS Organizations. Untuk informasi selengkapnya tentang menyiapkan organisasi, lihat Memulai dengan AWS Organizations.
- Akun IPAM harus berupa akun anggota AWS Organizations. Anda tidak dapat menggunakan akun manajemen AWS Organizations sebagai akun IPAM.
- Akun IPAM harus menggunakan peran IAM yang memiliki kebijakan IAM yang melekat padanya yang memungkinkan tindakan. `iam:CreateServiceLinkedRole` Saat membuat IPAM, Anda secara otomatis membuat peran AWSServiceRoleForIPAM terkait layanan.
- Pengguna yang terkait dengan akun manajemen AWS Organizations harus menggunakan peran IAM yang memiliki tindakan kebijakan IAM berikut:
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`
  - `iam:CreateServiceLinkedRole`

  Untuk informasi selengkapnya tentang membuat peran IAM, lihat Membuat peran untuk mendelegasikan izin ke pengguna IAM di Panduan Pengguna IAM.
- Pengguna yang terkait dengan akun manajemen AWS Organizations dapat menggunakan peran IAM yang memiliki tindakan kebijakan IAM berikut yang dilampirkan untuk mencantumkan administrator delegasi AWS Orgs Anda saat ini: `organizations:ListDelegatedAdministrators`

AWS Management Console

Untuk memilih akun IPAM

1. Menggunakan akun manajemen AWS Organizations, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di Konsol AWS Manajemen, pilih AWS Wilayah tempat Anda ingin bekerja dengan IPAM.
3. Di panel navigasi, pilih Pengaturan organisasi.

4. Opsi Delegasi hanya tersedia jika Anda masuk ke konsol sebagai akun manajemen AWS Organisasi. Pilih Delegasikan.
5. Masukkan ID AWS akun untuk akun IPAM. Administrator IPAM harus merupakan akun anggota AWS Organizations.
6. Pilih Simpan perubahan.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

- Untuk mendelegasikan akun admin IPAM menggunakan AWS CLI, gunakan perintah berikut: -account enable-ipam-organization-admin

Saat Anda mendelegasikan akun anggota Organizations sebagai akun IPAM, IPAM secara otomatis membuat peran IAM terkait layanan di semua akun anggota di organisasi Anda. IPAM memantau penggunaan alamat IP di akun ini dengan mengasumsikan peran IAM terkait layanan di setiap akun anggota, menemukan sumber daya dan CIDR mereka, dan mengintegrasikannya dengan IPAM. Sumber daya dalam semua akun anggota akan dapat ditemukan oleh IPAM terlepas dari Unit Organisasi mereka. Jika ada akun anggota yang telah membuat VPC, misalnya, Anda akan melihat VPC dan CIDR-nya di bagian Sumber Daya konsol IPAM.

> **Important**
>
> Peran akun AWS Organizations manajemen yang mendelegasikan admin IPAM sekarang selesai. Untuk terus menggunakan IPAM, akun admin IPAM harus masuk ke Amazon VPC IPAM dan membuat IPAM.

Integrasikan IPAM dengan akun di luar organisasi

Bagian ini menjelaskan cara mengintegrasikan IPAM Anda denganAWS akun di luar organisasi Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus telah menyelesaikan langkah-langkah diIntegrasikan IPAM dengan akun di Organisasi AWS dan mendelegasikan akun IPAM.

Mengintegrasikan IPAM denganAWS akun di luar organisasi memungkinkan Anda untuk melakukan hal-hal berikut:

- Kelola alamat IP di luar organisasi Anda dari satu akun IPAM.
- Bagikan kolam IPAM dengan layanan pihak ketiga yang diselenggarakan olehAWS akun lain di lainAWS Organizations.

Setelah mengintegrasikan IPAM denganAWS akun di luar organisasi, Anda dapat membagikan kumpulan IPAM secara langsung dengan akun yang diinginkan dari organisasi lain.

Daftar Isi

- Pertimbangan dan batasan
- Gambaran umum proses

Pertimbangan dan batasan

Bagian ini berisi pertimbangan dan batasan untuk mengintegrasikan IPAM dengan akun di luar organisasi Anda:

- Saat Anda berbagi penemuan sumber daya dengan akun lain, satu-satunya data yang dipertukarkan adalah alamat IP dan data pemantauan status akun. Anda dapat melihat data ini sebelum berbagi menggunakan perintah get-ipam-discovered-resource-cidrs dan get-ipam-discovered-accountsCLI atau GetIpamDiscoveredResourceCidrsdan GetIpamDiscoveredAccountsAPI. Untuk penemuan sumber daya yang memantau sumber daya di seluruh organisasi, tidak ada data organisasi (seperti nama Unit Organisasi di organisasi Anda) yang dibagikan.
- Saat Anda membuat penemuan sumber daya, penemuan sumber daya memantau semua sumber daya yang terlihat di akun pemilik. Jika akun pemilik adalahAWS akun layanan pihak ketiga yang membuat sumber daya untuk beberapa pelanggan mereka sendiri, sumber daya tersebut akan ditemukan oleh penemuan sumber daya. Jika akunAWS layanan pihak ketiga membagikan penemuan sumber daya denganAWS akun pengguna akhir, pengguna akhir akan memiliki visibilitas ke sumber daya pelanggan lain dariAWS layanan pihak ketiga. Oleh karena itu,AWS layanan pihak ketiga harus berhati-hati dalam membuat dan berbagi penemuan sumber daya atau menggunakanAWS akun terpisah untuk setiap pelanggan.

Gambaran umum proses

Bagian ini menjelaskan cara mengintegrasikan IPAM Anda denganAWS akun di luar organisasi Anda. Ini mengacu pada topik yang dibahas di bagian lain dari panduan ini. Jaga agar halaman

ini tetap terlihat, dan buka topik yang ditautkan di bawah ini di jendela baru sehingga Anda dapat kembali ke halaman ini untuk mendapatkan panduan.

Ketika Anda mengintegrasikan IPAM denganAWS akun di luar organisasi Anda, ada 4AWS akun yang terlibat dalam proses:

- Pemilik Org Utama - AkunAWS Organizations manajemen untuk organisasi 1.
- Akun IPAM Org Primer - Akun administrator yang didelegasikan IPAM untuk organisasi 1.
- Pemilik Org Sekunder - AkunAWS Organizations manajemen untuk organisasi 2.
- Akun Admin Org Sekunder - Akun administrator yang didelegasikan IPAM untuk organisasi 2.

Langkah-langkah

1. Pemilik Org Utama mendelegasikan anggota organisasi mereka sebagai Akun IPAM Org Primer (lihatIntegrasikan IPAM dengan akun di Organisasi AWS).
2. Akun IPAM Org Primer membuat IPAM (lihatBuat IPAM).
3. Pemilik Org Sekunder mendelegasikan anggota organisasi mereka sebagai Akun Admin Org Sekunder (lihatIntegrasikan IPAM dengan akun di Organisasi AWS).
4. Akun Admin Org Sekunder membuat penemuan sumber daya dan membagikannya dengan Akun IPAM Org Primer menggunakanAWS RAM (lihatBuat penemuan sumber daya danBagikan penemuan sumber daya). Penemuan sumber daya harus dibuat dalam Wilayah asal yang sama dengan Organisasi Pratama IPAM.
5. Akun IPAM Org Utama menerima undangan berbagi sumber daya yang digunakanAWS RAM (lihat Menerima dan menolak undangan berbagi sumber daya di PanduanAWS RAM Pengguna).
6. Akun IPAM Org Primer mengaitkan penemuan sumber daya dengan IPAM mereka (lihatKaitkan penemuan sumber daya dengan IPAM).
7. Akun IPAM Org Primer sekarang dapat memantau dan/atau mengelola sumber daya IPAM yang dibuat oleh akun di Secondary Org.
8. (Opsional) Akun Primer Org IPAM berbagi kumpulan IPAM dengan akun anggota di Org Sekunder (lihatMembagikan kumpulan IPAM menggunakanAWS RAM).
9. (Opsional) Jika Akun IPAM Org Primer ingin berhenti menemukan sumber daya di Org Sekunder, itu dapat memisahkan penemuan sumber daya dari IPAM (lihatPutuskan penemuan sumber daya).
10. (Opsional) Jika Akun Admin Org Sekunder ingin berhenti berpartisipasi dalam IPAM Org Primer, mereka dapat membatalkan berbagi penemuan sumber daya bersama (lihat Memperbarui

pangsa sumber dayaAWS RAM di dalam PanduanAWS RAM Pengguna) atau menghapus penemuan sumber daya (lihatHapus penemuan sumber daya).

Gunakan IPAM dengan satu akun

Jika Anda memilih untuk tidakIntegrasikan IPAM dengan akun di Organisasi AWS melakukannya, Anda dapat menggunakan IPAM dengan satuAWS akun.

Saat Anda membuat IPAM di bagian berikutnya, peran terkait layanan secara otomatis dibuat untuk layanan Amazon VPC IPAM diAWS Identity and Access Management. IPAM menggunakan peran tertaut layanan untuk memantau dan menyimpan metrik untuk CIDR yang terkait dengan sumber daya jaringan EC2. Untuk informasi selengkapnya tentang peran tertaut layanan dan cara IPAM menggunakannya, lihatPeran tertaut layanan untuk IPAM.

> **Important**
>
> Jika Anda menggunakan IPAM dengan satuAWS akun, Anda harus memastikan bahwaAWS akun yang Anda gunakan untuk membuat IPAM menggunakan peran IAM dengan kebijakan yang melekat padanya yang memungkinkan`iam:CreateServiceLinkedRole` tindakan tersebut. Saat Anda membuat IPAM, Anda secara otomatis membuat peran AWSServiceRoleForIPAM terkait layanan. Untuk informasi selengkapnya tentang mengelola kebijakan IAM, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

Setelah satuAWS akun memiliki izin untuk membuat peran terkait layanan IPAM, bukaBuat IPAM.

Buat IPAM

Ikuti langkah-langkah di bagian ini untuk membuat IPAM Anda. Jika Anda telah mendelegasikan administrator IPAM, langkah-langkah ini harus diselesaikan oleh akun IPAM.

> **Important**
>
> Ketika Anda membuat IPAM, Anda akan diminta untuk mengizinkan IPAM untuk mereplikasi data dari akun sumber ke akun delegasi IPAM. Untuk mengintegrasikan IPAM dengan AWS Organizations, IPAM memerlukan izin Anda untuk mereplikasi rincian penggunaan sumber daya dan IP di seluruh akun (dari akun anggota ke akun anggota IPAM yang didelegasikan) dan di seluruh AWS Wilayah (dari Wilayah operasi ke Wilayah asal IPAM

Anda). Untuk pengguna IPAM akun tunggal, IPAM memerlukan izin Anda untuk mereplikasi detail penggunaan sumber daya dan IP di seluruh Wilayah operasi ke Wilayah asal IPAM Anda.

Saat Anda membuat IPAM, Anda memilih AWS Wilayah di mana IPAM diizinkan untuk mengelola CIDR alamat IP. AWSWilayah ini disebut Wilayah Operasi. IPAM menemukan dan memantau sumber daya hanya di AWS Wilayah yang Anda pilih sebagai Wilayah operasi. IPAM tidak menyimpan data apa pun di luar Wilayah operasi yang Anda pilih.

Hirarki contoh berikut menunjukkan bagaimana AWS Wilayah yang Anda tetapkan saat membuat IPAM akan memengaruhi Wilayah yang akan tersedia untuk kumpulan yang Anda buat nanti.

- IPAM beroperasi di AWS Wilayah 1 dan AWS Wilayah 2
  - Ruang lingkup pribadi
    - Kolam IPAM tingkat atas
      - Kolam IPAM Regional di AWSWilayah 2
        - Kolam pengembangan
          - Alokasi untuk VPC AWS di Wilayah 2

Anda hanya dapat membuat satu IPAM. Untuk informasi lebih lanjut tentang peningkatan kuota yang terkait dengan IPAM, lihat. Kuota untuk IPAM Anda

AWS Management Console

Untuk membuat IPAM

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di Konsol AWS Manajemen, pilih AWS Wilayah tempat Anda ingin membuat IPAM. Buat IPAM di Wilayah operasi utama Anda.
3. Pada halaman beranda layanan, pilih Buat IPAM.
4. Pilih Izinkan Pengelola Alamat IP VPC Amazon untuk mereplikasi data dari akun sumber ke akun delegasi IPAM. Jika Anda tidak memilih opsi ini, Anda tidak dapat membuat IPAM.
5. Pilih tingkat IPAM. Untuk informasi selengkapnya tentang fitur yang tersedia di setiap tingkatan dan biaya yang terkait dengan tingkatan, lihat tab IPAM di halaman harga Amazon VPC.

6. Di bawah Wilayah Operasi, pilih AWS Wilayah di mana IPAM ini dapat mengelola dan menemukan sumber daya. AWSWilayah di mana Anda membuat IPAM Anda dipilih sebagai salah satu Wilayah operasi secara default. Misalnya, jika Anda membuat IPAM ini di AWS Wilayah `us-east-1` tetapi Anda ingin membuat kumpulan IPAM Regional nanti yang menyediakan CIDR ke VPC, pilih di sini. `us-west-2` `us-west-2` Jika Anda lupa Wilayah operasi, Anda dapat kembali di lain waktu dan mengedit pengaturan IPAM Anda.

   > **Note**
   >
   > Jika Anda membuat IPAM di Tingkat Gratis, Anda dapat memilih beberapa Wilayah operasi untuk IPAM Anda, tetapi satu-satunya fitur IPAM yang akan tersedia di seluruh Wilayah operasi adalah wawasan IP Publik. Anda tidak dapat menggunakan fitur lain di Tingkat Gratis, seperti BYOIP, di seluruh Wilayah operasi IPAM. Anda hanya dapat menggunakannya di Wilayah asal IPAM. Untuk menggunakan semua fitur IPAM di seluruh Wilayah operasi, buat IPAM di Tingkat Lanjut.

7. Pilih Buat IPAM.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk membuat, memodifikasi, dan melihat detail yang terkait dengan IPAM Anda:

1. Buat IPAM: create-ipam
2. Lihat IPAM yang telah Anda buat: describe-ipams
3. Lihat cakupan yang dibuat secara otomatis: describe-ipam-scopes
4. Ubah IPAM yang ada: modify-ipam

Setelah Anda menyelesaikan langkah-langkah ini, IPAM telah melakukan hal berikut:

- Membuat IPAM Anda. Anda dapat melihat IPAM dan Wilayah operasi yang saat ini dipilih dengan memilih IPAM di panel navigasi kiri konsol.
- Dibuat satu ruang lingkup pribadi dan satu publik. Anda dapat melihat cakupan dengan memilih Lingkup di panel navigasi. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.

Merencanakan penyediaan alamat IP

Ikuti langkah-langkah di bagian ini untuk merencanakan penyediaan alamat IP dengan menggunakan kolam IPAM. Jika Anda telah mengonfigurasi akun IPAM, langkah-langkah ini harus diselesaikan oleh akun itu. Proses pembuatan kolam renang berbeda untuk kolam dalam lingkup publik dan pribadi. Bagian ini mencakup langkah-langkah untuk membuat kolam regional dalam lingkup pribadi. Untuk tutorial BYOIP dan BYOASN, lihat. Tutorial

Important

Untuk menggunakan kolam IPAM di seluruh AWS akun, Anda harus mengintegrasikan IPAM dengan AWS Organizations atau beberapa fitur mungkin tidak berfungsi dengan baik. Untuk informasi selengkapnya, lihat Integrasikan IPAM dengan akun di Organisasi AWS.

Di IPAM, pool adalah kumpulan rentang alamat IP yang berdekatan (atau CIDR). Pools memungkinkan Anda untuk mengatur alamat IP Anda sesuai dengan kebutuhan routing dan keamanan Anda. Anda dapat membuat kolam untuk AWS Wilayah di luar Wilayah IPAM Anda. Misalnya, jika Anda memiliki kebutuhan perutean dan keamanan terpisah untuk aplikasi pengembangan dan produksi, Anda dapat membuat kumpulan untuk masing-masing aplikasi.

Pada langkah pertama di bagian ini, Anda akan membuat kolam tingkat atas. Kemudian, Anda akan membuat kolam Regional di dalam kolam tingkat atas. Di dalam kolam Regional, Anda dapat membuat kolam tambahan sesuai kebutuhan, seperti kolam lingkungan produksi dan pengembangan. Secara default, Anda dapat membuat pool hingga kedalaman 10. Untuk informasi tentang kuota IPAM, lihat. Kuota untuk IPAM Anda

Note

Ketentuan ketentuan dan alokasi digunakan di seluruh panduan pengguna ini dan konsol IPAM. Ketentuan digunakan saat Anda menambahkan CIDR ke kolam IPAM. Alokasikan digunakan saat Anda mengaitkan CIDR dari kolam IPAM dengan sumber daya.

Berikut ini adalah contoh hierarki struktur kolam yang akan Anda buat dengan menyelesaikan langkah-langkah di bagian ini:

- IPAM beroperasi di AWS Wilayah 1 dan AWS Wilayah 2

- Ruang lingkup pribadi
  - Kolam renang tingkat atas
    - Kolam renang regional di AWS Wilayah 1
      - Kolam pengembangan
        - Alokasi untuk VPC

Struktur ini berfungsi sebagai contoh bagaimana Anda mungkin ingin menggunakan IPAM, tetapi Anda dapat menggunakan IPAM untuk memenuhi kebutuhan organisasi Anda. Untuk informasi selengkapnya tentang praktik terbaik, lihat Praktik Terbaik Manajer Alamat IP VPC Amazon.

Jika Anda membuat kolam IPAM tunggal, selesaikan langkah-langkahnya Buat kolam IPv4 tingkat atas dan kemudian lewati keAlokasikan CIDR.

Konten

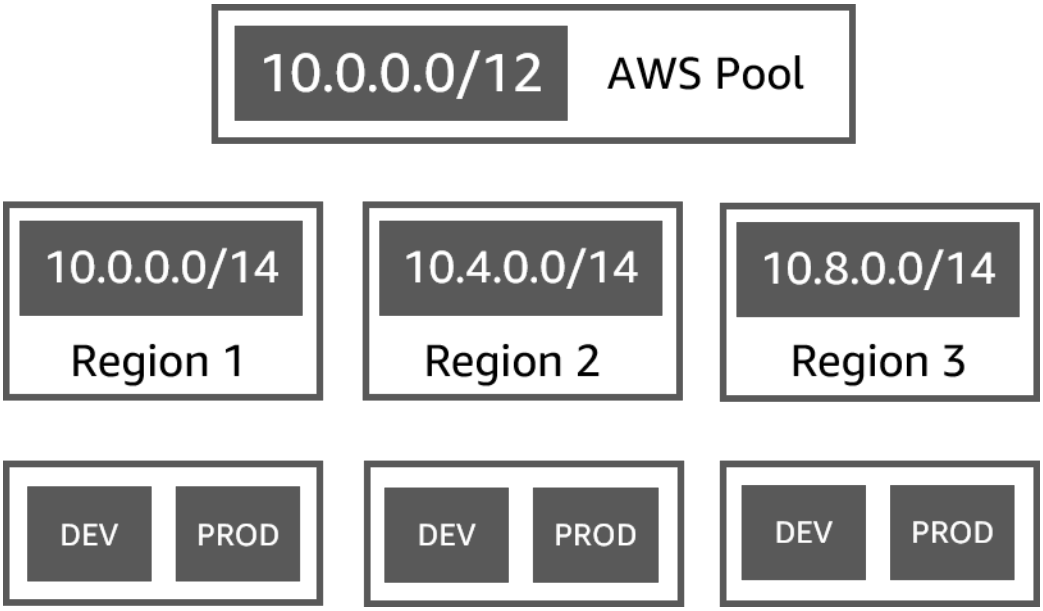
- Contoh rencana kolam IPAM
- Buat kolam IPv4
- Buat kolam IPv6

Contoh rencana kolam IPAM

Anda dapat menggunakan IPAM untuk memenuhi kebutuhan organisasi Anda. Bagian ini memberikan contoh bagaimana Anda dapat mengatur alamat IP Anda.

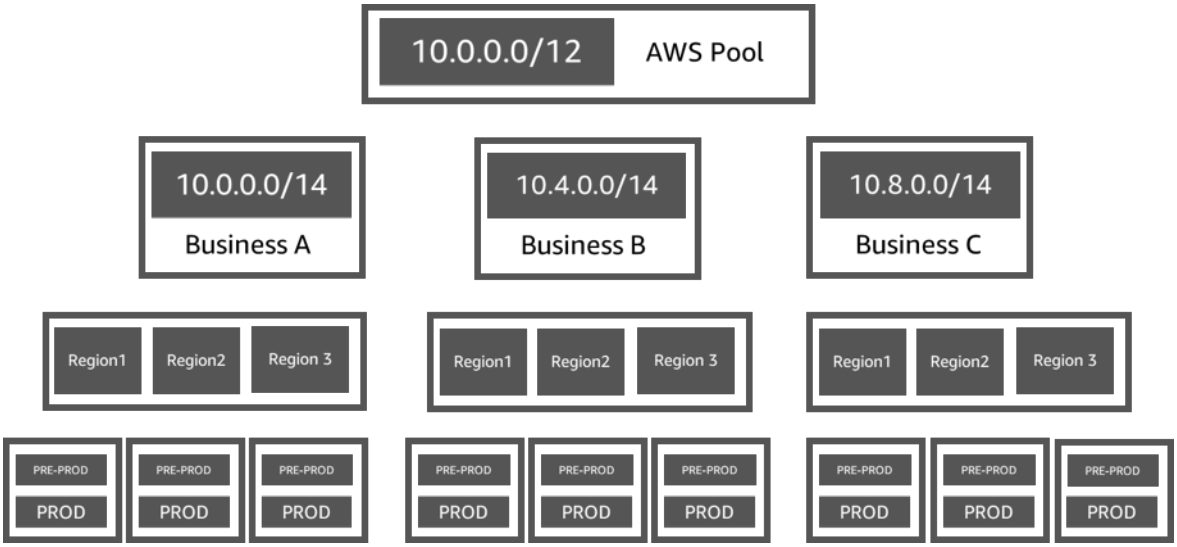
Kolam IPv4 di beberapa Wilayah AWS

Contoh berikut menunjukkan hierarki kolam IPAM untuk beberapa AWS Wilayah dalam kolam tingkat atas. Setiap kolam AWS Regional memiliki dua kolam pengembangan IPAM di dalamnya, satu kolam untuk sumber daya pengembangan dan satu kolam untuk sumber daya produksi.



IPv4 pool untuk berbagai lini bisnis

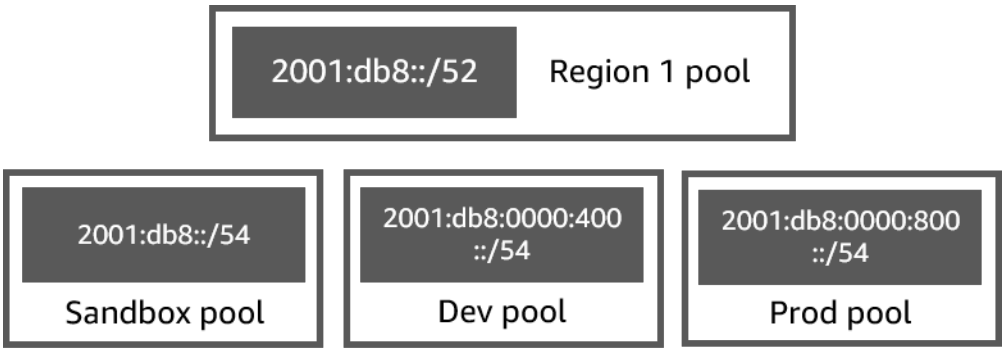
Contoh berikut menunjukkan hierarki kolam IPAM untuk beberapa lini bisnis dalam kolam tingkat atas. Setiap kolam untuk setiap lini bisnis berisi tiga kolam AWS Regional. Setiap kolam Regional memiliki dua kolam pengembangan IPAM di dalamnya, satu kolam untuk sumber daya pra-produksi dan satu kolam untuk sumber daya produksi.



Kolam IPv6 di suatu Wilayah AWS

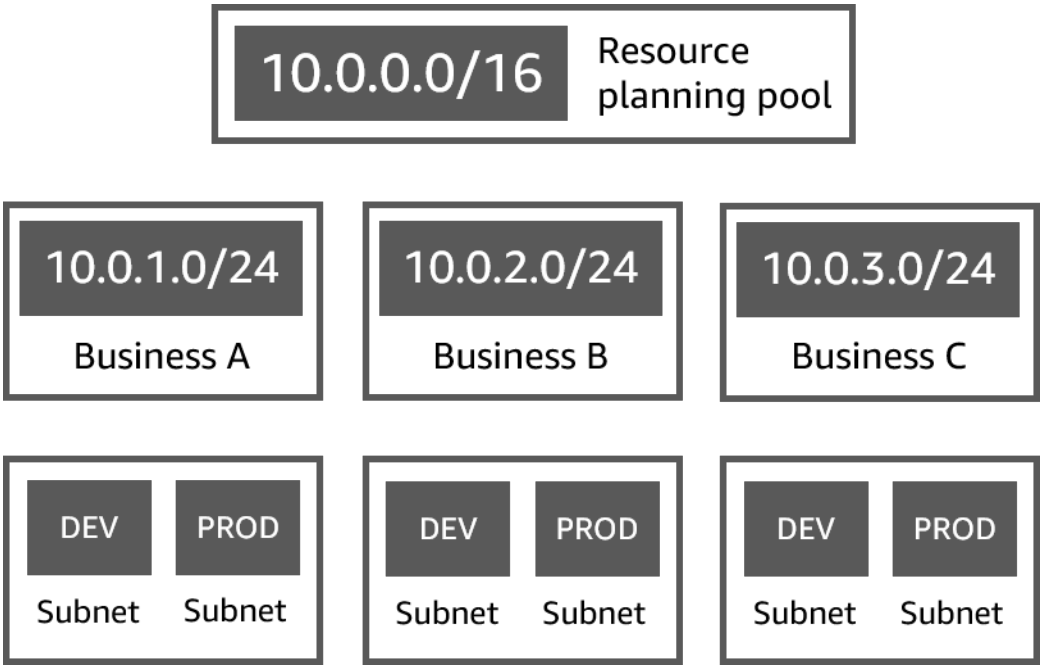
Contoh berikut menunjukkan hierarki kolam IPv6 IPAM untuk beberapa lini bisnis dalam kolam Regional. Setiap kolam Regional memiliki tiga kolam IPAM di dalamnya, satu kolam untuk sumber

daya kotak pasir, satu kolam untuk sumber daya pengembangan, dan satu kolam untuk sumber daya produksi.



Subnet pool untuk berbagai lini bisnis

Contoh berikut menunjukkan hierarki kumpulan perencanaan sumber daya untuk beberapa lini bisnis dan kumpulan subnet dev/ prod. Untuk informasi selengkapnya tentang perencanaan ruang alamat IP subnet menggunakan IPAM, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet



Buat kolam IPv4

Ikuti langkah-langkah dalam bagian ini untuk membuat hierarki

Contoh berikut menunjukkan hirarki struktur kolam yang dapat Anda buat dengan petunjuk dalam panduan ini. Pada bagian ini, Anda membuat hierarki kolam IPv4 IPAM:

- IPAM beroperasi diAWS Wilayah 1 danAWS Wilayah 2
  - Lingkup
    - Kolam di atas (10.0.0.0/8)
      - Kolam diAWS Wilayah 2 (10.0.0.0/16)
        - Pengembangan (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.0.0/25)

Dalam contoh sebelumnya, CIDR yang digunakan adalah contoh saja. Mereka menggambarkan bahwa setiap pool dalam pool tingkat atas disediakan dengan porsi CIDR tingkat atas.

Konten

- Buat kolam IPv4 tingkat atas
- Buat kolam IPv4 Regional
- Buat kolam IPv4 pengembangan

Buat kolam IPv4 tingkat atas

Ikuti langkah-langkah di bagian ini untuk membuat kolam IPAM tingkat atas IPv4. Saat Anda membuat kolam, Anda menyediakan CIDR untuk kolam yang akan digunakan. Anda kemudian menetapkan ruang itu ke alokasi. Alokasi adalah tugas CIDR dari kolam IPAM ke kolam IPAM lain atau ke sumber daya.

Contoh berikut menunjukkan hierarki struktur kolam yang dapat Anda buat dengan instruksi dalam panduan ini. Pada langkah ini, Anda membuat kolam IPAM tingkat atas:

- IPAM beroperasi di AWS Wilayah 1 dan AWS Wilayah 2
  - Ruang lingkup pribadi
    - Kolam renang tingkat atas (10.0.0.0/8)
      - Kolam regional di AWS Wilayah 1 (10.0.0.0/16)
        - Kumpulan pengembangan untuk VPC non-produksi (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.0.0/25)

Dalam contoh sebelumnya, CIDR yang digunakan adalah contoh saja. Mereka menggambarkan bahwa setiap kolam dalam kolam tingkat atas disediakan dengan sebagian CIDR tingkat atas.

Saat membuat kolam IPAM, Anda dapat mengonfigurasi aturan untuk alokasi yang dibuat dalam kolam IPAM.

Aturan alokasi memungkinkan Anda mengonfigurasi hal berikut:

- Apakah IPAM harus secara otomatis mengimpor CIDR ke kolam IPAM jika menemukannya dalam rentang CIDR kumpulan ini
- Panjang netmask yang diperlukan untuk alokasi di dalam kolam
- Tag yang diperlukan untuk sumber daya di dalam kolam
- Lokal yang diperlukan untuk sumber daya di dalam kolam. Lokal adalah AWS Wilayah di mana kolam IPAM tersedia untuk alokasi.

Aturan alokasi menentukan apakah sumber daya sesuai atau tidak sesuai. Untuk informasi tambahan tentang kepatuhan, lihatPantau penggunaan CIDR berdasarkan sumber daya.

> **Important**
>
> Ada aturan implisit tambahan yang tidak ditampilkan dalam aturan alokasi. Jika sumber daya berada di kolam IPAM yang merupakan sumber daya bersama di AWS Resource Access Manager (RAM), pemilik sumber daya harus dikonfigurasi sebagai prinsipal dalam AWS RAM. Untuk informasi selengkapnya tentang berbagi pool dengan RAM, lihatMembagikan kumpulan IPAM menggunakanAWS RAM.

Contoh berikut menunjukkan cara Anda menggunakan aturan alokasi untuk mengontrol akses ke kolam IPAM:

Example

Saat Anda membuat kumpulan berdasarkan kebutuhan perutean dan keamanan, Anda mungkin hanya ingin mengizinkan sumber daya tertentu untuk menggunakan kolam renang. Dalam kasus seperti itu, Anda dapat menetapkan aturan alokasi yang menyatakan bahwa sumber daya apa pun yang menginginkan CIDR dari kumpulan ini harus memiliki tag yang cocok dengan persyaratan tag aturan alokasi. Misalnya, Anda dapat menetapkan aturan alokasi yang menyatakan bahwa hanya VPC dengan tag prod yang bisa mendapatkan CIDR dari kumpulan IPAM. Anda juga dapat menetapkan aturan yang menyatakan bahwa CIDR yang dialokasikan dari kumpulan ini tidak boleh lebih besar dari /24. Dalam hal ini, sumber daya masih dapat dibuat menggunakan CIDR yang lebih

besar dari /24 dari kumpulan ini jika ruang tersedia, tetapi karena hal itu melanggar aturan alokasi pada kumpulan, IPAM menandai sumber daya ini sebagai tidak sesuai.

> **Important**
>
> Topik ini mencakup cara membuat kolam IPv4 tingkat atas dengan rentang alamat IP yang disediakan oleh. AWS Jika Anda ingin membawa rentang alamat IPv4 Anda sendiri ke AWS (BYOIP), ada prasyarat. Untuk informasi selengkapnya, lihat Tutorial: Bawa alamat IP Anda ke IPAM.

AWS Management Console

Untuk membuat kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih Buat kolam.
4. Di bawah cakupan IPAM, pilih ruang lingkup pribadi yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.

   Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Kolam dalam lingkup pribadi harus berupa kolam IPv4. Kolam dalam lingkup publik dapat berupa kolam IPv4 atau IPv6. Ruang lingkup publik ditujukan untuk semua ruang publik.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.
6. Di bawah Sumber, pilih cakupan IPAM.
7. Di bawah Keluarga alamat, pilih IPv4.
8. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
9. Untuk Locale, pilih None. Anda akan mengatur lokal di kolam Regional.

   Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena

pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP.

10. (Opsional) Anda dapat membuat pool tanpa CIDR, tetapi Anda tidak akan dapat menggunakan pool untuk alokasi sampai Anda telah menyediakan CIDR untuk itu. Untuk menyediakan CIDR, pilih Tambahkan CIDR baru. Masukkan IPv4 CIDR untuk penyediaan kolam. Jika Anda ingin membawa rentang alamat IP IPv4 atau IPv6 Anda sendiri ke AWS sana ada prasyarat. Untuk informasi selengkapnya, lihat Tutorial: Bawa alamat IP Anda ke IPAM.
11. Pilih aturan alokasi opsional untuk kumpulan ini:

    - Impor sumber daya yang ditemukan secara otomatis: Opsi ini tidak tersedia jika Lokal disetel ke Tidak Ada. Jika dipilih, IPAM akan terus mencari sumber daya dalam rentang CIDR kumpulan ini dan secara otomatis mengimpornya sebagai alokasi ke IPAM Anda. Perhatikan hal berikut:
        - CIDR yang akan dialokasikan untuk sumber daya ini tidak boleh dialokasikan ke sumber daya lain agar impor berhasil.
        - IPAM akan mengimpor CIDR terlepas dari kepatuhannya dengan aturan alokasi kumpulan, sehingga sumber daya dapat diimpor dan kemudian ditandai sebagai tidak patuh.
        - Jika IPAM menemukan beberapa CIDR yang tumpang tindih, IPAM akan mengimpor CIDR terbesar saja.
        - Jika IPAM menemukan beberapa CIDR dengan CIDR yang cocok, IPAM akan mengimpor salah satunya secara acak saja.

    ⚠ Warning
    - Setelah Anda membuat IPAM, saat Anda membuat VPC, pilih opsi blok CIDR yang dialokasikan IPAM. Jika tidak, CIDR yang Anda pilih untuk VPC Anda mungkin tumpang tindih dengan alokasi CIDR IPAM.
    - Jika Anda memiliki VPC yang sudah dialokasikan di kolam IPAM, VPC dengan CIDR yang tumpang tindih tidak dapat diimpor secara otomatis. Misalnya, jika Anda memiliki VPC dengan 10.0.0.0/26 CIDR yang dialokasikan di kolam IPAM, VPC dengan CIDR 10.0.0.0/23 (yang akan mencakup 10.0.0.0/26 CIDR) tidak dapat diimpor.

- Dibutuhkan beberapa waktu untuk alokasi CIDR VPC yang ada untuk diimpor secara otomatis ke IPAM.

- Panjang netmask minimum: Panjang netmask minimum yang diperlukan untuk alokasi CIDR di kolam IPAM ini agar sesuai dan blok CIDR ukuran terbesar yang dapat dialokasikan dari kolam. Panjang netmask minimum harus kurang dari panjang netmask maksimum. Kemungkinan panjang netmask untuk alamat IPv4 adalah 0 - 32. Kemungkinan panjang netmask untuk alamat IPv6 adalah 0 - 128.
- Panjang netmask default: Panjang netmask default untuk alokasi ditambahkan ke pool ini. Misalnya, jika CIDR yang disediakan untuk kumpulan ini **`10.0.0.0/8`** dan Anda masuk ke **`16`** sini, alokasi baru apa pun di kumpulan ini akan default ke panjang netmask /16.
- Panjang netmask maksimum: Panjang netmask maksimum yang akan diperlukan untuk alokasi CIDR di kolam ini. Nilai ini menentukan blok CIDR ukuran terkecil yang dapat dialokasikan dari kolam.
- Persyaratan penandaan: Tag yang diperlukan untuk sumber daya untuk mengalokasikan ruang dari kolam. Jika tag sumber daya diubah setelah mereka mengalokasikan ruang atau jika aturan penandaan alokasi diubah pada kumpulan, sumber daya dapat ditandai sebagai tidak sesuai.
- Lokal: Lokal yang akan dibutuhkan untuk sumber daya yang menggunakan CIDR dari kolam ini. Sumber daya yang diimpor secara otomatis yang tidak memiliki lokal ini akan ditandai tidak sesuai. Sumber daya yang tidak secara otomatis diimpor ke kolam tidak akan diizinkan mengalokasikan ruang dari kolam kecuali mereka berada di lokal ini.

12. (Opsional) Pilih Tag untuk kolam renang.
13. Pilih Buat kolam.
14. Lihat Buat kolam IPv4 Regional.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk membuat atau mengedit kumpulan tingkat atas di IPAM Anda:

1. Buat kolam: create-ipam-pool.
2. Edit kumpulan setelah Anda membuatnya untuk mengubah aturan alokasi: modify-ipam-pool.

Buat kolam IPv4 Regional

Ikuti langkah-langkah di bagian ini untuk membuat kumpulan Regional di dalam kolam tingkat atas Anda. Jika Anda hanya membutuhkan kolam tingkat atas, dan tidak memerlukan kolam Regional dan pengembangan tambahan, lewati saja. Alokasikan CIDR

> **Note**
>
> Proses pembuatan kolam renang berbeda untuk kolam dalam lingkup publik dan pribadi. Bagian ini mencakup langkah-langkah untuk membuat kolam regional dalam lingkup pribadi. Untuk tutorial BYOIP dan BYOASN, lihat. Tutorial

Contoh berikut menunjukkan hierarki struktur kolam yang Anda buat dengan mengikuti petunjuk dalam panduan ini. Pada langkah ini, Anda membuat kolam IPAM Regional:

- IPAM beroperasi di AWS Wilayah 1 dan AWS Wilayah 2
  - Ruang lingkup pribadi
    - Kolam renang tingkat atas (10.0.0.0/8)
      - Kolam regional di AWS Wilayah 1 (10.0.0.0/16)
        - Kumpulan pengembangan untuk VPC non-produksi (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.0.0/25)

Dalam contoh sebelumnya, CIDR yang digunakan adalah contoh saja. Mereka menggambarkan bahwa setiap kolam dalam kolam tingkat atas disediakan dengan sebagian CIDR tingkat atas.

AWS Management Console

Untuk membuat kolam Regional dalam kolam tingkat atas

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih Buat kolam.
4. Di bawah cakupan IPAM, pilih lingkup yang sama dengan yang Anda gunakan saat membuat kumpulan tingkat atas. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.

6. Di bawah Sumber, pilih kolam IPAM. Kemudian pilih kolam tingkat atas yang Anda buat di bagian sebelumnya.
7. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
8. Pilih lokasi untuk kolam renang. Memilih lokal memastikan tidak ada dependensi lintas wilayah antara kumpulan Anda dan sumber daya yang dialokasikan darinya. Opsi yang tersedia berasal dari Wilayah operasi yang Anda pilih saat Anda membuat IPAM Anda.

   Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP.

   > **Note**
   >
   > Jika Anda membuat kolam di Tingkat Gratis, Anda hanya dapat memilih lokal yang cocok dengan Wilayah asal IPAM Anda. Untuk menggunakan semua fitur IPAM di seluruh lokal, tingkatkan ke Tingkat Lanjut.

9. (Opsional) Pilih CIDR untuk disediakan untuk kolam. Anda dapat membuat pool tanpa CIDR, tetapi Anda tidak akan dapat menggunakan pool untuk alokasi sampai Anda telah menyediakan CIDR untuk itu. Anda dapat menambahkan CIDR ke kolam kapan saja dengan mengedit kolam.
10. Anda memiliki opsi aturan alokasi yang sama di sini seperti yang Anda lakukan saat membuat kumpulan tingkat atas. Lihat Buat kolam IPv4 tingkat atas penjelasan tentang opsi yang tersedia saat Anda membuat kumpulan. Aturan alokasi untuk kolam Regional tidak diwarisi dari kolam tingkat atas. Jika Anda tidak menerapkan aturan apa pun di sini, tidak akan ada aturan alokasi yang ditetapkan untuk kumpulan.
11. (Opsional) Pilih Tag untuk kolam renang.
12. Setelah selesai mengonfigurasi pool, pilih Create pool.
13. Lihat Buat kolam IPv4 pengembangan.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk membuat kumpulan Regional di IPAM Anda:

1. Dapatkan ID cakupan tempat Anda ingin membuat kumpulan di: describe-ipam-scopes
2. Dapatkan ID kolam tempat Anda ingin membuat pool di: describe-ipam-pools
3. Buat kolam renang: create-ipam-pool
4. Lihat kolam baru: describe-ipam-pools

Ulangi langkah-langkah ini untuk membuat kolam tambahan di dalam kolam tingkat atas, sesuai kebutuhan.

Buat kolam IPv4 pengembangan

Ikuti langkah-langkah di bagian ini untuk membuat kumpulan pengembangan di dalam kumpulan Regional Anda. Jika Anda hanya membutuhkan kolam tingkat atas dan Regional, dan tidak membutuhkan kolam pengembangan, lewati saja. Alokasikan CIDR

Contoh berikut menunjukkan hierarki struktur kolam yang dapat Anda buat dengan instruksi dalam panduan ini. Pada langkah ini, Anda membuat kumpulan IPAM pengembangan:

- IPAM beroperasi di AWS Wilayah 1 dan AWS Wilayah 2
  - Ruang lingkup pribadi
    - Kolam renang tingkat atas (10.0.0.0/8)
      - Kolam regional di AWS Wilayah 1 (10.0.0.0/16)
        - Kumpulan pengembangan untuk VPC non-produksi (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.1.0/25)

Dalam contoh sebelumnya, CIDR yang digunakan adalah contoh saja. Mereka menggambarkan bahwa setiap kolam dalam kolam tingkat atas disediakan dengan sebagian CIDR tingkat atas.

AWS Management Console

Untuk membuat kolam pengembangan di dalam kolam Regional

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih Buat kolam.
4. Di bawah cakupan IPAM, pilih cakupan yang sama dengan yang Anda gunakan saat membuat kumpulan tingkat atas dan Regional. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.
6. Di bawah Sumber, pilih kolam IPAM. Kemudian pilih kolam Regional.
7. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
8. (Opsional) Pilih CIDR untuk disediakan untuk kolam. Anda hanya dapat menyediakan CIDR yang disediakan ke kolam tingkat atas. Anda dapat membuat pool tanpa CIDR, tetapi Anda tidak akan dapat menggunakan pool untuk alokasi sampai Anda telah menyediakan CIDR untuk itu. Anda dapat menambahkan CIDR ke kolam kapan saja dengan mengedit kolam.
9. Anda memiliki opsi aturan alokasi yang sama di sini seperti yang Anda lakukan saat membuat kumpulan tingkat atas dan Regional. Lihat Buat kolam IPv4 tingkat atas penjelasan tentang opsi yang tersedia saat Anda membuat kumpulan. Aturan alokasi untuk pool tidak diwarisi dari pool di atasnya dalam hierarki. Jika Anda tidak menerapkan aturan apa pun di sini, tidak ada aturan alokasi yang akan ditetapkan untuk kolam renang.
10. (Opsional) Pilih Tag untuk pool.
11. Setelah selesai mengonfigurasi pool, pilih Create pool.
12. Lihat Alokasikan CIDR.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk membuat kumpulan Regional di IPAM Anda:

1. Dapatkan ID cakupan tempat Anda ingin membuat kumpulan di: describe-ipam-scopes

2. Dapatkan ID kolam tempat Anda ingin membuat pool di: describe-ipam-pools
3. Buat kolam: create-ipam-pool
4. Lihat kolam baru: describe-ipam-pools

Ulangi langkah-langkah ini untuk membuat kumpulan pengembangan tambahan di dalam kolam Regional, sesuai kebutuhan.

Buat kolam IPv6

Ikuti langkah-langkah dalam bagian ini untuk membuat hierarki IPv6. Ketika Anda membuat kolam renang, Anda dapat menyediakan CIDR untuk kolam renang untuk digunakan. Kolam memberikan ruang di dalam CIDR itu untuk alokasi di dalam kolam renang. Alokasi adalah tugas CIDR dari kumpulan IPAM ke sumber daya lain atau kumpulan IPAM.

Contoh berikut menunjukkan hirarki struktur kolam yang dapat Anda buat dengan petunjuk dalam panduan ini. Pada bagian ini, Anda membuat hierarki kolam IPv6 IPAM:

- IPAM beroperasi diAWS Wilayah 1 danAWS Wilayah 2
  - Lingkup
    - Kolam regional diAWS Wilayah 1 (2001:db8: :/52)
      - Kolam pengembangan (2001: db8: :/54)
        - Alokasi untuk VPC (2001: db8: :/56)

Konten

- Buat kolam IPv6 Regional
- Buat kolam IPv6 pengembangan

Buat kolam IPv6 Regional

Ikuti langkah-langkah di bagian ini untuk membuat kolam IPAM regional IPv6. Saat Anda menyediakan blok IPv6 CIDR yang disediakan Amazon ke kolam, blok tersebut harus disediakan ke kolam dengan lokal (Wilayah) yang dipilih. AWS Ketika Anda membuat pool, Anda dapat menyediakan CIDR untuk pool untuk digunakan atau menambahkannya nanti. Anda kemudian menetapkan ruang itu ke alokasi. Alokasi adalah tugas CIDR dari kolam IPAM ke kolam IPAM lain atau ke sumber daya.

Contoh berikut menunjukkan hierarki struktur kolam yang dapat Anda buat dengan instruksi dalam panduan ini. Pada langkah ini, Anda membuat kolam IPAM regional IPv6:

- IPAM beroperasi di AWS Wilayah 1 dan AWS Wilayah 2
  - Ruang lingkup publik
    - Kolam regional di AWS Wilayah 1 (2001:db8: :/52)
      - Kolam pengembangan (2001:db8: :/54)
        - Alokasi untuk VPC (2001:db8: :/56)

Dalam contoh sebelumnya, CIDR yang digunakan adalah contoh saja. Mereka menggambarkan bahwa setiap kolam dalam kolam regional IPv6 disediakan dengan sebagian dari CIDR regional IPv6.

Saat membuat kolam IPAM, Anda dapat mengonfigurasi aturan untuk alokasi yang dibuat dalam kolam IPAM.

Aturan alokasi memungkinkan Anda mengonfigurasi hal berikut:

- Panjang netmask yang diperlukan untuk alokasi di dalam kolam
- Tag yang diperlukan untuk sumber daya di dalam kolam
- Lokal yang diperlukan untuk sumber daya di dalam kolam. Lokal adalah AWS Wilayah di mana kolam IPAM tersedia untuk alokasi.

Aturan alokasi menentukan apakah sumber daya sesuai atau tidak sesuai. Untuk informasi tambahan tentang kepatuhan, lihatPantau penggunaan CIDR berdasarkan sumber daya.

> **Important**
>
> Ada aturan implisit tambahan yang tidak ditampilkan dalam aturan alokasi. Jika sumber daya berada di kolam IPAM yang merupakan sumber daya bersama di AWS Resource Access Manager (RAM), pemilik sumber daya harus dikonfigurasi sebagai prinsipal dalam AWS RAM. Untuk informasi selengkapnya tentang berbagi pool dengan RAM, lihatMembagikan kumpulan IPAM menggunakanAWS RAM.

Contoh berikut menunjukkan cara Anda menggunakan aturan alokasi untuk mengontrol akses ke kolam IPAM:

Example

Saat Anda membuat kumpulan berdasarkan kebutuhan perutean dan keamanan, Anda mungkin hanya ingin mengizinkan sumber daya tertentu untuk menggunakan kolam renang. Dalam kasus seperti itu, Anda dapat menetapkan aturan alokasi yang menyatakan bahwa sumber daya apa pun yang menginginkan CIDR dari kumpulan ini harus memiliki tag yang cocok dengan persyaratan tag aturan alokasi. Misalnya, Anda dapat menetapkan aturan alokasi yang menyatakan bahwa hanya VPC dengan tag prod yang bisa mendapatkan CIDR dari kumpulan IPAM.

> **Important**
>
> Topik ini mencakup cara membuat kolam regional IPv6 dengan rentang alamat IP yang disediakan oleh. AWS Jika Anda ingin membawa rentang alamat IP IPv4 atau IPv6 Anda sendiri ke AWS (BYOIP), ada prasyarat. Untuk informasi selengkapnya, lihat Tutorial: Bawa alamat IP Anda ke IPAM.

AWS Management Console

Untuk membuat kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih Buat kolam.
4. Di bawah lingkup IPAM, pilih ruang lingkup publik. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.

   Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Kolam dalam lingkup pribadi harus berupa kolam IPv4. Kolam dalam lingkup publik dapat berupa kolam IPv4 atau IPv6. Ruang lingkup publik ditujukan untuk semua ruang yang dapat atau saat ini diiklankan oleh AWS ke internet.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.
6. Di bawah Sumber, pilih cakupan IPAM.
7. Untuk keluarga Alamat, pilih IPv6. Alihkan Izinkan CIDR di kolam ini agar dapat diiklankan secara publik muncul. Secara default, semua CIDR di kolam ini akan dapat diiklankan secara publik. Anda tidak dapat mengaktifkan atau menonaktifkan opsi ini.

8. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
9. Pilih Lokal untuk kolam renang. Saat Anda menyediakan blok IPv6 CIDR yang disediakan Amazon ke kolam, blok tersebut harus disediakan ke kolam dengan lokal (Wilayah) yang dipilih. AWS Memilih lokal memastikan tidak ada dependensi lintas wilayah antara kumpulan Anda dan sumber daya yang dialokasikan darinya. Opsi yang tersedia berasal dari Wilayah operasi yang Anda pilih untuk IPAM saat Anda membuatnya. Anda dapat menambahkan Wilayah operasi tambahan kapan saja.

   Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP.

   > **Note**
   >
   > Jika Anda membuat kolam di Tingkat Gratis, Anda hanya dapat memilih lokal yang cocok dengan Wilayah asal IPAM Anda. Untuk menggunakan semua fitur IPAM di seluruh lokal, tingkatkan ke Tingkat Lanjut.

10. Di bawah Layanan, pilih EC2 (EIP/VPC). Layanan yang Anda pilih menentukan AWS layanan di mana CIDR akan dapat diiklankan. Saat ini, satu-satunya pilihan adalah EC2 (EIP/VPC), yang berarti bahwa CIDR yang dialokasikan dari kumpulan ini akan dapat diiklankan untuk layanan Amazon EC2 (untuk alamat IP Elastis) dan layanan Amazon VPC (untuk CIDR yang terkait dengan VPC).
11. Di bawah opsi Sumber IP Publik, pilih Amazon yang dimiliki untuk AWS menyediakan rentang alamat IPv6 untuk kumpulan ini. Seperti disebutkan di bagian atas halaman ini, topik ini mencakup cara membuat kolam regional IPv6 dengan rentang alamat IP yang disediakan oleh. AWS Jika Anda ingin membawa rentang alamat IPv4 atau IPv6 Anda sendiri ke AWS (BYOIP), ada prasyarat. Untuk informasi selengkapnya, lihat Tutorial: Bawa alamat IP Anda ke IPAM.
12. Untuk pool dalam lingkup publik yang menggunakan sumber IP publik BYOIP, Anda dapat mengontrol apakah AWS dapat secara publik mengiklankan CIDR di kolam ini dengan Izinkan CIDR di kolam ini agar dapat diiklankan secara publik. Secara default opsi ini

diaktifkan. Nonaktifkan opsi ini jika Anda tidak ingin mengizinkan AWS untuk mengiklankan CIDR secara publik di kolam ini.

13. (Opsional) Anda dapat membuat pool tanpa CIDR, tetapi Anda tidak akan dapat menggunakan pool untuk alokasi sampai Anda telah menyediakan CIDR untuk itu. Untuk menyediakan CIDR, pilih Tambahkan CIDR milik Amazon dan pilih ukuran netmask antara /40 dan /52 untuk CIDR.

> **Note**
>
> Perhatikan hal berikut:
>
> - Secara default, Anda dapat menambahkan satu blok CIDR IPv6 yang disediakan Amazon ke kolam Regional. Untuk informasi tentang meningkatkan batas default, lihatKuota untuk IPAM Anda.
> - Ketika Anda memilih panjang netmask di menu dropdown, Anda melihat panjang netmask serta jumlah /56 CIDR yang diwakili oleh netmask.

14. Pilih aturan alokasi opsional untuk kumpulan ini:

- Panjang netmask minimum: Panjang netmask minimum yang diperlukan untuk alokasi CIDR di kolam IPAM ini agar sesuai dan blok CIDR ukuran terbesar yang dapat dialokasikan dari kolam. Panjang netmask minimum harus kurang dari panjang netmask maksimum. Kemungkinan panjang netmask untuk alamat IPv6 adalah 0 - 128.
- Panjang netmask default: Panjang netmask default untuk alokasi ditambahkan ke pool ini. Misalnya, jika CIDR yang disediakan untuk kumpulan ini `2001:db8::/52` dan Anda memasukkan 56 di sini, alokasi baru apa pun di kumpulan ini akan default ke panjang netmask /56.
- Panjang netmask maksimum: Panjang netmask maksimum yang akan diperlukan untuk alokasi CIDR di kolam ini. Nilai ini menentukan blok CIDR ukuran terkecil yang dapat dialokasikan dari kolam. Misalnya, jika Anda memasukkan /56 di sini, panjang netmask terkecil yang dapat dialokasikan untuk CIDR dari kumpulan ini adalah /56.
- Persyaratan penandaan: Tag yang diperlukan untuk sumber daya untuk mengalokasikan ruang dari kolam. Jika tag sumber daya diubah setelah mereka mengalokasikan ruang atau jika aturan penandaan alokasi diubah pada kumpulan, sumber daya dapat ditandai sebagai tidak sesuai.

- Lokal: Lokal yang akan dibutuhkan untuk sumber daya yang menggunakan CIDR dari kolam ini. Sumber daya yang diimpor secara otomatis yang tidak memiliki lokal ini akan ditandai tidak sesuai. Sumber daya yang tidak secara otomatis diimpor ke kolam tidak akan diizinkan mengalokasikan ruang dari kolam kecuali mereka berada di lokal ini.

15. (Opsional) Pilih Tag untuk kolam renang.
16. Pilih Buat kolam.
17. Lihat Buat kolam IPv6 pengembangan.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk membuat atau mengedit kolam regional IPv6 di IPAM Anda:

1. Buat kolam: create-ipam-pool.
2. Edit kumpulan setelah Anda membuatnya untuk mengubah aturan alokasi: modify-ipam-pool.

Buat kolam IPv6 pengembangan

Ikuti langkah-langkah di bagian ini untuk membuat kumpulan pengembangan dalam kolam Regional IPv6 Anda. Jika Anda hanya membutuhkan kolam Regional dan tidak membutuhkan kolam pengembangan, lewati sajaAlokasikan CIDR.

Contoh berikut menunjukkan hierarki struktur kolam yang dapat Anda buat dengan instruksi dalam panduan ini. Pada langkah ini, Anda membuat kumpulan IPAM pengembangan:

- IPAM beroperasi di AWS Wilayah 1 dan AWS Wilayah 2
  - Ruang lingkup publik
    - Kolam regional di AWS Wilayah 1 (2001:db8: :/52)
      - Kolam pengembangan (2001:db8: :/54)
        - Alokasi untuk VPC (2001:db8: :/56)

Dalam contoh sebelumnya, CIDR yang digunakan adalah contoh saja. Mereka menggambarkan bahwa setiap kolam dalam kolam tingkat atas disediakan dengan sebagian CIDR tingkat atas.

AWS Management Console

Untuk membuat kolam pengembangan dalam kolam Regional IPv6

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih Buat kolam.
4. Di bawah lingkup IPAM, pilih ruang lingkup publik. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.

   Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Kolam dalam lingkup pribadi harus kolam IPv4. Kolam dalam lingkup publik dapat berupa kolam IPv4 atau IPv6. Ruang lingkup publik ditujukan untuk semua ruang yang dapat atau saat ini diiklankan oleh AWS ke internet.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.
6. Di bawah Sumber, pilih kolam IPAM. Kemudian, di bawah Source pool, pilih IPv6 Regional pool.
7. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
8. (Opsional) Pilih CIDR untuk disediakan untuk kolam. Anda hanya dapat menyediakan CIDR yang disediakan ke kolam tingkat atas. Anda dapat membuat pool tanpa CIDR, tetapi Anda tidak akan dapat menggunakan pool untuk alokasi sampai Anda telah menyediakan CIDR untuk itu. Anda dapat menambahkan CIDR ke kolam kapan saja dengan mengedit kolam.
9. Anda memiliki opsi aturan alokasi yang sama di sini seperti yang Anda lakukan saat membuat kolam Regional IPv6. Lihat Buat kolam IPv6 Regional penjelasan tentang opsi yang tersedia saat Anda membuat kumpulan. Aturan alokasi untuk pool tidak diwarisi dari pool di atasnya dalam hierarki. Jika Anda tidak menerapkan aturan apa pun di sini, tidak ada aturan alokasi yang akan ditetapkan untuk kolam renang.
10. (Opsional) Pilih Tag untuk pool.
11. Setelah selesai mengonfigurasi pool, pilih Create pool.
12. Lihat Alokasikan CIDR.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk membuat kolam Regional IPv6 di IPAM Anda:

1. Dapatkan ID cakupan tempat Anda ingin membuat kumpulan di: describe-ipam-scopes
2. Dapatkan ID kolam tempat Anda ingin membuat pool di: describe-ipam-pools
3. Buat kolam: create-ipam-pool
4. Lihat kolam baru: describe-ipam-pools

Ulangi langkah-langkah ini untuk membuat kumpulan pengembangan tambahan dalam kolam Regional IPv6, sesuai kebutuhan.

Alokasikan CIDR

Ikuti langkah-langkah dalam bagian ini untuk mengalokasikan CIDR pada pool IPAM pada sumber daya.

> **Note**
>
> Ketentuan ketentuan dan alokasi digunakan di seluruh panduan pengguna ini dan konsol IPAM. Ketentuan digunakan saat Anda menambahkan CIDR ke kolam IPAM. Mengalokasikan digunakan ketika Anda mengaitkan CIDR dari kolam IPAM dengan sumber daya.

Anda dapat mengalokasikan CIDR dari pool IPAM dengan cara-cara berikut:

- GunakanAWS layanan yang terintegrasi dengan IPAM, seperti Amazon VPC, dan pilih opsi untuk menggunakan kumpulan IPAM untuk CIDR. IPAM secara otomatis membuat alokasi di kolam renang untuk Anda.
- Secara manual mengalokasikan CIDR dalam kumpulan IPAM untuk memesannya untuk digunakan nanti denganAWS layanan yang terintegrasi dengan IPAM, seperti Amazon VPC.

Bagian ini memandu Anda melalui kedua opsi: cara menggunakanAWS layanan yang terintegrasi dengan IPAM untuk menyediakan CIDR kumpulan IPAM, dan cara memesan ruang alamat IP secara manual.

Daftar Isi

- Buat VPC yang menggunakan CIDR kolam IPAM
- Secara manual mengalokasikan CIDR ke pool untuk memesan ruang alamat IP

Buat VPC yang menggunakan CIDR kolam IPAM

Ikuti langkah-langkah dalam Membuat VPC di Panduan Pengguna Amazon VPC. Ketika Anda mencapai langkah untuk memilih CIDR untuk VPC, Anda akan memiliki opsi untuk menggunakan CIDR dari kolam IPAM.

Jika Anda memilih opsi untuk menggunakan kolam IPAM saat Anda membuat VPC,AWS alokasikan CIDR di kolam IPAM. Anda dapat melihat alokasi di IPAM dengan memilih pool di panel konten konsol IPAM dan melihat tab Resources untuk pool.

> **Note**
>
> Untuk instruksi lengkap menggunakanAWS CLI, termasuk membuat VPC, lihatTutorial untuk Manajer Alamat IP VPC Amazon bagian.

Secara manual mengalokasikan CIDR ke pool untuk memesan ruang alamat IP

Ikuti langkah-langkah dalam bagian ini untuk secara manual mengalokasikan CIDR pada pool. Anda mungkin melakukan ini untuk memesan CIDR dalam kolam IPAM untuk digunakan nanti. Anda juga dapat memesan ruang di pangkalan IPAM untuk mewakili jaringan lokal. IPAM akan mengelola reservasi tersebut untuk Anda dan menunjukkan apakah ada CIDR yang tumpang tindih dengan ruang IP lokal Anda.

AWS Management Console

Untuk mengalokasikan CIDR secara manual

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.

2. Di panel navigasi, pilih Pools.
3. Secara default, lingkup privat default. Jika Anda tidak ingin menggunakan lingkup pribadi default, dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi selengkapnya tentang lingkup, lihatCara kerja IPAM.
4. Di panel konten, pilih pool.
5. Pilih Tindakan > Buat alokasi khusus.
6. Pilih apakah akan menambahkan CIDR tertentu untuk mengalokasikan (`10.0.0.0/24`misalnya, untuk IPv4 atau`2001:db8::/52` IPv6) atau menambahkan CIDR berdasarkan ukuran dengan memilih panjang netmask saja (misalnya,`/24` untuk IPv4 atau`/52` IPv6).
7. Pilih Alokasikan.
8. Anda dapat melihat alokasi di IPAM dengan memilih Pools di panel navigasi, memilih pool, dan melihat tab Alokasi untuk pool.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk mengalokasikan CIDR secara manual ke pool:

1. Dapatkan ID dari kolam IPAM yang ingin Anda buat alokasi di: describe-ipam-pools.
2. Buat alokasi: allocate-ipam-pool-cidr.
3. Lihat alokasi: get-ipam-pool-allocations.

Untuk melepaskan CIDR yang dialokasikan secara manual, lihatRilis alokasi yang berbeda..

Mengelola ruang alamat IP di IPAM

Tugas di bagian ini adalah opsional. Jika Anda ingin menyelesaikan tugas di bagian ini, dan Anda telah mendelegasikan akun IPAM, tugas harus diselesaikan oleh administrator IPAM.

Ikuti langkah-langkah di bagian ini untuk mengelola ruang alamat IP Anda di IPAM.

Konten

- Terapkan penggunaan IPAM untuk pembuatan VPC
- Membagikan kumpulan IPAM menggunakanAWS RAM
- Menyediakan CIDR ke kolam
- Deprovision CIDR dari kolam
- Mengedit kolam yang lebih baik.
- Menghapus kolam kolam kolam kolam kolam kolam renang
- Bekerja dengan penemuan sumber daya
- Buat cakupan tambahan
- Memindahkan CIDR VPC antar cakupan
- Ubah status pemantauan CIDR VPC
- Menghapus cakupan
- Rilis alokasi yang berbeda.
- Memodifikasi IPAM
- Menghapus IPAM

Terapkan penggunaan IPAM untuk pembuatan VPC

> **Note**
>
> Bagian ini hanya berlaku untuk Anda jika Anda telah mengaktifkan IPAM untuk diintegrasikanAWS Organizations. Untuk informasi selengkapnya, lihat Integrasikan IPAM dengan akun di Organisasi AWS.

Bagian ini menjelaskan cara membuat kebijakan kontrol layananAWS Organizations yang mengharuskan anggota di organisasi Anda menggunakan IPAM saat mereka membuat VPC.

Kebijakan kontrol layanan (SCP) adalah jenis kebijakan organisasi yang memungkinkan Anda mengelola izin dalam organisasi Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan di PanduanAWS Organizations pengguna.

Terapkan IPAM saat membuat VPC

Ikuti langkah-langkah di bagian ini untuk meminta anggota dalam organisasi Anda untuk menggunakan IPAM saat membuat VP.

Untuk membuat SCP dan membatasi pembuatan VPC ke IPAM

1. Ikuti langkah-langkah dalam Membuat SCP di PanduanAWS Organizations Pengguna dan masukkan teks berikut di 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. Lampirkan kebijakan ke satu atau beberapa unit organisasi di organisasi Anda. Untuk informasi selengkapnya, lihat Melampirkan dan melepaskan kebijakan kontrol layanan di PanduanAWS Organizations Pengguna.

Menegakkan kolam IPAM saat membuat VPC

Ikuti langkah-langkah di bagian ini untuk mewajibkan anggota di organisasi Anda menggunakan pangkalan IPAM tertentu saat membuat VPC.

Untuk membuat SCP dan membatasi pembuatan VPC ke kolam IPAM

1. Ikuti langkah-langkah dalam Membuat SCP di PanduanAWS Organizations Pengguna dan masukkan teks berikut di 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. Ubah nilai`ipam-pool-0123456789abcdefg` contoh ke ID pool IPv4 yang ingin Anda batasi pengguna.
3. Lampirkan kebijakan ke satu atau beberapa unit organisasi di organisasi Anda. Untuk informasi selengkapnya, lihat Melampirkan dan melepaskan kebijakan kontrol layanan di PanduanAWS Organizations Pengguna.

Terapkan IPAM untuk semua kecuali daftar OU yang diberikan

Ikuti langkah-langkah di bagian ini untuk menegakkan IPAM untuk semua kecuali daftar Unit Organisasi (OU) yang diberikan. Kebijakan yang dijelaskan di bagian ini memerlukan OU dalam organisasi kecuali untuk OU yang Anda tentukan`aws:PrincipalOrgPaths` untuk menggunakan IPAM untuk membuat dan memperluas VPC. OU yang terdaftar dapat menggunakan IPAM saat membuat VPC atau menentukan rentang alamat IP secara manual.

Untuk membuat SCP dan menegakkan IPAM untuk semua kecuali daftar OU yang diberikan

1. Ikuti langkah-langkah dalam Membuat SCP di PanduanAWS Organizations Pengguna dan masukkan teks berikut di 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. Hapus nilai contoh (sepertio-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/) dan tambahkan jalur entitasAWS Organizations dari OU yang ingin Anda miliki opsi (tetapi tidak memerlukan) untuk menggunakan IPAM. Untuk informasi selengkapnya tentang jalur entitas, lihat Memahami jalur entitasAWS Organizations dan aws:PrincipalOrgPaths di PanduanAWS Identity and Access Management Pengguna.
3. Lampirkan kebijakan ke root organisasi Anda. Untuk informasi selengkapnya, lihat Melampirkan dan melepaskan kebijakan kontrol layanan di PanduanAWS Organizations Pengguna.

Membagikan kumpulan IPAM menggunakanAWS RAM

Ikuti langkah-langkah dalam bagian ini untuk membagikan kumpulan IPAM menggunakanAWS Resource Access Manager (RAM). Saat Anda berbagi kumpulan IPAM dengan RAM, “prinsipal” dapat mengalokasikan CIDR dari kumpulan keAWS sumber daya, seperti VPC, dari akun masing-masing. Principal adalah konsep dalam RAM yang berartiAWS akun, peran IAM, atau unit Organizations apa pun dalamAWS Organisasi. Untuk informasi selengkapnya, lihat BerbagiAWS sumber daya Anda di Panduan PenggunaAWS RAM.

> **Note**
>
> - Anda hanya dapat berbagi kumpulan IPAM denganAWS RAM jika Anda telah mengintegrasikan IPAM denganAWS Organizations. Untuk informasi selengkapnya, lihat Integrasikan IPAM dengan akun di Organisasi AWS. Anda tidak dapat berbagi kumpulan IPAM denganAWS RAM jika Anda adalah pengguna IPAM satu akun.

- Anda harus mengaktifkan pembagian sumber daya denganAWS Organizations dalamAWS RAM. Untuk informasi selengkapnya, lihat Mengaktifkan berbagi sumber daya dalamAWS Organizations di Panduan PenggunaAWS RAM.
- Berbagi RAM hanya tersedia diAWS Wilayah asal IPAM Anda. Anda harus membuat bagian diAWS Wilayah tempat IPAM berada, bukan di Wilayah kumpulan IPAM.
- Akun yang membuat dan menghapus saham sumber daya kumpulan IPAM harus memiliki izin berikut dalam kebijakan IAM yang melekat pada peran IAM mereka:
  - `ec2:PutResourcePolicy`
  - `ec2:DeleteResourcePolicy`
- Anda dapat menambahkan beberapa kumpulan IPAM ke berbagi RAM.

AWS Management Console

Membagikan kumpulan IPAM menggunakan RAM

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, lingkup privat default dipilih. Jika Anda tidak ingin menggunakan lingkup pribadi default, dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Di panel konten, pilih pool yang ingin Anda bagikan dan pilih Tindakan > Lihat detail.
5. Dalam Berbagi sumber daya, pilih Buat berbagi sumber daya. Akibatnya, konsolAWS RAM terbuka. Anda akan membuat kolam bersama dalamAWS RAM.
6. Pilih Buat berbagi sumber daya.
7. Tambahkan Nama untuk sumber daya bersama.
8. Di bawah Pilih jenis sumber daya, pilih kumpulan IPAM dan pilih satu atau beberapa kumpulan IPAM.
9. Pilih Selanjutnya.
10. Pilih salah satu izin untuk berbagi sumber daya:
    - AWSRAMDefaultPermissionsIpamPool: Pilih izin ini untuk mengizinkan prinsipal melihat CIDR dan alokasi di kumpulan IPAM bersama dan mengalokasi/melepaskan CIDR di pangkalan.

- AWSRAMPermissionIpamPoolByoipCidrImport: Pilih izin ini untuk mengizinkan prinsipal mengimpor CIDR BYOIP ke dalam kumpulan IPAM bersama. Anda akan memerlukan izin ini hanya jika Anda memiliki CIDR BYOIP yang ada dan Anda ingin mengimpornya ke IPAM dan membagikannya dengan prinsipal. Untuk informasi tambahan tentang CIDR BYOIP ke IPAM, lihatTutorial: Transfer BYOIP IPv4 CIDR ke IPAM.

11. Pilih prinsipal yang diizinkan untuk mengakses sumber daya ini. Jika prinsipal akan mengimpor CIDR BYOIP yang ada ke kumpulan IPAM bersama ini, tambahkan akun pemilik BYOIP CIDR sebagai prinsipal.
12. Tinjau opsi berbagi sumber daya dan prinsipal yang akan Anda bagikan dan pilih Buat.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Di sana Anda akan menemukan deskripsi terperinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

GunakanAWS CLI perintah berikut untuk berbagi kumpulan IPAM menggunakan RAM:

1. Dapatkan ARN IPAM: describe-ipam-pools
2. Buat pangsa sumber daya: create-resource-share
3. Lihat pangsa sumber daya: get-resource-shares

Sebagai hasil dari menciptakan pangsa sumber daya dalam RAM, prinsipal lain sekarang dapat mengalokasikan CIDR ke sumber daya menggunakan kolam IPAM. Untuk informasi tentang sumber daya pemantauan yang dibuat oleh kepala sekolah, lihatPantau penggunaan CIDR berdasarkan sumber daya. Untuk informasi selengkapnya tentang cara membuat VPC dan mengalokasikan CIDR dari kumpulan IPAM bersama, lihat Membuat VPC di Panduan Pengguna Amazon VPC.

Menyediakan CIDR ke kolam

Ikuti langkah-langkah dalam bagian ini untuk menyediakan CIDR ke kolam. Jika Anda sudah menyediakan CIDR saat membuat pool, Anda mungkin perlu menyediakan CIDR tambahan jika pool mendekati alokasi penuh. Untuk memantau penggunaan kolam renang, lihatMemantau penggunaan CIDR dengan dasbor IPAM.

> **Note**
>
> Ketentuan ketentuan dan alokasi digunakan di seluruh panduan pengguna ini dan konsol IPAM. Ketentuan digunakan saat Anda menambahkan CIDR ke kolam IPAM. Alokasikan digunakan saat Anda mengaitkan CIDR dari kolam IPAM dengan alamat IP VPC atau Elastic.

AWS Management Console

Untuk menyediakan CIDR ke pool

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, lingkup privat default dipilih. Jika Anda tidak ingin menggunakan lingkup pribadi default, dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Di panel konten, pilih kolam yang ingin ditambahkan CIDR.
5. Pilih Tindakan > Menyediakan CIDR.
6. Masukkan CIDR yang ingin Anda tambahkan, lalu pilih Tambahkan CIDR baru untuk CIDR tambahan.

   > **Note**
   >
   > - Secara default, Anda dapat menambahkan blok CIDR IPv6 yang disediakan Amazon ke kolam Regional. Untuk informasi tentang meningkatkan batas default, lihatKuota untuk IPAM Anda.
   > - CIDR yang ingin Anda sediakan harus tersedia dalam lingkup.
   > - Jika Anda menyediakan CIDR ke kolam renang dalam kolam renang, maka ruang CIDR yang ingin Anda sediakan harus tersedia di kolam renang.

7. Pilih Minta penyediaan.
8. Anda dapat melihat CIDR di IPAM dengan memilih Pools di panel navigasi, memilih kolam renang, dan melihat tab CIDRs untuk kolam renang.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk menyediakan CIDR ke pool:

1. Dapatkan ID dari kolam IPAM: describe-ipam-pools
2. Dapatkan CIDR yang disediakan ke pool: get-ipam-pool-cidrs
3. Menyediakan CIDR baru ke pool: provision-ipam-pool-cidr
4. Dapatkan CIDR yang disediakan untuk kolam renang dan melihat CIDR baru: get-ipam-pool-cidrs

Deprovision CIDR dari kolam

Ikuti langkah-langkah di bagian ini untuk menghapus CIDR dari pool IPAM. Ketika Anda membatalkan semua CIDR pool, pool tidak dapat lagi digunakan untuk alokasi. Anda harus terlebih dahulu menyediakan CIDR baru ke pool sebelum Anda dapat menggunakan pool untuk alokasi.

> **Important**
>
> Anda tidak dapat membatalkan penyediaan CIDR jika ada alokasi di pool. Untuk menghapus alokasi, lihatRilis alokasi yang berbeda..

AWS Management Console

Untuk deprovision kolam CIDR

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Pada panel navigasi, pilih Pools.
3. Pada menu dropdown di bagian atas panel konten, pilih scope yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Pada panel konten, pilih pool yang CIDR yang ingin Anda deprovision.
5. Pilih tab CIDRs.
6. Pilih satu atau lebih CIDR dan pilih Deprovision CIDR.

7. Pilih Deprovision CIDR.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk membatalkan penyediaan kolam CIDR:

1. Dapatkan ID kolam IPAM: describe-ipam-pools
2. Lihat CIDR Anda saat ini untuk pool: get-ipam-pool-cidrs
3. Deprovision CIDR: deprovision-ipam-pool-cidr
4. Lihat CIDR Anda yang diperbarui: get-ipam-pool-cidrs

Untuk penyediaan CIDR baru ke kolam renang, lihatDeprovision CIDR dari kolam. Jika Anda ingin menghapus pool, lihatMenghapus kolam kolam kolam kolam kolam renang.

Mengedit kolam yang lebih baik.

Ikuti langkah-langkah di bagian ini untuk mengedit kolam IPAM. Anda mungkin ingin mengedit pangkalan untuk mengubah aturan alokasi di pangkalan. Untuk informasi selengkapnya tentang aturan alokasi, lihatBuat kolam IPv4 tingkat atas.

AWS Management Console

Untuk mengedit pool

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Poles.
3. Secara default, lingkup privat default dipilih. Jika Anda tidak ingin menggunakan lingkup pribadi default, dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi selengkapnya tentang cakupan selengkapnya tentang cakupan selengkapnya tentang cakupan selengkapnyaCara kerja IPAM
4. Di panel konten, pilih kolam yang ingin Anda edit.
5. Pilih Tindakan > Edit.
6. Membuat perubahan yang Anda butuhkan untuk kolam renang. Untuk informasi tentang opsi konfigurasi pool, lihatBuat kolam IPv4 tingkat atas.

7. Pilih Update (Perbarui).

Command line

GunakanAWS CLI perintah berikut untuk mengedit pool:

1. Dapatkan ID kolam IPAM: describe-ipam-pools
2. Memodifikasi pool: modify-ipam-pool

Menghapus kolam kolam kolam kolam kolam kolam renang

Ikuti langkah-langkah di bagian ini untuk menghapus kolam IPAM.

> **Important**
>
> Anda tidak dapat menghapus pangkalan alamat IP jika ada alokasi di dalamnya. Anda harus melepaskan alokasi terlebih dahulu danDeprovision CIDR dari kolam sebelum Anda dapat menghapus kolam kolam kolam.

AWS Management Console

Untuk menghapus kolam kolam kolam kolam kolam kolam kolam renang

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih kolam.
3. Dari menu tarik-turun pada bagian atas panel konten, pilih scope yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Di panel konten, pilih kolam kolam yang ingin Anda hapus.
5. Pilih Tindakan > Hapus pool.
6. Masukkan**`delete`** dan kemudian pilih Hapus.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk menghapus pool:

1. Lihat pool dan dapatkan ID kolam IPAM: describe-ipam-pools
2. Menghapus pool: delete-ipam-pool
3. Lihat kolam renang Anda: describe-ipam-pools

Untuk membuat kolam kolam kolam kolam baru, lihatBuat kolam IPv4 tingkat atas kolam kolam kolam kolam kolam kolam kolam kolam kolam baru

Bekerja dengan penemuan sumber daya

Penemuan sumber daya adalah komponen IPAM yang memungkinkan IPAM untuk mengelola dan memantau sumber daya milik akun yang dimiliki. Penemuan sumber daya dibuat secara default saat Anda membuat IPAM. Anda juga dapat membuat penemuan sumber daya secara independen dari IPAM dan mengintegrasikannya dengan IPAM yang dimiliki oleh akun atau organisasi lain. Jika pemilik penemuan sumber daya adalah administrator organisasi yang didelegasikan, IPAM akan memantau sumber daya untuk semua anggota organisasi.

> **Note**
>
> Membuat, berbagi, dan mengaitkan penemuan sumber daya adalah bagian dari proses mengintegrasikan IPAM dengan akun di luar organisasi Anda (lihat). Integrasikan IPAM dengan akun di luar organisasi Jika Anda tidak membuat IPAM dan mengintegrasikannya dengan akun di luar organisasi Anda, Anda tidak perlu membuat, berbagi, atau mengaitkan penemuan sumber daya.

Daftar Isi

- Buat penemuan sumber daya
- Lihat detail penemuan sumber daya
- Bagikan penemuan sumber daya
- Kaitkan penemuan sumber daya dengan IPAM
- Putuskan penemuan sumber daya
- Hapus penemuan sumber daya

Buat penemuan sumber daya

Bagian ini menjelaskan cara membuat penemuan sumber daya. Penemuan sumber daya dibuat secara default saat Anda membuat IPAM. Kuota default untuk penemuan sumber daya per Wilayah adalah 1. Untuk informasi lebih lanjut tentang kuota IPAM, lihat. Kuota untuk IPAM Anda

> **Note**
>
> Membuat, berbagi, dan mengaitkan penemuan sumber daya adalah bagian dari proses mengintegrasikan IPAM dengan akun di luar organisasi Anda (lihat). Integrasikan IPAM dengan akun di luar organisasi Jika Anda tidak membuat IPAM dan mengintegrasikannya dengan akun di luar organisasi Anda, Anda tidak perlu membuat, berbagi, atau mengaitkan penemuan sumber daya.

Jika Anda mengintegrasikan IPAM dengan akun di luar organisasi Anda, ini adalah langkah wajib yang harus diselesaikan oleh Akun Admin Org Sekunder. Untuk informasi lebih lanjut tentang peran yang terlibat dalam proses ini, lihatGambaran umum proses.

AWS Management Console

Untuk membuat penemuan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Penemuan sumber daya.
3. Pilih Buat penemuan sumber daya.
4. Pilih Izinkan Pengelola Alamat IP VPC Amazon untuk mereplikasi data dari akun sumber ke akun delegasi IPAM. Jika Anda tidak memilih opsi ini, Anda tidak dapat membuat penemuan sumber daya.
5. (Opsional) Tambahkan tag Nama ke penemuan sumber daya. Tanda merupakan sebuah label yang Anda tetapkan ke sebuah sumber daya AWS. Setiap tanda terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tag untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
6. (Opsional) Tambahkan deskripsi.
7. Di bawah Wilayah operasi, pilih AWS Wilayah di mana sumber daya akan ditemukan. Wilayah saat ini secara otomatis akan ditetapkan sebagai salah satu Wilayah yang beroperasi. Jika Anda membuat penemuan sumber daya sehingga Anda dapat

membagikannya dengan IPAM di Wilayah operasi`us-east-1`, pastikan Anda memilih `us-east-1` di sini. Jika Anda lupa Wilayah operasi, Anda dapat kembali di lain waktu dan mengedit pengaturan penemuan sumber daya Anda.

> **Note**
>
> Dalam kebanyakan kasus, penemuan sumber daya harus memiliki Wilayah operasi yang sama dengan IPAM atau Anda hanya akan mendapatkan penemuan sumber daya di satu Wilayah itu.

8. (Opsional) Pilih Tag tambahan untuk kolam.
9. Pilih Create (Buat).

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

- Buat penemuan sumber daya: create-ipam-resource-discovery

Lihat detail penemuan sumber daya

Bagian ini menjelaskan cara melihat detail untuk penemuan sumber daya. Ini termasuk CIDR sumber daya dan status penemuan akun yang dipantau di bawah penemuan sumber daya Anda.

AWS Management Console

Untuk melihat detail penemuan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Penemuan sumber daya.
3. Pilih penemuan sumber daya.
4. Di bawah Detail penemuan sumber daya, lihat detail yang terkait dengan penemuan sumber daya, seperti Default, yang menunjukkan apakah penemuan sumber daya adalah default. Penemuan sumber daya default adalah penemuan sumber daya yang dibuat secara otomatis saat Anda membuat IPAM.
5. Di tab, lihat detail penemuan sumber daya:

- Sumber daya yang ditemukan - Sumber daya dipantau di bawah penemuan sumber daya. IPAM memantau CIDR dari jenis sumber daya berikut VPC, kolam IPv4 Publik, subnet VPC, dan alamat IP Elastis.
  - Nama (ID Sumber Daya) — ID penemuan sumber daya.
  - Penggunaan IP — Persentase ruang alamat IP yang digunakan. Untuk mengubah desimal menjadi persentase, kalikan desimal dengan 100. Perhatikan hal berikut -
    - Untuk sumber daya yang merupakan VPC, ini adalah persentase ruang alamat IP di VPC yang diambil oleh CIDR subnet.
    - Untuk sumber daya yang merupakan subnet, jika subnet memiliki IPv4 CIDR yang disediakan untuk itu, ini adalah persentase ruang alamat IPv4 di subnet yang digunakan. Jika subnet memiliki IPv6 CIDR yang disediakan untuk itu, persentase ruang alamat IPv6 yang digunakan tidak diwakili. Persentase ruang alamat IPv6 yang digunakan saat ini tidak dapat dihitung.
    - Untuk sumber daya yang merupakan kolam IPv4 publik, ini adalah persentase ruang alamat IP di kolam yang telah dialokasikan ke alamat IP Elastic (EIP).
  - CIDR — Sumber Daya CIDR.
  - Wilayah — Wilayah Sumber Daya.
  - ID Pemilik — ID pemilik sumber daya.
  - Waktu sampel — Waktu penemuan sumber daya terakhir yang berhasil.
- Akun yang ditemukan: AWS akun yang dipantau di bawah penemuan sumber daya. Jika Anda telah mengintegrasikan IPAM dengan AWS Organizations, semua akun di organisasi adalah akun yang ditemukan.
  - ID Akun — ID akun.
  - Wilayah — AWS Wilayah tempat informasi akun dikembalikan.
  - Waktu penemuan terakhir yang dicoba — Waktu penemuan sumber daya terakhir yang dicoba.
  - Waktu penemuan sukses terakhir — Waktu penemuan sumber daya terakhir yang berhasil.
  - Status — Alasan kegagalan penemuan sumber daya.
- Wilayah operasi — Wilayah operasi untuk penemuan sumber daya.
- Berbagi sumber daya — Jika penemuan sumber daya telah dibagikan, ARN berbagi sumber daya terdaftar.

- Pembagian sumber daya ARN — Pembagian sumber daya ARN.
- Status — Status saat ini dari pembagian sumber daya. Nilai yang mungkin adalah:
  - Aktif — Berbagi sumber daya aktif dan tersedia untuk digunakan.
  - Dihapus - Berbagi sumber daya dihapus dan tidak lagi tersedia untuk digunakan.
  - Tertunda — Undangan untuk menerima pembagian sumber daya sedang menunggu tanggapan.
- Dibuat di — Saat pembagian sumber daya dibuat.

- Tag — Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tag untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

- Lihat detail penemuan sumber daya: describe-ipam-resource-discovery

Bagikan penemuan sumber daya

Ikuti langkah-langkah di bagian ini untuk membagikan penemuan sumber daya menggunakanAWS Resource Access Manager. Untuk informasi selengkapnyaAWS RAM, lihat Berbagi AWS sumber daya Anda di Panduan AWS RAM Pengguna.

> **Note**
>
> Membuat, berbagi, dan mengaitkan penemuan sumber daya adalah bagian dari proses mengintegrasikan IPAM dengan akun di luar organisasi Anda (lihat). Integrasikan IPAM dengan akun di luar organisasi Jika Anda tidak membuat IPAM dan mengintegrasikannya dengan akun di luar organisasi Anda, Anda tidak perlu membuat, berbagi, atau mengaitkan penemuan sumber daya.

Saat Anda membuat IPAM yang memantau akun di luar organisasi Anda, Akun Admin Org Sekunder membagikan penemuan sumber dayanya dengan Akun IPAM Org Utama menggunakan. AWS RAM Anda harus terlebih dahulu membagikan penemuan sumber daya dengan Akun IPAM Org Utama

sebelum Akun IPAM Org Utama dapat mengaitkan penemuan sumber daya dengan IPAM mereka. Untuk informasi lebih lanjut tentang peran yang terlibat dalam proses ini, lihatGambaran umum proses.

> **Note**
>
> - Saat Anda membuat pembagian sumber daya menggunakan AWS RAM untuk berbagi penemuan sumber daya, Anda harus membuat pembagian sumber daya di Wilayah beranda IPAM Org Utama.
> - Akun yang membuat dan menghapus pembagian sumber daya untuk penemuan sumber daya harus memiliki izin berikut dalam kebijakan IAM mereka:
>   - EC2: PutResourcePolicy
>   - EC2: DeleteResourcePolicy

Jika Anda mengintegrasikan IPAM dengan akun di luar organisasi Anda, ini adalah langkah wajib yang harus diselesaikan oleh Akun Admin Org Sekunder.

AWS Management Console

Untuk berbagi penemuan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Penemuan sumber daya.
3. Pilih tab Berbagi sumber daya.
4. Pilih Buat berbagi sumber daya. AWS RAMKonsol terbuka, di mana Anda akan membuat pembagian sumber daya.
5. Di AWS RAM konsol, pilih Pengaturan.
6. Pilih Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.
7. Pilih Buat berbagi sumber daya.
8. Tambahkan Nama untuk sumber daya bersama.
9. Di bawah Pilih jenis sumber daya, pilih IPAM Resource Discovery, dan pilih penemuan sumber daya.
10. Pilih Selanjutnya.

11. Di bawah Izin asosiasi, Anda dapat melihat izin default yang akan diaktifkan untuk prinsipal yang diberikan akses ke pembagian sumber daya ini:
    - AWSRAMPermissionIpamResourceDiscovery
    - Tindakan yang diizinkan oleh izin ini:
      - EC2: AssociateIpamResourceDiscovery
      - EC2: GetIpamDiscoveredAccounts
      - EC2: GetIpamDiscoveredPublicAddresses
      - EC2: GetIpamDiscoveredResourceCidrs
12. Tentukan prinsipal yang diizinkan mengakses sumber daya bersama. Untuk Prinsipal, pilih Akun IPAM Org Utama, lalu pilih Tambah.
13. Pilih Selanjutnya.
14. Tinjau opsi berbagi sumber daya dan prinsipal yang akan Anda bagikan. Kemudian pilih Buat berbagi sumber daya.
15. Setelah penemuan sumber daya dibagikan, itu harus diterima oleh Akun IPAM Org Utama dan kemudian dikaitkan dengan IPAM oleh Akun IPAM Org Utama. Untuk informasi selengkapnya, lihat Kaitkan penemuan sumber daya dengan IPAM.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

1. Buat berbagi sumber daya: create-resource-share
2. Lihat bagian sumber daya: get-resource-shares

Kaitkan penemuan sumber daya dengan IPAM

Bagian ini menjelaskan cara mengaitkan penemuan sumber daya dengan IPAM. Saat Anda mengaitkan penemuan sumber daya dengan IPAM, IPAM memantau semua CIDR sumber daya dan akun yang ditemukan di bawah penemuan sumber daya. Saat Anda membuat IPAM, penemuan sumber daya default dibuat untuk IPAM Anda dan secara otomatis dikaitkan dengan IPAM Anda.

Kuota default untuk asosiasi penemuan sumber daya adalah 5. Untuk informasi selengkapnya (termasuk cara menyesuaikan kuota ini), lihatKuota untuk IPAM Anda.

> **Note**
>
> Membuat, berbagi, dan mengaitkan penemuan sumber daya adalah bagian dari proses mengintegrasikan IPAM dengan akun di luar organisasi Anda (lihat). Integrasikan IPAM dengan akun di luar organisasi Jika Anda tidak membuat IPAM dan mengintegrasikannya dengan akun di luar organisasi Anda, Anda tidak perlu membuat, berbagi, atau mengaitkan penemuan sumber daya.

Jika Anda mengintegrasikan IPAM dengan akun di luar organisasi Anda, ini adalah langkah wajib yang harus diselesaikan oleh Akun IPAM Org Utama. Untuk informasi lebih lanjut tentang peran yang terlibat dalam proses ini, lihatGambaran umum proses.

AWS Management Console

Untuk mengaitkan penemuan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih iPAMS.
3. Pilih Penemuan terkait, lalu pilih Penemuan sumber daya asosiasi.
4. Di bawah penemuan sumber daya IPAM, pilih penemuan sumber daya yang telah dibagikan dengan Anda oleh Akun Admin Org Sekunder.
5. Pilih Kaitkan.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

- Kaitkan penemuan sumber daya: associate-ipam-resource-discovery

Putuskan penemuan sumber daya

Bagian ini menjelaskan cara memisahkan penemuan sumber daya dari IPAM. Ketika Anda memisahkan penemuan sumber daya dari IPAM, IPAM tidak lagi memantau semua CIDR sumber daya dan akun yang ditemukan di bawah penemuan sumber daya.

> **Note**
>
> Anda tidak dapat memisahkan asosiasi penemuan sumber daya default. Asosiasi penemuan sumber daya default adalah asosiasi yang dibuat secara otomatis saat Anda membuat IPAM. Namun, asosiasi penemuan sumber daya default akan dihapus jika Anda menghapus IPAM.

Langkah ini harus diselesaikan oleh Akun IPAM Org Utama. Untuk informasi lebih lanjut tentang peran yang terlibat dalam proses ini, lihatGambaran umum proses.

AWS Management Console

Untuk memisahkan penemuan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih iPAMS.
3. Pilih Penemuan terkait, lalu pilih Putuskan penemuan sumber daya.
4. Di bawah penemuan sumber daya IPAM, pilih penemuan sumber daya yang telah dibagikan dengan Anda oleh Akun Admin Org Sekunder.
5. Pilih Pisahkan.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

- Untuk memisahkan penemuan sumber daya: disassociate-ipam-resource-discovery

Hapus penemuan sumber daya

Bagian ini menjelaskan cara menghapus penemuan sumber daya.

> **Note**
>
> Anda tidak dapat menghapus penemuan sumber daya default. Penemuan sumber daya default adalah penemuan yang dibuat secara otomatis saat Anda membuat IPAM. Namun, penemuan sumber daya default akan dihapus jika Anda menghapus IPAM.

Langkah ini harus diselesaikan oleh Akun Admin Org Sekunder. Untuk informasi lebih lanjut tentang peran yang terlibat dalam proses ini, lihatGambaran umum proses.

AWS Management Console

Untuk menghapus penemuan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Penemuan sumber daya.
3. Pilih penemuan sumber daya dan pilih Tindakan > Hapus penemuan sumber daya.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

- Untuk menghapus penemuan sumber daya: delete-ipam-resource-discovery

Buat cakupan tambahan

Ikuti langkah-langkah dalam bagian ini untuk membuat cakupan tambahan.

Ruang lingkup adalah wadah tingkat tertinggi dalam IPAM. Saat Anda membuat IPAM, IPAM membuat dua cakupan default untuk Anda. Setiap ruang lingkup mewakili ruang IP untuk satu jaringan. Ruang lingkup pribadi ditujukan untuk semua ruang pribadi. Ruang lingkup publik ditujukan untuk semua ruang publik. Cakupan memungkinkan Anda untuk menggunakan kembali alamat IP di beberapa jaringan yang tidak terhubung tanpa menyebabkan tumpang tindih alamat IP atau konflik.

Saat Anda membuat IPAM, cakupan default (satu pribadi dan satu publik) dibuat untuk Anda. Anda dapat membuat cakupan pribadi tambahan. Anda tidak dapat membuat cakupan publik tambahan.

Anda dapat membuat cakupan pribadi tambahan jika memerlukan dukungan untuk beberapa jaringan pribadi yang terputus. Cakupan pribadi tambahan memungkinkan Anda membuat kumpulan dan mengelola sumber daya yang menggunakan ruang IP yang sama.

> **Important**
>
> Jika IPAM menemukan sumber daya dengan CIDR IPv4 pribadi, CIDR sumber daya diimpor ke cakupan pribadi default dan tidak muncul dalam cakupan pribadi tambahan yang Anda

buat. Anda dapat memindahkan CIDR dari lingkup pribadi default ke lingkup pribadi lain. Untuk informasi, lihat Memindahkan CIDR VPC antar cakupan.

AWS Management Console

Untuk membuat cakupan privat tambahan

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Lingkup.
3. Pilih Buat cakupan.
4. Pilih IPAM yang ingin Anda tambahkan ruang lingkup.
5. Tambahkan deskripsi untuk lingkup.
6. Pilih Buat cakupan.
7. Anda dapat melihat cakupan di IPAM dengan memilih Lingkup di panel navigasi.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk membuat cakupan pribadi tambahan:

1. Lihat cakupan Anda saat ini: describe-ipam-scopes
2. Buat cakupan pribadi baru: create-ipam-scope
3. Lihat cakupan Anda saat ini untuk melihat cakupan baru: describe-ipam-scopes

Memindahkan CIDR VPC antar cakupan

Ikuti langkah-langkah di bagian ini untuk memindahkan CIDR VPC dari satu lingkup ke lingkup lainnya.

⚠ Important

- Anda hanya dapat memindahkan CIDR VPC. Saat Anda memindahkan CIDR VPC, CIDR subnet VPC akan dipindahkan secara otomatis juga.

- Anda hanya dapat memindahkan CIDR VPC dari satu lingkup pribadi ke yang lain. Anda tidak dapat memindahkan CIDR VPC dari ruang lingkup publik ke ruang lingkup pribadi atau dari ruang lingkup pribadi ke ruang lingkup publik.
- AWSAkun yang sama harus memiliki kedua cakupan.
- Jika CIDR VPC saat ini dialokasikan dari pangkalan dalam lingkup pribadi, permintaan pemindahan berhasil, tetapi CIDR VPC tidak akan dipindahkan sampai Anda melepaskan alokasi VPC CIDR dari pangkalan saat ini. Untuk informasi tentang merilis alokasi, lihat Merilis alokasi.

AWS Management Console

Untuk memindahkan CIDR dialokasikan ke VPC

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Sumber Daya.
3. Dari menu tarik-turun pada bagian atas panel konten, pilih scope yang ingin Anda gunakan.
4. Pada panel konten, pilih VPC dan sumber VPC sumber sumber
5. Di bawah VPC CIDR, pilih salah satu CIDR yang dialokasikan ke sumber daya dan pilih Actions > Move CIDR ke scope yang berbeda.
6. Pilih ruang lingkup yang ingin Anda pindahkan yaitu sumber sumber sumber sumber sumber sumber sumber sumber VPC sumber sumber sumber sumber sumber sumber sumber.
7. Pilih Pindahkan CIDR ke lingkup yang berbeda.

Command line

GunakanAWS CLI perintah berikut untuk memindahkan CIDR VPC:

1. Dapatkan CIDR VPC dalam lingkup saat ini: get-ipam-resource-cidrs
2. Pindahkan CIDR VPC: modify-ipam-resource-cidr
3. Dapatkan CIDR VPC di lingkup lainnya: get-ipam-resource-cidrs

Ubah status pemantauan CIDR VPC

Ikuti langkah-langkah di bagian ini untuk mengubah status pemantauan CIDR VPC. Anda mungkin ingin mengubah CIDR VPC dari yang dipantau menjadi diabaikan jika Anda tidak ingin IPAM mengelola atau memantau VPC dan mengizinkan CIDR yang dialokasikan ke VPC tersedia untuk digunakan. Anda mungkin ingin mengubah CIDR VPC dari diabaikan menjadi dipantau jika Anda ingin IPAM mengelola dan memantau CIDR VPC.

> **Note**
>
> - Anda tidak dapat mengabaikan CIDR VPC di ruang lingkup publik.
> - Jika CIDR diabaikan, Anda masih dikenakan biaya untuk alamat IP aktif di CIDR. Untuk informasi selengkapnya, lihat Harga untuk IPAM.
> - Jika CIDR diabaikan, Anda masih dapat melihat riwayat alamat IP di CIDR. Untuk informasi selengkapnya, lihat Lihat riwayat alamat IP.

Anda dapat mengubah status pemantauan CIDR VPC menjadi dipantau atau diabaikan:

- Dipantau: VPC CIDR telah terdeteksi oleh IPAM dan sedang dipantau untuk tumpang tindih dengan CIDR lain dan kepatuhan aturan alokasi.
- Diabaikan: CIDR VPC telah dipilih untuk dibebaskan dari pemantauan. CIDR VPC yang diabaikan tidak dievaluasi untuk tumpang tindih dengan CIDR lain atau kepatuhan aturan Alokasi. Setelah CIDR VPC dipilih untuk diabaikan, ruang apa pun yang dialokasikan kepadanya dari kolam IPAM dikembalikan ke kolam dan CIDR VPC tidak akan diimpor lagi melalui impor otomatis (jika aturan Alokasi impor otomatis diatur di kolam).

AWS Management Console

Untuk mengubah status pemantauan CIDR yang dialokasikan ke VPC

1. Buka konsol IPAM dihttps://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Sumber Daya.
3. Dari menu tarik-turun di bagian atas panel konten, pilih ruang lingkup pribadi yang ingin Anda gunakan.
4. Di panel konten, pilih VPC dan lihat detail VPC.

5. Di bawahVPC CIDR, pilih salah satu CIDR yang dialokasikan ke VPC dan pilihTindakan>Tandai sebagai diabaikanatauHapus tanda sebagai diabaikan.
6. PilihTandai sebagai diabaikanatauHapus tanda sebagai diabaikan.

Command line

Gunakan yang berikutAWS CLIperintah untuk mengubah status pemantauan CIDR VPC:

1. Dapatkan ID lingkup:describe-ipam-scopes
2. Lihat status pemantauan saat ini untuk VPC CIDR:get-ipam-resource-cidrs
3. Ubah status CIDR VPC:modify-ipam-resource-cidr
4. Lihat status pemantauan baru untuk VPC CIDR:get-ipam-resource-cidrs

Menghapus cakupan

Ikuti langkah-langkah dalam bagian ini untuk menghapus cakupan IPAM.

Important

Anda tidak dapat menghapus cakupan jika salah satu hal berikut ini benar:

- Ruang lingkup adalah lingkup default. Saat Anda membuat IPAM, dua cakupan default (satu publik, satu pribadi) dibuat secara otomatis, dan tidak dapat dihapus. Untuk melihat apakah ruang lingkup adalah cakupan default, lihat jenis Cakupan dalam rincian cakupan.
- Ada satu atau lebih kolam dalam ruang lingkup. Anda harus terlebih dahuluMenghapus kolam kolam kolam kolam kolam kolam renang sebelum Anda dapat menghapus cakupan.

AWS Management Console

Untuk menghapus cakupan

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Cakupan.
3. Di panel konten, pilih cakupan yang ingin Anda hapus.
4. Pilih Tindakan > Hapus cakupan.

5. Masukkan**`delete`** dan kemudian pilih Hapus.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk menghapus ruang lingkup:

1. Lihat cakupan: describe-ipam-scopes
2. Menghapus cakupan: delete-ipam-scope
3. Lihat cakupan yang diperbarui: describe-ipam-scopes

Untuk membuat cakupan baru, lihatBuat cakupan tambahan. Untuk menghapus IPAM, lihatMenghapus IPAM.

Rilis alokasi yang berbeda.

Ikuti langkah-langkah di bagian ini untuk melepaskan alokasi CIDR dari pool IPAM. Alokasi adalah tugas CIDR dari kumpulan IPAM ke sumber daya lain atau kumpulan IPAM.

Jika Anda berencana untuk menghapus pool, Anda mungkin perlu melepaskan alokasi pool. Anda tidak dapat menghapus kumpulan jika kumpulan memiliki CIDR yang disediakan, dan Anda tidak dapat membatalkan CIDR jika CIDR dialokasikan ke sumber daya.

> **Note**
>
> - Untuk melepaskan alokasi manual, gunakan langkah-langkah di bagian ini atau panggil ReleaseIpamPoolAllocation API.
> - Untuk melepaskan alokasi dalam lingkup pribadi, Anda harus mengabaikan atau menghapus CIDR sumber daya. Untuk informasi selengkapnya, lihat Ubah status pemantauan CIDR VPC. Setelah beberapa waktu, Amazon VPC IPAM akan secara otomatis merilis alokasi atas nama Anda.
>
> Example
>
> Contoh

Jika Anda memiliki CIDR VPC dalam lingkup pribadi, untuk melepaskan alokasi Anda harus mengabaikan atau menghapus CIDR VPC. Setelah beberapa waktu, Amazon VPC IPAM akan secara otomatis merilis alokasi VPC CIDR dari kumpulan IPAM.

- Untuk melepaskan alokasi dalam lingkup publik, Anda harus menghapus CIDR sumber daya. Anda tidak dapat mengabaikan CIDR sumber daya publik. Untuk informasi selengkapnya, lihat Pembersihan diBawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS atau Pembersihan diBawa IPv6 CIDR Anda sendiri ke IPAM hanya menggunakan CLI AWS. Setelah beberapa waktu, Amazon VPC IPAM akan secara otomatis merilis alokasi atas nama Anda.

Agar Amazon VPC IPAM merilis alokasi atas nama Anda, semua izin akun harus dikonfigurasi dengan benar untuk penggunaan akun tunggal atau penggunaan multi-akun.

Saat Anda merilis CIDR yang dikelola oleh IPAM Anda, Amazon VPC IPAM mendaur ulang CIDR kembali ke kumpulan IPAM. Dibutuhkan waktu beberapa menit untuk CIDR untuk menjadi tersedia untuk alokasi future yang akan datang. Untuk informasi lebih lanjut tentang kumpulan dan alokasi, lihatCara kerja IPAM.

AWS Management Console

Untuk melepaskan alokasi kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Pada panel navigasi, pilih Pools.
3. Pada bagian atas panel konten, pilih scope yang ingin Anda gunakan pada bagian atas panel konten yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Pada panel konten, pilih pool yang dialokasikan alokasi tersebut.
5. Pilih tab Alokasi.
6. Pilih satu atau beberapa alokasi yang berbeda. Anda dapat mengidentifikasi alokasi berdasarkan jenis Resource mereka:
   - kustom: Sebuah alokasi kustom.
   - vpc: Alokasi VPC.

- ipam-pool: Alokasi kolam IPAM.
- ec2-public-ipv4-pool: Alokasi kolam IPv4 publik.

7. Pilih Tindakan > Lepaskan alokasi khusus.
8. Pilih Deallocate CIDR.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk melepaskan alokasi pool:

1. Dapatkan ID kolam IPAM: describe-ipam-pools
2. Lihat alokasi Anda saat ini di pool: get-ipam-pool-allocations
3. Lepaskan alokasi: release-ipam-pool-allocation
4. Lihat alokasi Anda yang diperbarui: get-ipam-pool-allocations

Untuk menambahkan alokasi baru, lihatAlokasikan CIDR. Untuk menghapus pangkalan setelah melepaskan alokasi, Anda harus terlebih dahuluDeprovision CIDR dari kolam.

Memodifikasi IPAM

Ikuti langkah-langkah di bagian ini untuk memodifikasi IPAM.

Daftar Isi

- Ubah tingkat IPAM
- Ubah Wilayah operasi IPAM

Ubah tingkat IPAM

Ikuti langkah-langkah di bagian ini untuk memodifikasi tingkat IPAM. IPAM menawarkan dua tingkatan: Tingkat Gratis dan Tingkat Lanjut. Untuk informasi selengkapnya tentang fitur yang tersedia di Tingkat Gratis dan biaya yang terkait dengan Tingkat Lanjut, lihat tab IPAM di halaman harga Amazon VPC.

Important

Sebelum Anda dapat beralih dari Tingkat Lanjut ke Tingkat Gratis, Anda harus:

- Hapus kolam lingkup pribadi.
- Hapus cakupan pribadi non-default.
- Hapus kolam dengan lokal yang berbeda dari Wilayah rumah IPAM.
- Hapus asosiasi penemuan sumber daya non-default.
- Hapus alokasi pool ke akun yang bukan pemilik IPAM.

AWS Management Console

Untuk memodifikasi tingkat IPAM

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih iPAMS.
3. Di panel konten, pilih IPAM Anda.
4. Pilih Tindakan > Edit.
5. Pilih tingkat IPAM yang ingin Anda gunakan untuk IPAM.
6. Pilih Save changes (Simpan perubahan).

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk melihat dan memodifikasi tingkat IPAM:

1. Lihat iPAM saat ini: deskripsikan-ipams
2. Ubah tingkat IPAM: modify-ipam
3. Lihat iPAM Anda yang diperbarui: deskripsikan-ipams

Ubah Wilayah operasi IPAM

Ikuti langkah-langkah di bagian ini untuk memodifikasi Wilayah operasi IPAM. Wilayah Operasi adalah AWS Wilayah di mana IPAM diizinkan untuk mengelola CIDR alamat IP. IPAM hanya menemukan dan memantau sumber daya di AWS Wilayah yang Anda pilih sebagai Wilayah operasi.

AWS Management Console

Untuk memodifikasi Wilayah operasi IPAM

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih iPAMS.
3. Di panel konten, pilih IPAM Anda.
4. Pilih Tindakan > Edit.
5. Di bawah pengaturan IPAM, pilih Wilayah Operasi yang ingin Anda gunakan untuk IPAM.
6. Pilih Save changes (Simpan perubahan).

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk melihat dan memodifikasi Kawasan operasi IPAM:

1. Lihat iPAM saat ini: deskripsikan-ipams
2. Menambah atau menghapus Kawasan operasi IPAM: modify-ipam
3. Lihat iPAM Anda yang diperbarui: deskripsikan-ipams

Menghapus IPAM

Ikuti langkah-langkah dalam bagian ini untuk menghapus IPAM. Untuk informasi tentang peningkatan jumlah default IPAM yang dapat Anda miliki daripada menghapus IPAM yang ada, lihatKuota untuk IPAM Anda.

> **Important**
>
> Menghapus IPAM menghapus semua data yang dipantau terkait dengan IPAM termasuk data historis untuk CIDR.

AWS Management Console

Untuk menghapus IPAM

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih IPAM.
3. Di panel konten, pilih IPAM Anda.
4. Pilih Tindakan > Hapus IPAM.
5. Lakukan salah satu dari berikut:

   - Pilih Hapus kaskade untuk menghapus IPAM, cakupan pribadi, kumpulan dalam cakupan pribadi, dan alokasi apa pun di kumpulan dalam cakupan pribadi. Anda tidak dapat menghapus IPAM dengan opsi ini jika ada pool dalam lingkup publik Anda. Jika Anda menggunakan opsi ini, IPAM melakukan hal berikut:
     - Deallocates setiap CIDR dialokasikan untuk sumber daya VPC (seperti VPC) di kolam renang dalam lingkup pribadi.

       > **Note**
       >
       > Tidak ada sumber daya VPC yang dihapus sebagai hasil dari mengaktifkan opsi ini. CIDR yang terkait dengan sumber daya tidak akan lagi dialokasikan dari kumpulan IPAM, tetapi CIDR itu sendiri akan tetap tidak berubah.

     - Deprovisions semua CIDR IPv4 yang disediakan untuk kumpulan IPAM dalam lingkup pribadi.
     - Menghapus semua kumpulan IPAM dalam lingkup pribadi.
     - Menghapus semua cakupan pribadi non-default di IPAM.
     - Menghapus cakupan publik dan pribadi default dan IPAM.
   - Jika Anda tidak memilih kotak centang Cascade delete, sebelum Anda dapat menghapus IPAM, Anda harus melakukan hal berikut:

- Melepaskan alokasi dalam kolam IPAM. Untuk informasi selengkapnya, lihat Rilis alokasi yang berbeda..
- Deprovisioned CIDR yang disediakan untuk pool dalam IPAM. Untuk informasi selengkapnya, lihat Deprovision CIDR dari kolam.
- Hapus cakupan non-default tambahan. Untuk informasi selengkapnya, lihat Menghapus cakupan.
- Hapus kumpulan IPAM Anda. Untuk informasi selengkapnya, lihat Menghapus kolam kolam kolam kolam kolam kolam renang.

6. Masukkan**`delete`** dan kemudian pilih Hapus.

Command line

Perintah di bagian ini menautkan ke dokumentasi ReferensiAWS CLI. Dokumentasi menyediakan deskripsi rinci tentang pilihan yang dapat Anda gunakan ketika Anda menjalankan perintah.

GunakanAWS CLI perintah berikut untuk menghapus IPAM:

1. Lihat IPAM saat ini: deskripsikan-ipams
2. Menghapus IPAM: menghapus-ipam
3. Lihat IPAM Anda yang diperbarui: deskripsikan-ipams

Untuk membuat IPAM baru, lihatBuat IPAM.

Melacak penggunaan alamat IP di IPAM

Tugas yang dijelaskan di bagian ini bersifat opsional. Jika Anda ingin menyelesaikan tugas di bagian ini, dan Anda telah mendelegasikan akun IPAM, tugas harus diselesaikan oleh akun IPAM.

Ikuti langkah-langkah di bagian ini untuk melacak penggunaan alamat IP dengan IPAM.

Konten

- Memantau penggunaan CIDR dengan dasbor IPAM
- Pantau penggunaan CIDR berdasarkan sumber daya
- Pantau IPAM dengan Amazon CloudWatch
- Lihat riwayat alamat IP
- Lihat wawasan IP publik

Memantau penggunaan CIDR dengan dasbor IPAM

Ikuti langkah-langkah di bagian ini untuk mengakses dasbor IPAM dan melihat status semua CIDR dalam lingkup IPAM tertentu.

AWS Management Console

Untuk memantau penggunaan CIDR menggunakan dasbor IPAM

1. Buka konsol IPAM dihttps://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Dasbor.
3. Secara default, saat Anda melihat dasbor, lingkup pribadi default dipilih. Jika Anda tidak ingin menggunakan lingkup pribadi default, dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi selengkapnya tentang cakupan, lihatCara kerja IPAM.
4. Dasbor menyajikan ikhtisar kolam IPAM dan CIDR Anda dalam lingkup. Anda dapat menambahkan, menghapus, mengubah ukuran, dan memindahkan widget untuk menyesuaikan dasbor.

    - Ruang lingkup: Rincian untuk lingkup ini. Ruang lingkup adalah wadah tingkat tertinggi dalam IPAM. IPAM berisi dua cakupan default, satu pribadi dan satu publik. Setiap ruang

lingkup mewakili ruang IP untuk satu jaringan. Anda mungkin memiliki beberapa cakupan pribadi, tetapi Anda hanya dapat memiliki satu ruang lingkup publik.

- ID Cakupan: ID untuk lingkup ini.
- Jenis lingkup: Jenis ruang lingkup.
- IPAM: ID IPAM tempat lingkup berada.
- Kumpulan IPAM dalam lingkup ini: ID IPAM tempat lingkup berada.
- Melihat sumber daya jaringan dalam lingkup ini: Membawa Anda keSumber Dayabagian dari konsol IPAM.
- Mencari riwayat alamat IP dalam lingkup ini: Membawa Anda keCari riwayat IPbagian dari konsol IPAM.

- Jenis sumber daya CIDR: Jenis-jenis CIDR sumber daya dalam lingkup.
  - Subnet: Jumlah CIDR untuk subnet.
  - VPC: Jumlah CIDR untuk VPC.
  - EIP: Jumlah CIDR untuk alamat IP Elastic.
  - Kolam IPv4 publik: Jumlah CIDR untuk kolam IPv4 publik.
- Negara manajemen: Keadaan manajemen CIDR.
  - CIDR yang tidak dikelola: Jumlah CIDR sumber daya untuk sumber daya tidak terkelola dalam lingkup ini.
  - CIDR yang diabaikan: Jumlah CIDR sumber daya yang telah Anda pilih untuk dibebaskan dari pemantauan dengan IPAM dalam lingkup. IPAM tidak mengevaluasi sumber daya yang diabaikan untuk tumpang tindih atau kepatuhan dalam lingkup. Ketika sumber daya dipilih untuk diabaikan, setiap ruang yang dialokasikan untuk itu dari pangkalan IPAM dikembalikan ke pangkalan, dan sumber daya tidak akan diimpor lagi melalui impor otomatis (jika aturan alokasi impor otomatis diatur di pangkalan).
  - CIDR yang Dikelola: Jumlah CIDR sumber daya untuk sumber daya yang dapat dikelola (VPC atau kumpulan IPv4 publik) yang dialokasikan dari kumpulan IPAM dalam lingkup.
- Tumpang tindih CIDRs sumber daya: Jumlah CIDR yang tumpang tindih dan tidak tumpang tindih. CIDR yang tumpang tindih dapat menyebabkan perutean yang salah di VPC Anda.
  - Tumpang tindih CIDRs: Jumlah CIDR yang saat ini tumpang tindih dalam kumpulan IPAM dalam lingkup ini. CIDR yang tumpang tindih dapat menyebabkan perutean yang salah di VPC Anda.
  - CIDR yang tidak tumpang tindih: Jumlah CIDR sumber daya yang tidak tumpang tindih dalam kumpulan IPAM dalam lingkup ini.

- CIDR sumber daya yang sesuai: Jumlah CIDR sumber daya compliant.
  - CIDR Compliant: Jumlah CIDR sumber daya yang mematuhi aturan alokasi untuk kumpulan IPAM dalam lingkup.
  - CIDR yang tidak patuh: Jumlah CIDR sumber daya yang tidak mematuhi aturan alokasi untuk kumpulan IPAM dalam ruang lingkup.
- Status tumpang tindih: Jumlah CIDR yang tumpang tindih dari waktu ke waktu.
  - OverlappingResourceCidrs: Jumlah CIDR yang tumpang tindih dalam kolam IPAM dalam lingkup ini. CIDR yang tumpang tindih dapat menyebabkan perutean yang salah di VPC Anda.
- Status kepatuhan: Jumlah CIDR yang mematuhi versus tidak mematuhi aturan alokasi untuk kumpulan IPAM dalam lingkup dari waktu ke waktu.
  - CompliantResourceCidrs: Jumlah CIDR sumber daya yang mematuhi aturan alokasi.
  - NoncompliantResourceCidrs: Jumlah CIDR sumber daya yang tidak sesuai dengan aturan alokasi.
- Pemanfaatan VPC: VPC (IPv4 dan IPv6) dengan pemanfaatan IP tertinggi atau terendah. Anda dapat menggunakan informasi ini untuk mengonfigurasi AmazonCloudWatchalarm yang akan diperingatkan jika ambang batas pemanfaatan IP dilanggar. Untuk informasi selengkapnya, lihat Metrik pemanfaatan sumber daya.
- Pemanfaatan subnet: Subnet (hanya IPv4) dengan pemanfaatan IP tertinggi atau terendah. Anda dapat menggunakan informasi ini untuk memutuskan apakah Anda ingin menyimpan atau menghapus sumber daya yang kurang dimanfaatkan. Untuk informasi selengkapnya, lihat Metrik pemanfaatan sumber daya.
- VPC dengan IP tertinggi dialokasikan: VPC yang memiliki persentase ruang alamat IP tertinggi yang dialokasikan untuk subnet. Ini berguna untuk menunjukkan kepada Anda jika Anda perlu menyediakan ruang alamat IP tambahan ke VPC.
- Subnet dengan IP tertinggi dialokasikan: Subnet yang memiliki persentase tertinggi ruang alamat IP yang dialokasikan untuk sumber daya. Ini berguna untuk menunjukkan kepada Anda jika Anda perlu menyediakan ruang alamat IP tambahan ke subnet.
- Penugasan kolam: Persentase ruang IP yang telah ditetapkan ke sumber daya dan alokasi manual dalam lingkup dari waktu ke waktu.
- Alokasi kolam: Persentase ruang IP pool yang telah dialokasikan ke pool lain dalam lingkup dari waktu ke waktu.

Command line

Informasi yang ditampilkan di dasbor berasal dari metrik yang disimpan di AmazonCloudWatch. Untuk informasi selengkapnya tentang metrik yang disimpan di AmazonCloudWatch, lihatPantau IPAM dengan Amazon CloudWatch. Gunakan AmazonCloudWatchpilihan diAWSReferensi CLIuntuk melihat metrik alokasi di kumpulan dan cakupan IPAM Anda.

Jika Anda menemukan bahwa CIDR yang disediakan untuk pool hampir sepenuhnya dialokasikan, Anda mungkin perlu menyediakan CIDR tambahan. Untuk informasi selengkapnya, lihat Menyediakan CIDR ke kolam.

Pantau penggunaan CIDR berdasarkan sumber daya

Dalam IPAM, sumber daya adalah entitas AWS layanan yang diberi alamat IP atau blok CIDR. IPAM mengelola beberapa sumber daya, tetapi hanya memantau sumber daya lainnya.

- Sumber daya terkelola: Sumber daya terkelola memiliki CIDR yang dialokasikan dari kolam IPAM. IPAM memantau CIDR untuk potensi alamat IP yang tumpang tindih dengan CIDR lain di kolam renang, dan memantau kepatuhan CIDR dengan aturan alokasi kumpulan. IPAM mendukung pengelolaan jenis sumber daya berikut:
  - VPC
  - Kolam IPv4 publik

    Important

    Kolam IPv4 publik dan kolam IPAM dikelola oleh sumber daya yang berbeda di. AWS Pool IPv4 publik adalah sumber daya akun tunggal yang memungkinkan Anda mengonversi CIDR milik publik ke alamat IP Elastis. Kolam IPAM dapat digunakan untuk mengalokasikan ruang publik Anda ke kolam IPv4 publik.
- Sumber daya yang dipantau: Jika sumber daya dipantau oleh IPAM, sumber daya telah terdeteksi oleh IPAM dan Anda dapat melihat detail tentang CIDR sumber daya saat Anda menggunakan AWS CLI, atau saat Anda melihat Sumber Daya **`get-ipam-resource-cidrs`** di panel navigasi. IPAM mendukung pemantauan sumber daya berikut:
  - VPC
  - Kolam IPv4 publik
  - Subnet VPC

- Alamat IP elastis

Langkah-langkah berikut menunjukkan kepada Anda cara memantau penggunaan CIDR dan kepatuhan aturan alokasi berdasarkan sumber daya.

AWS Management Console

Untuk memantau penggunaan CIDR berdasarkan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Sumber Daya.
3. Dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Gunakan peta CIDR sumber daya untuk melihat ruang alamat IP yang tersedia, dialokasikan, dan tumpang tindih dalam cakupan:

   - Tersedia: Rentang alamat IP tersedia untuk alokasi.
   - Sesuai dan tidak tumpang tindih: Rentang alamat IP dialokasikan ke sumber daya yang dikelola oleh IPAM.
   - Diduduki: Rentang alamat IP dialokasikan ke sumber daya.
   - Tumpang tindih: Rentang alamat IP telah dialokasikan ke beberapa sumber daya dan tumpang tindih.
   - Noncompliant: Rentang alamat IP tidak sesuai. Ada sumber daya yang menggunakan rentang alamat IP yang tidak sesuai dengan aturan alokasi yang disiapkan untuk kumpulan.

   Di peta CIDR, pilih blok alamat IP di bagian bawah peta untuk melihat sumber daya di blok CIDR yang lebih kecil. Pilih blok alamat IP di bagian atas peta untuk melihat sumber daya di blok CIDR yang lebih besar.
5. Dalam tabel, Anda dapat melihat detail berikut tentang sumber daya dalam ruang lingkup:

   - Nama (ID Sumber Daya): Nama dan ID sumber daya sumber daya.
   - CIDR: CIDR terkait dengan sumber daya.
   - Status manajemen: Keadaan sumber daya.

    - Dikelola: Sumber daya memiliki CIDR yang dialokasikan dari kolam IPAM dan sedang dipantau oleh IPAM untuk potensi tumpang tindih CIDR dan kepatuhan terhadap aturan alokasi kumpulan.
    - Tidak dikelola: Sumber daya tidak memiliki CIDR yang dialokasikan dari kolam IPAM dan tidak dipantau oleh IPAM untuk potensi kepatuhan CIDR dengan aturan alokasi kumpulan. CIDR dipantau untuk tumpang tindih.
    - Diabaikan: Sumber daya telah dipilih untuk dibebaskan dari pemantauan. Sumber daya yang diabaikan tidak dievaluasi untuk kepatuhan aturan tumpang tindih atau alokasi. Ketika sumber daya dipilih untuk diabaikan, setiap ruang yang dialokasikan kepadanya dari kolam IPAM dikembalikan ke kolam dan sumber daya tidak akan diimpor lagi melalui impor otomatis (jika aturan alokasi impor otomatis disetel di kolam).
    - -: Sumber daya ini bukan salah satu jenis sumber daya yang dapat dikelola IPAM.
- Status kepatuhan: Status kepatuhan CIDR.
    - Sesuai: Sumber daya yang dikelola mematuhi aturan alokasi kolam IPAM.
    - Tidak patuh: CIDR sumber daya tidak mematuhi satu atau lebih aturan alokasi kumpulan IPAM.

      Example

      Jika VPC memiliki CIDR yang tidak memenuhi parameter panjang netmask dari kolam IPAM, atau jika sumber daya tidak berada di AWS Wilayah yang sama dengan kolam IPAM, itu akan ditandai sebagai tidak sesuai.
    - Tidak dikelola: Sumber daya tidak memiliki CIDR yang dialokasikan dari kolam IPAM dan tidak dipantau oleh IPAM untuk potensi kepatuhan CIDR dengan aturan alokasi kumpulan. CIDR dipantau untuk tumpang tindih.
    - Diabaikan: Sumber daya telah dipilih untuk dibebaskan dari pemantauan. Sumber daya yang diabaikan tidak dievaluasi untuk kepatuhan aturan tumpang tindih atau alokasi. Ketika sumber daya dipilih untuk diabaikan, setiap ruang yang dialokasikan kepadanya dari kolam IPAM dikembalikan ke kolam dan sumber daya tidak akan diimpor lagi melalui impor otomatis (jika aturan alokasi impor otomatis disetel di kolam).
    - -: Sumber daya ini bukan salah satu jenis sumber daya yang dapat dikelola IPAM.
- Status tumpang tindih: Status tumpang tindih CIDR.
    - Tidak tumpang tindih: CIDR sumber daya tidak tumpang tindih dengan CIDR lain dalam lingkup yang sama.

- Tumpang tindih: CIDR sumber daya tumpang tindih dengan CIDR lain dalam lingkup yang sama. Perhatikan bahwa jika CIDR sumber daya tumpang tindih, itu bisa tumpang tindih dengan alokasi manual.
- Diabaikan: Sumber daya telah dipilih untuk dibebaskan dari pemantauan. IPAM tidak mengevaluasi sumber daya yang diabaikan untuk kepatuhan aturan tumpang tindih atau alokasi. Ketika sumber daya dipilih untuk diabaikan, setiap ruang yang dialokasikan kepadanya dari kolam IPAM dikembalikan ke kolam dan sumber daya tidak akan diimpor lagi melalui impor otomatis (jika aturan alokasi impor otomatis disetel di kolam).
- -: Sumber daya ini bukan salah satu jenis sumber daya yang dapat dikelola IPAM.

- Penggunaan IP: Untuk sumber daya yang merupakan VPC, ini adalah persentase ruang alamat IP di VPC yang diambil oleh CIDR subnet. Untuk sumber daya yang merupakan subnet, jika subnet memiliki IPv4 CIDR yang disediakan untuk itu, ini adalah persentase ruang alamat IPv4 di subnet yang digunakan. Jika subnet memiliki IPv6 CIDR yang disediakan untuk itu, persentase ruang alamat IPv6 yang digunakan tidak terwakili. Persentase ruang alamat IPv6 yang digunakan saat ini tidak dapat dihitung. Untuk sumber daya yang merupakan kolam IPv4 publik, ini adalah persentase ruang alamat IP di kolam yang telah dialokasikan ke alamat IP Elastic (EIP).
- Wilayah: AWS Wilayah sumber daya.
- ID Pemilik: ID AWS akun orang yang membuat sumber daya ini.
- Jenis sumber daya: Apakah sumber daya adalah VPC, subnet, alamat IP Elastis, atau kolam IPv4 publik.
- ID Pool: ID kolam IPAM tempat sumber daya berada.

6. Gunakan sumber daya Filter untuk memfilter tabel sumber daya menurut properti kolom, seperti ID VPC atau status kepatuhan.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk memantau penggunaan CIDR berdasarkan sumber daya:

1. Dapatkan ID lingkup: describe-ipam-scopes
2. Minta informasi sumber daya: get-ipam-resource-cidrs

Pantau IPAM dengan Amazon CloudWatch

IPAM secara otomatis menyimpan metrik yang terkait dengan penggunaan alamat IP (seperti ruang alamat IP yang tersedia di kolam IPAM Anda dan jumlah CIDR sumber daya yang mematuhi aturan alokasi) dan pemanfaatan sumber daya di CloudWatch namespace `AWS/IPAM` Amazon di Wilayah asal IPAM Anda.

Daftar Isi

- Metrik kolam dan cakupan IPAM
- Metrik pemanfaatan sumber daya

Metrik kolam dan cakupan IPAM

IPAM menerbitkan data tentang kolam dan cakupan IPAM Anda ke Amazon. CloudWatch Anda dapat menggunakan metrik ini untuk membuat alarm untuk kolam IPAM guna memberi tahu Anda jika kumpulan alamat hampir habis atau jika sumber daya gagal mematuhi aturan alokasi yang ditetapkan pada kumpulan. Membuat alarm dan mengatur notifikasi dengan Amazon CloudWatch berada di luar cakupan bagian ini. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch alarm Amazon di Panduan CloudWatch Pengguna Amazon.

Metrik dan dimensi yang dikirim IPAM ke Amazon CloudWatch tercantum di bawah ini.

Metrik kolam IPAM

Nama metrik	Deskripsi
CompliantResourceCidrs	Jumlah CIDR sumber daya terkelola yang mematuhi aturan alokasi kolam IPAM. Untuk informasi selengkapnya tentang aturan alokasi, lihatBuat kolam IPv4 tingkat atas.
NoncompliantResourceCidrs	Jumlah CIDR sumber daya terkelola yang tidak mematuhi aturan alokasi kolam IPAM. Untuk informasi selengkapnya tentang aturan alokasi, lihatBuat kolam IPv4 tingkat atas.
PercentAllocated	Persentase ruang IP pool yang telah dialokasikan ke kolam lain.
PercentAssigned	Persentase ruang IP pool yang telah dialokasikan untuk sumber daya, termasuk alokasi manual.

Nama metrik	Deskripsi
PercentAvailable	Persentase ruang IP pool yang belum dialokasikan ke kolam atau sumber daya lain.

Metrik cakupan IPAM

Nama metrik	Deskripsi
CompliantResourceCidrs	Jumlah CIDR sumber daya yang mematuhi aturan alokasi untuk kolam IPAM dalam ruang lingkup.
ManagedResourceCidrs	Jumlah CIDR sumber daya untuk sumber daya yang dapat dikelola (VPC atau kolam IPv4 publik) yang dialokasikan dari kolam IPAM dalam ruang lingkup.
NoncompliantResourceCidrs	Jumlah CIDR sumber daya yang tidak mematuhi aturan alokasi untuk kumpulan IPAM dalam ruang lingkup.
OverlappingResourceCidrs	Jumlah CIDR sumber daya yang tumpang tindih dalam ruang lingkup.
UnmanagedResourceCidrs	Jumlah CIDR sumber daya dalam lingkup yang saat ini terkait dengan sumber daya yang dapat dikelola tetapi tidak dikelola oleh IPAM.

Dimensi yang dapat Anda gunakan untuk memfilter metrik IPAM tercantum di bawah ini.

Dimensi	Deskripsi
AddressFamily	Keluarga alamat IP untuk CIDR sumber daya (IPv4 atau IPv6).
Lokal	AWSWilayah di mana kolam IPAM tersedia untuk alokasi.
PooLid	ID kolam.
ScopeID	ID ruang lingkup.

Untuk informasi tentang memantau VPC dengan Amazon CloudWatch, lihat CloudWatch metrik untuk VPC Anda di Panduan Pengguna Amazon Virtual Private Cloud.

Metrik pemanfaatan sumber daya

IPAM menerbitkan metrik pemanfaatan IP untuk sumber daya yang dipantau IPAM ke Amazon. CloudWatch Sumber daya ini meliputi:

- VPC (IPv4 dan IPv6)
- Subnet (IPv4)
- Kolam IPv4 publik

IPAM menghitung dan menerbitkan metrik pemanfaatan IP secara terpisah oleh keluarga alamat IP (IPv4 atau IPv6). Pemanfaatan IP sumber daya dihitung di semua CIDR dari keluarga alamat yang sama.

Untuk setiap jenis sumber daya dan kombinasi keluarga alamat, IPAM menggunakan tiga aturan untuk menentukan metrik mana yang akan diterbitkan:

- Hingga 50 sumber daya dengan pemanfaatan IP tertinggi. Anda dapat menggunakan informasi ini untuk mengonfigurasi alarm agar diperingatkan jika ambang batas penggunaan IP dilanggar.
- Hingga 50 sumber daya dengan pemanfaatan IP terendah. Anda dapat menggunakan informasi ini untuk memutuskan apakah Anda ingin menyimpan atau menghapus sumber daya yang kurang dimanfaatkan.
- Hingga 50 sumber daya lainnya. Anda dapat menggunakan informasi ini untuk secara konsisten melacak pemanfaatan IP sumber daya yang mungkin tidak ditangkap dalam kelompok pemanfaatan tinggi atau rendah.
  - Hingga 50 VPC berisi CIDR yang dialokasikan dari kolam IPAM (diprioritaskan berdasarkan ukuran total blok CIDR).
  - Hingga 50 subnet yang VPC-nya berisi CIDR yang dialokasikan dari kolam IPAM (diprioritaskan berdasarkan ukuran total blok CIDR).
  - Hingga 50 kolam IPv4 publik yang berisi CIDR yang dialokasikan dari kolam IPAM (diprioritaskan berdasarkan ukuran total blok CIDR).

Setelah menerapkan setiap aturan, metrik dikumpulkan dan diterbitkan dengan nama metrik yang sama untuk setiap jenis sumber daya. Lihat di bawah untuk informasi rinci tentang nama metrik dan dimensinya.

> **Important**
>
> Ada batasan unik untuk setiap jenis sumber daya, keluarga alamat, dan kombinasi aturan. Nilai default dari setiap batas adalah 50. Anda dapat menyesuaikan batasan ini dengan menghubungi Pusat AWS Dukungan seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS

Example Contoh

Katakanlah IPAM Anda memonitor 2.500 VPC dan 10.000 subnet, semuanya dengan IPv4 dan IPv6 CIDR. IPAM menerbitkan metrik pemanfaatan IP berikut:

- Hingga 150 metrik untuk pemanfaatan IP VPC IPv4, termasuk:
  - 50 VPC dengan pemanfaatan IP IPv4 tertinggi
  - 50 VPC dengan pemanfaatan IPv4 terendah
  - Hingga 50 VPC yang berisi IPv4 CIDR yang dialokasikan dari kolam IPAM
- Hingga 150 metrik untuk pemanfaatan VPC IPv6, termasuk:
  - 50 VPC dengan pemanfaatan IP IPv6 tertinggi
  - 50 VPC dengan pemanfaatan IPv6 terendah
  - Hingga 50 VPC yang berisi IPv6 CIDR yang dialokasikan dari kolam IPAM
- Hingga 150 metrik untuk pemanfaatan IPv4 subnet, termasuk:
  - 50 subnet dengan pemanfaatan IP IPv4 tertinggi
  - 50 subnet dengan pemanfaatan IP IPv4 terendah
  - Hingga 50 subnet yang VPC-nya berisi IPv4 CIDR yang dialokasikan dari kolam IPAM

Metrik VPC

Nama dan deskripsi metrik VPC tercantum di bawah ini.

Nama metrik	Deskripsi
VPCIpUsage	Total IP yang dicakup oleh CIDR dalam subnet VPC dibagi dengan total IP yang dicakup oleh CIDR dalam VPC. Ini dihitung di semua CIDR VPC dalam Lingkup IPAM yang sama dan secara terpisah untuk IPv4 dan IPv6 CIDR.

Dimensi yang dapat Anda gunakan untuk memfilter metrik VPC tercantum di bawah ini.

Dimensi	Deskripsi
AddressFamily	Keluarga alamat IP untuk CIDR sumber daya (IPv4 atau IPv6).
OwnerID	ID pemilik VPC.
Wilayah	AWSWilayah tempat VPC berada.
ScopeID	ID lingkup IPAM yang dimiliki VPC.
VPCid	ID VPC.

Metrik subnet

Nama dan deskripsi metrik subnet tercantum di bawah ini.

Nama metrik	Deskripsi
SubnetIpuSage	Jumlah IP aktif dibagi dengan total IP di IPv4 CIDR subnet.

Dimensi yang dapat Anda gunakan untuk memfilter metrik subnet tercantum di bawah ini.

Dimensi	Deskripsi
AddressFamily	Keluarga alamat IP untuk CIDR sumber daya (hanya IPv4).
OwnerID	ID pemilik subnet.

Dimensi	Deskripsi
Wilayah	AWSWilayah tempat subnet berada.
ScopeID	ID lingkup IPAM yang dimiliki subnet.
SubnetID	ID subnet.
VPCid	ID VPC yang dimiliki subnet.

Metrik kolam IPv4 publik

Nama dan deskripsi metrik kolam IPv4 publik tercantum di bawah ini.

Nama metrik	Deskripsi
Publicipv4poolipusage	Jumlah EIP dari IPv4 Pool publik dibagi dengan total IP di kolam renang.

Dimensi yang dapat Anda gunakan untuk memfilter metrik kolam IPv4 publik tercantum di bawah ini.

Dimensi	Deskripsi
OwnerID	ID pemilik kolam IPv4 publik.
Publicipv4poolid	ID kolam IPv4 publik.
Wilayah	AWSWilayah tempat kolam IPv4 publik berada.
ScopeID	ID lingkup IPAM yang dimiliki kolam IPv4 publik.

Metrik wawasan IP publik

Nama dan deskripsi metrik wawasan IP publik tercantum di bawah ini.

Nama metrik	Deskripsi
AmazonOwnedElasticIP	Jumlah alamat IP Elastic milik Amazon yang telah Anda sediakan atau tetapkan ke sumber daya di akun Anda. AWS
AssociatedAmazonOwnedElasticIP	Jumlah alamat IP Elastic milik Amazon yang telah Anda kaitkan dengan sumber daya di akun AndaAWS.
AssociatedBringYourOwnIP	Jumlah alamat IPv4 publik yang Anda bawa AWS menggunakan Bawa alamat IP Anda sendiri (BYOIP) dan telah dikaitkan dengan sumber daya di akun Anda. AWS
BringYourOwnIP	Jumlah alamat IPv4 publik yang telah Anda bawa AWS menggunakan Bring your own IP address (BYOIP).
EC2PublicIps	Jumlah alamat IPv4 publik yang ditetapkan ke instans EC2 saat instance diluncurkan ke subnet default atau ke subnet yang dikonfigurasi untuk secara otomatis menetapkan alamat IPv4 publik.
ServiceManagedBringYourOwnIP	Jumlah alamat IPv4 publik yang telah Anda bawa AWS menggunakan Bring your own IP address (BYOIP) yang disediakan dan dikelola oleh suatu layanan. AWS
ServiceManagedIP	Jumlah alamat IPv4 publik yang disediakan dan dikelola oleh suatu layanan. AWS
UnassociatedAmazonOwnedElasticIP	Jumlah alamat IP Elastic milik Amazon yang belum Anda kaitkan dengan sumber daya di akun AndaAWS.
UnassociatedBringYourOwnIP	Jumlah alamat IPv4 publik yang Anda bawa AWS menggunakan Bawa alamat IP Anda sendiri (BYOIP) dan belum terkait dengan sumber daya apa pun di akun Anda. AWS

Dimensi yang dapat Anda gunakan untuk memfilter metrik wawasan IP publik tercantum di bawah ini.

Dimensi	Deskripsi
IpamId	ID IPAM yang menjadi milik alamat IP.
Wilayah	AWSWilayah tempat alamat IP publik berada.

Kiat cepat untuk membuat alarm

Untuk membuat CloudWatch alarm Amazon dengan cepat untuk sumber daya dengan penggunaan alamat IP tinggi, buka CloudWatch konsol, pilih Metrik, Semua metrik, pilih tab Kueri, pilih Namespace**`AWS/IPAM > VPC IP Usage Metrics`**, atau**`AWS/IPAM > Subnet IP Usage Metrics`**, pilih nama Metrik **`AWS/IPAM > Public IPv4 Pool IP Usage Metrics`**, atau **`MAX(VpcIPUsage)`** **`MAX(SubnetIPUsage)`****`MAX(PublicIPv4PoolIPUsage)`**, dan pilih Buat alarm. Untuk informasi selengkapnya, lihat Membuat alarm pada kueri Wawasan Metrik di Panduan Pengguna Amazon. CloudWatch

Lihat riwayat alamat IP

Ikuti langkah-langkah di bagian ini untuk melihat riwayat alamat IP atau CIDR dalam lingkup IPAM. Anda dapat menggunakan data historis untuk menganalisis dan mengaudit keamanan jaringan dan kebijakan perutean Anda. IPAM secara otomatis menyimpan data pemantauan alamat IP hingga tiga tahun.

Anda dapat menggunakan data historis IP untuk mencari perubahan status alamat IP atau CIDR untuk jenis sumber daya berikut:

- VPC
- Subnet VPC
- Alamat IP elastis
- Instans EC2
- Antarmuka jaringan EC2 yang dilampirkan ke instance

Important

Meskipun IPAM tidak memantau instans Amazon EC2 atau antarmuka jaringan EC2 yang dilampirkan ke instans, Anda dapat menggunakan fitur riwayat IP Pencarian untuk mencari data historis pada instans EC2 dan CIDR antarmuka jaringan.

Note

- Jika Anda memindahkan sumber daya dari satu cakupan IPAM ke cakupan IPAM lainnya, catatan riwayat sebelumnya berakhir dan catatan riwayat baru dibuat di bawah lingkup baru. Untuk informasi selengkapnya, lihat Memindahkan CIDR VPC antar cakupan.
- Jika Anda menghapus atau mentransfer sumber daya ke AWS akun yang tidak dipantau oleh IPAM Anda, riwayat baru apa pun yang terkait dengan sumber daya tidak akan terlihat dan IPAM Anda tidak akan memantau sumber daya. Alamat IP sumber daya, bagaimanapun, masih dapat dicari.
- Jika AndaIntegrasikan IPAM dengan akun di luar organisasi, pemilik IPAM dapat melihat riwayat alamat IP dari semua CIDR sumber daya yang dimiliki oleh akun tersebut.

AWS Management Console

Untuk melihat sejarah CIDR

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Cari riwayat IP.
3. Masukkan alamat IP IPv4 atau IPv6 atau CIDR. Ini harus menjadi CIDR khusus untuk sumber daya.
4. Pilih ID cakupan IPAM.
5. Pilih rentang tanggal/waktu.
6. Jika Anda ingin memfilter hasil berdasarkan VPC, masukkan ID VPC. Gunakan opsi ini jika CIDR muncul di beberapa VPC.
7. Pilih Cari.

Command line

Perintah di bagian ini menautkan ke dokumentasi Referensi AWS CLI. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

- Lihat riwayat CIDR: get-ipam-address-history

Untuk melihat contoh bagaimana Anda dapat menggunakan AWS CLI untuk menganalisis dan mengaudit penggunaan alamat IP, lihat Tutorial: Lihat riwayat alamat IP menggunakan file AWS CLI.

Hasil pencarian diatur ke dalam kolom berikut:

- Contoh waktu akhir: Contoh waktu akhir dari asosiasi Sumber Daya-ke-CIDR dalam lingkup IPAM. Perubahan diambil dalam snapshot periodik, sehingga waktu akhir mungkin telah terjadi sebelum waktu tertentu ini.
- Contoh waktu mulai: Contoh waktu mulai dari asosiasi Resource-to-CIDR dalam lingkup IPAM. Perubahan diambil dalam snapshot periodik, sehingga waktu mulai mungkin telah terjadi sebelum waktu tertentu ini.

  Example

  Untuk membantu menjelaskan waktu yang Anda lihat di bawah Waktu mulai sampel dan waktu akhir Sampel, mari kita lihat contoh kasus penggunaan:

  Pada pukul 14:00, VPC dibuat dengan CIDR 10.0.0.0/16. Pada pukul 15:00, Anda membuat kolam IPAM dan IPAM dengan CIDR 10.0.0.0/8, dan pilih opsi impor otomatis untuk memungkinkan IPAM menemukan dan mengimpor CIDR apa pun yang termasuk dalam kisaran alamat IP 10.0.0.0/8. Karena IPAM mengambil perubahan pada CIDR dalam snapshot berkala, IPAM tidak menemukan CIDR VPC yang ada hingga 15:05. Saat Anda mencari ID VPC ini menggunakan fitur riwayat IP Pencarian, waktu mulai Sampel untuk VPC Anda adalah 3:05 PM, yaitu saat IPAM menemukannya, bukan 2:00 PM, yaitu saat Anda membuat VPC. Sekarang, katakanlah Anda memutuskan untuk menghapus VPC pada pukul 17:00. Ketika VPC dihapus, CIDR 10.0.0.0/16 yang dialokasikan ke VPC didaur ulang kembali ke kolam IPAM. IPAM mengambil snapshot periodiknya pada pukul 17:05 dan mengambil perubahannya. Saat Anda mencari ID VPC ini dalam riwayat IP Pencarian, 5:05 PM adalah waktu akhir Sampel untuk CIDR VPC, bukan 17:00, yaitu saat VPC dihapus.
- ID Sumber Daya: ID yang dihasilkan saat sumber daya dikaitkan dengan CIDR.

- Nama: Nama sumber daya (jika ada).
- Status kepatuhan: Status kepatuhan CIDR.
  - Sesuai: Sumber daya yang dikelola mematuhi aturan alokasi kolam IPAM.
  - Tidak patuh: CIDR sumber daya tidak mematuhi satu atau lebih aturan alokasi kumpulan IPAM.

    Example

    Jika VPC memiliki CIDR yang tidak memenuhi parameter panjang netmask dari kolam IPAM, atau jika sumber daya tidak berada di AWS Wilayah yang sama dengan kolam IPAM, itu akan ditandai sebagai tidak sesuai.
  - Tidak dikelola: Sumber daya tidak memiliki CIDR yang dialokasikan dari kolam IPAM dan tidak dipantau oleh IPAM untuk potensi kepatuhan CIDR dengan aturan alokasi kumpulan. CIDR dipantau untuk tumpang tindih.
  - Diabaikan: Sumber daya yang dikelola telah dipilih untuk dibebaskan dari pemantauan. Sumber daya yang diabaikan tidak dievaluasi untuk kepatuhan aturan tumpang tindih atau alokasi. Ketika sumber daya dipilih untuk diabaikan, setiap ruang yang dialokasikan kepadanya dari kolam IPAM dikembalikan ke kolam dan sumber daya tidak akan diimpor lagi melalui impor otomatis (jika aturan alokasi impor otomatis disetel di kolam).
  - -: Sumber daya ini bukan salah satu jenis sumber daya yang dapat dipantau atau dikelola IPAM.
- Status tumpang tindih: Status tumpang tindih CIDR.
  - Tidak tumpang tindih: CIDR sumber daya tidak tumpang tindih dengan CIDR lain dalam lingkup yang sama.
  - Tumpang tindih: CIDR sumber daya tumpang tindih dengan CIDR lain dalam lingkup yang sama. Perhatikan bahwa jika CIDR sumber daya tumpang tindih, itu bisa tumpang tindih dengan alokasi manual.
  - Diabaikan: Sumber daya yang dikelola telah dipilih untuk dibebaskan dari pemantauan. IPAM tidak mengevaluasi sumber daya yang diabaikan untuk kepatuhan aturan tumpang tindih atau alokasi. Ketika sumber daya dipilih untuk diabaikan, setiap ruang yang dialokasikan kepadanya dari kolam IPAM dikembalikan ke kolam dan sumber daya tidak akan diimpor lagi melalui impor otomatis (jika aturan alokasi impor otomatis disetel di kolam).
  - -: Sumber daya ini bukan salah satu jenis sumber daya yang dapat dipantau atau dikelola IPAM.
- Jenis sumber daya
  - vpc: CIDR dikaitkan dengan VPC.
  - subnet: CIDR dikaitkan dengan subnet VPC.

  - eip: CIDR dikaitkan dengan alamat IP Elastis.
  - contoh: CIDR dikaitkan dengan instans EC2.
  - network-interface: CIDR dikaitkan dengan antarmuka jaringan.
- ID VPC: ID VPC yang dimiliki sumber daya ini (jika ada).
- Wilayah: AWS Wilayah sumber daya ini.
- ID Pemilik: ID AWS akun pengguna yang membuat sumber daya ini (jika ada).

Lihat wawasan IP publik

Alamat IPv4 publik adalah alamat IPv4 yang dapat dirutekan dari internet. Alamat IPv4 publik diperlukan agar sumber daya dapat dijangkau secara langsung dari internet melalui IPv4.

> **Note**
>
> AWS mengenakan biaya untuk semua alamat IPv4 publik, termasuk alamat IPv4 publik yang terkait dengan instans yang sedang berjalan dan alamat IP Elastis. Untuk informasi selengkapnya, lihat tab Alamat IPv4 Publik di halaman harga Amazon VPC.

Anda dapat melihat wawasan tentang jenis alamat IPv4 publik berikut:

- Alamat IP elastis (EIP): Alamat IPv4 publik statis yang disediakan oleh Amazon yang dapat Anda kaitkan dengan instans EC2, elastic network interface, atau sumber daya. AWS
- Alamat IPv4 publik EC2: Alamat IPv4 publik yang ditetapkan ke instans EC2 oleh Amazon (jika instans EC2 diluncurkan ke subnet default atau jika instance diluncurkan ke subnet yang telah dikonfigurasi untuk secara otomatis menetapkan alamat IPv4 publik).
- Alamat BYOIPv4: Alamat IPv4 publik dalam rentang alamat IPv4 yang Anda bawa AWS menggunakan Bring your own IP address (BYOIP).
- Alamat IPv4 yang dikelola layanan: Alamat IPv4 publik secara otomatis disediakan pada sumber daya dan dikelola oleh layanan. AWS AWS Misalnya, alamat IPv4 publik di Amazon ECS, Amazon RDS, atau Amazon. WorkSpaces

Anda dapat menggunakan wawasan IP Publik untuk melihat hal berikut:

- Jika IPAM Anda terintegrasi dengan akun di AWS Organisasi, Anda dapat melihat semua alamat IPv4 publik yang digunakan oleh layanan di semua AWS Wilayah untuk seluruh Organisasi Anda. AWS
- Jika IPAM Anda terintegrasi dengan satu akun, Anda dapat melihat semua alamat IPv4 publik yang digunakan oleh layanan di semua AWS Wilayah di akun Anda.

Wawasan IP publik menunjukkan kepada Anda semua alamat IPv4 publik yang digunakan oleh layanan di seluruh Wilayah. Anda dapat menggunakan wawasan ini untuk mengidentifikasi penggunaan alamat IPv4 publik dan melihat rekomendasi untuk merilis alamat IP Elastis yang tidak digunakan.

- Jenis IP Publik: Jumlah alamat IPv4 publik yang diatur berdasarkan jenis.
  - EIP milik Amazon: Alamat IP elastis yang telah Anda sediakan atau tetapkan ke sumber daya di akun Anda. AWS
  - IP publik EC2: Alamat IPv4 publik yang ditetapkan ke instans EC2 saat instance diluncurkan ke subnet default atau ke subnet yang telah dikonfigurasi untuk secara otomatis menetapkan alamat IPv4 publik.
  - BYOIP: Alamat IPv4 publik yang telah Anda bawa AWS menggunakan Bring your own IP address (BYOIP).
  - IP terkelola layanan: Alamat IPv4 publik yang disediakan dan dikelola oleh layanan. AWS
- Penggunaan EIP: Jumlah alamat IP Elastis yang diatur berdasarkan cara penggunaannya.
  - EIP milik Amazon terkait: Alamat IP elastis yang telah Anda sediakan di AWS akun Anda dan yang telah Anda kaitkan dengan instans EC2, antarmuka jaringan, atau sumber daya. AWS
  - BYOIP Terkait: Alamat IPv4 publik yang Anda bawa AWS menggunakan BYOIP yang telah Anda kaitkan dengan antarmuka jaringan.
  - EIP milik Amazon yang tidak terkait: Alamat IP elastis yang telah Anda sediakan di AWS akun Anda tetapi Anda belum terkait dengan antarmuka jaringan.
  - BYOIP Tidak Terkait: Alamat IPv4 publik yang Anda bawa AWS menggunakan BYOIP tetapi Anda belum terkait dengan antarmuka jaringan.
- Alamat IP Publik: Tabel alamat IPv4 publik dan atributnya.
  - Alamat IP: Alamat IPv4 publik.
  - Terkait: Apakah alamat dikaitkan dengan instans EC2, antarmuka jaringan, atau AWS sumber daya.

  - Terkait: Alamat IPv4 publik dikaitkan dengan instans EC2, antarmuka jaringan, atau sumber daya. AWS
  - Tidak terkait: Alamat IPv4 publik tidak terkait dengan sumber daya apa pun dan tidak digunakan di akun Anda. AWS
- Jenis alamat: Jenis alamat IP.
  - EIP milik Amazon: Alamat IPv4 publik adalah alamat IP Elastis.
  - BYOIP: Alamat IPv4 publik dibawa menggunakan BYOIP. AWS
  - IP publik EC2: Alamat IPv4 publik ditetapkan secara otomatis ke instans EC2.
  - Layanan BYOIP yang dikelola: Alamat IPv4 publik dibawa AWS menggunakan Bring Your Own IP (BYOIP).
  - IP yang dikelola layanan: Alamat IPv4 publik disediakan dan dikelola oleh layanan. AWS
- Layanan: Layanan yang dikaitkan dengan alamat IP.
  - AGA: Sebuah AWS Global Accelerator. Jika akselerator perutean khusus digunakan, IP publiknya tidak terdaftar. Untuk melihat IP publik ini, lihat Melihat akselerator perutean kustom Anda.
  - Database Migration Service: Sebuah AWS Database Migration Service contoh replikasi (DMS).
  - Redshift: Gugus Pergeseran Merah Amazon.
  - RDS: Instans Amazon Relational Database Service (RDS).
  - Load balancer (EC2): Application Load Balancer atau Network Load Balancer.
  - Gateway NAT (VPC): Gateway NAT publik VPC Amazon.
  - Site-to-Site VPN: Gateway pribadi virtual. AWS Site-to-Site VPN
  - Lainnya: Layanan lain yang saat ini tidak dapat diidentifikasi.
- Nama (ID EIP): Jika alamat IPv4 publik ini adalah alokasi alamat IP Elastis, ini adalah nama dan ID dari alokasi EIP.
- ID antarmuka jaringan: Jika alamat IPv4 publik ini dikaitkan dengan antarmuka jaringan, ini adalah ID antarmuka jaringan.
- ID Instance: Jika alamat IPv4 publik ini dikaitkan dengan instans EC2, ini adalah ID instans.
- Grup keamanan: Jika alamat IPv4 publik ini dikaitkan dengan instans EC2, ini adalah nama dan ID grup keamanan yang ditetapkan ke instans.
- Kolam IPv4 Publik: Jika ini adalah alamat IP Elastis dari kumpulan alamat IP yang dimiliki dan dikelola oleh Amazon, nilainya adalah “-”. Jika ini adalah alamat IP Elastis dari rentang alamat IP

yang Anda miliki dan telah dibawa ke Amazon (menggunakan BYOIP), nilainya adalah ID kolam IPv4 publik.

- Grup perbatasan jaringan: Jika alamat IP diiklankan, ini adalah AWS Wilayah tempat alamat IP diiklankan.
- ID Pemilik: AWS Nomor akun pemilik sumber daya.
- Contoh waktu: Waktu penemuan sumber daya terakhir yang berhasil.
- ID penemuan sumber daya: ID penemuan sumber daya yang telah menemukan alamat IPv4 publik ini.
- Sumber daya layanan: Sumber daya ARN atau ID.

Jika alamat IP Elastis dialokasikan ke akun Anda tetapi tidak terkait dengan antarmuka jaringan, spanduk muncul yang memberi tahu Anda bahwa Anda memiliki EIP yang tidak terkait di akun Anda dan Anda harus melepaskannya.

> **Important**
>
> Wawasan IP publik baru-baru ini diperbarui. Jika Anda melihat kesalahan terkait tidak memiliki izin untuk menelepon GetIpamDiscoveredPublicAddresses, izin terkelola yang dilampirkan ke penemuan sumber daya yang dibagikan dengan Anda perlu diperbarui. Hubungi orang yang membuat penemuan sumber daya dan minta mereka memperbarui izin terkelola `AWSRAMPermissionIpamResourceDiscovery` ke versi default. Untuk informasi selengkapnya, lihat Memperbarui bagian sumber daya di Panduan AWS RAM Pengguna.

AWS Management Console

Untuk melihat wawasan alamat IP publik

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Wawasan IP Publik.
3. Untuk melihat detail alamat IP publik, pilih alamat IP dengan mengkliknya.
4. Lihat informasi berikut tentang alamat IP:
   - Detail: Informasi yang sama terlihat di kolom panel wawasan IP Publik utama, seperti Jenis alamat dan Layanan.

- Aturan grup keamanan masuk: Jika alamat IP ini dikaitkan dengan instans EC2, ini adalah aturan grup keamanan yang mengontrol lalu lintas masuk ke instance.
- Aturan grup keamanan keluar: Jika alamat IP ini dikaitkan dengan instans EC2, ini adalah aturan grup keamanan yang mengontrol lalu lintas keluar dari instance.
- Tag: Pasangan kunci dan nilai yang bertindak sebagai metadata untuk mengatur sumber daya Anda AWS .

Command line

Gunakan perintah berikut untuk mendapatkan alamat IP publik yang telah ditemukan oleh IPAM: get-ipam-discovered-public -address

Tutorial untuk Manajer Alamat IP VPC Amazon

Tutorial berikut menunjukkan kepada Anda bagaimana melakukan tugas-tugas IPAM umum menggunakan AWS CLI. Untuk mendapatkanAWS CLI, lihatAkses IPAM. Untuk informasi lebih lanjut tentang konsep IPAM yang disebutkan dalam tutorial ini, lihatCara kerja IPAM.

Konten

- Tutorial: Buat IPAM dan pool menggunakan konsol
- Tutorial: Buat IPAM dan pool menggunakanAWS CLI
- Tutorial: Lihat riwayat alamat IP menggunakanAWS CLI
- Tutorial: Bawa ASN Anda ke IPAM
- Tutorial: Bawa alamat IP Anda ke IPAM
- Tutorial: Transfer BYOIP IPv4 CIDR ke IPAM
- Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet

Tutorial: Buat IPAM dan pool menggunakan konsol

Dalam tutorial ini, Anda membuat IPAM, mengintegrasikan denganAWS Organizations, membuat kumpulan alamat IP, dan membuat VPC dengan CIDR dari kolam IPAM.

Tutorial ini menunjukkan kepada Anda bagaimana Anda dapat menggunakan IPAM untuk mengatur ruang alamat IP berdasarkan kebutuhan pengembangan yang berbeda. Setelah Anda menyelesaikan tutorial ini, Anda akan memiliki satu kumpulan alamat IP untuk sumber daya pra-produksi. Anda kemudian dapat membuat pool lain berdasarkan kebutuhan routing dan keamanan Anda, seperti kolam untuk sumber daya produksi.

Meskipun Anda dapat menggunakan IPAM sebagai pengguna tunggal, mengintegrasikan dengan AWS Organizations memungkinkan Anda mengelola alamat IP di seluruh akun di organisasi Anda. Tutorial ini mencakup mengintegrasikan IPAM dengan akun dalam organisasi. Itu tidak mencakup bagaimana caranyaIntegrasikan IPAM dengan akun di luar organisasi.

> **Note**
>
> Untuk keperluan tutorial ini, instruksi akan memberi tahu Anda untuk memberi nama sumber daya IPAM dengan cara tertentu, membuat sumber daya IPAM di Wilayah tertentu, dan

menggunakan rentang CIDR alamat IP tertentu untuk kumpulan Anda. Ini dimaksudkan untuk merampingkan pilihan yang tersedia di IPAM dan membantu Anda memulai dengan IPAM dengan cepat. Setelah Anda menyelesaikan tutorial ini, Anda dapat memutuskan untuk membuat IPAM baru dan mengkonfigurasinya secara berbeda.

Daftar Isi

- Prasyarat
- Bagaimana AWS Organizations terintegrasi dengan IPAM
- Langkah 1: Delegasikan administrator IPAM
- Langkah 2: Buat IPAM
- Langkah 3: Buat kolam IPAM tingkat atas
- Langkah 4: Buat kolam IPAM Regional
- Langkah 5: Buat kumpulan pengembangan pra-produksi
- Langkah 6: Bagikan kolam IPAM
- Langkah 7: Buat VPC dengan CIDR yang dialokasikan dari kolam IPAM
- Langkah 8: Pembersihan

Prasyarat

Sebelum memulai, Anda harus menyiapkan AWS Organizations akun dengan setidaknya satu akun anggota. Untuk petunjuk caranya, lihat Membuat dan mengelola organisasi di AWS OrganizationsPanduan Pengguna.

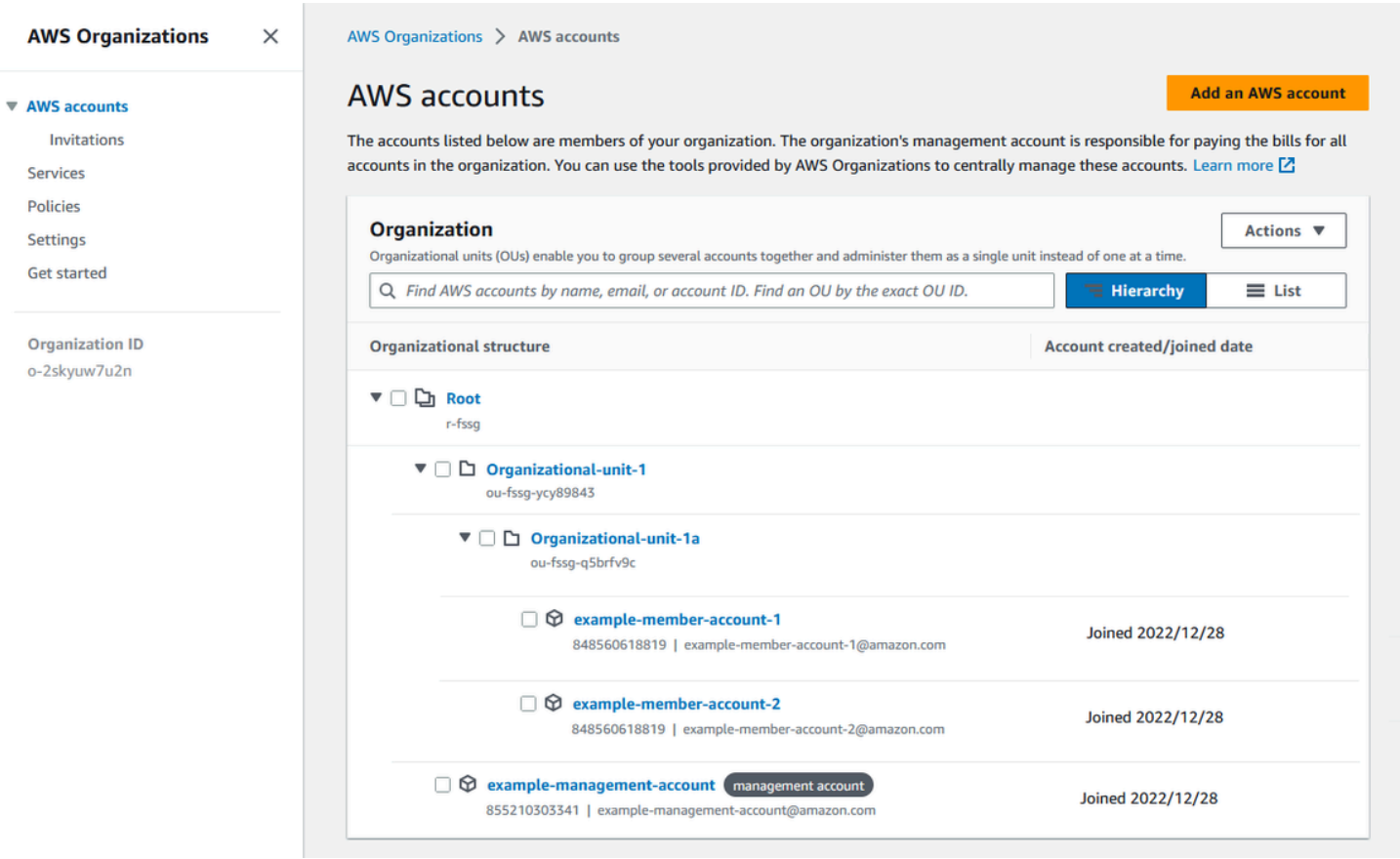
Bagaimana AWS Organizations terintegrasi dengan IPAM

Bagian ini menunjukkan contoh AWS Organizations akun yang Anda gunakan dalam tutorial ini. Ada tiga akun di organisasi Anda yang Anda gunakan ketika Anda mengintegrasikan dengan IPAM dalam tutorial ini:

- Akun manajemen (dipanggil example-management-accountdalam gambar berikut) untuk masuk ke konsol IPAM dan mendelegasikan admin IPAM. Anda tidak dapat menggunakan akun manajemen organisasi sebagai admin IPAM Anda.
- Akun anggota (disebut example-member-account-1 pada gambar berikut) sebagai akun admin IPAM. Akun admin IPAM bertanggung jawab untuk membuat IPAM dan menggunakannya untuk

mengelola dan memantau penggunaan alamat IP di seluruh organisasi. Setiap akun anggota di organisasi Anda dapat didelegasikan sebagai admin IPAM.

- Akun anggota (disebut example-member-account-2 berikut ini di atas) sebagai akun pengembang. Akun ini membuat VPC dengan CIDR yang dialokasikan dari kolam IPAM.



Selain akun, Anda memerlukan ID unit organisasi (ou-fssg-q5brfv9c pada gambar sebelumnya) yang berisi akun anggota yang akan Anda gunakan sebagai akun pengembang. Anda memerlukan ID ini sehingga, pada langkah selanjutnya, ketika Anda berbagi kolam IPAM Anda, Anda dapat membagikannya dengan OU ini.

> **Note**
>
> Untuk informasi selengkapnya tentang jenis AWS Organizations akun seperti akun manajemen dan anggota, lihat AWS Organizationsterminologi dan konsep.

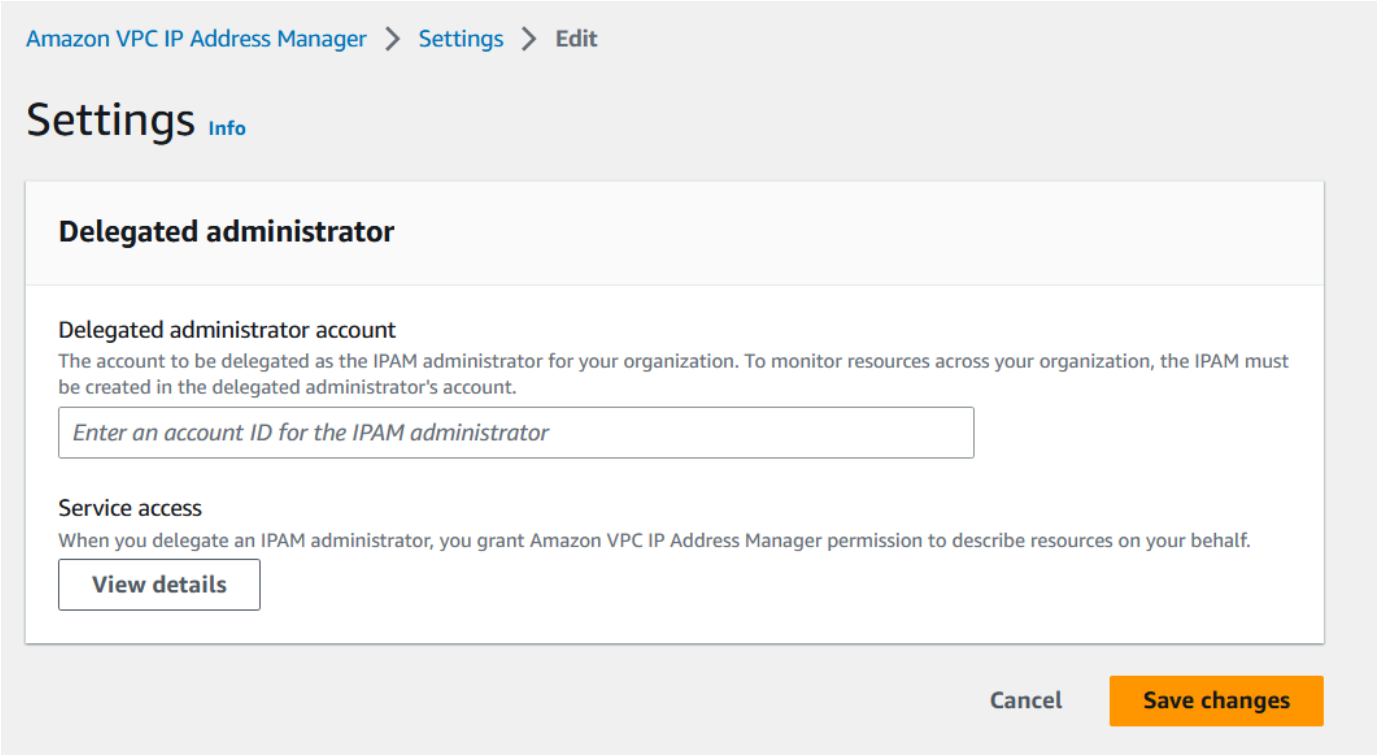
Langkah 1: Delegasikan administrator IPAM

Pada langkah ini, Anda akan mendelegasikan akun AWS Organizations anggota sebagai admin IPAM. Saat Anda mendelegasikan admin IPAM, peran terkait layanan akan dibuat secara otomatis di setiap akun anggota Anda. AWS Organizations IPAM memantau penggunaan alamat IP di akun ini dengan mengasumsikan peran terkait layanan di setiap akun anggota. Kemudian dapat menemukan sumber daya dan CIDR mereka terlepas dari Unit Organisasi mereka.

Anda tidak dapat menyelesaikan langkah ini kecuali Anda memiliki izin yang diperlukan AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat Integrasikan IPAM dengan akun di Organisasi AWS.

Untuk mendelegasikan akun admin IPAM

1. Menggunakan akun AWS Organizations manajemen, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di Konsol AWS Manajemen, pilih AWS Wilayah tempat Anda ingin bekerja dengan IPAM.
3. Di panel navigasi, pilih Pengaturan organisasi.
4. Pilih Delegasikan. Opsi Delegasi hanya tersedia jika Anda masuk ke konsol sebagai akun AWS Organizations manajemen.
5. Masukkan ID AWS akun untuk akun anggota organisasi. Administrator IPAM harus menjadi akun AWS Organizations anggota, bukan akun manajemen.



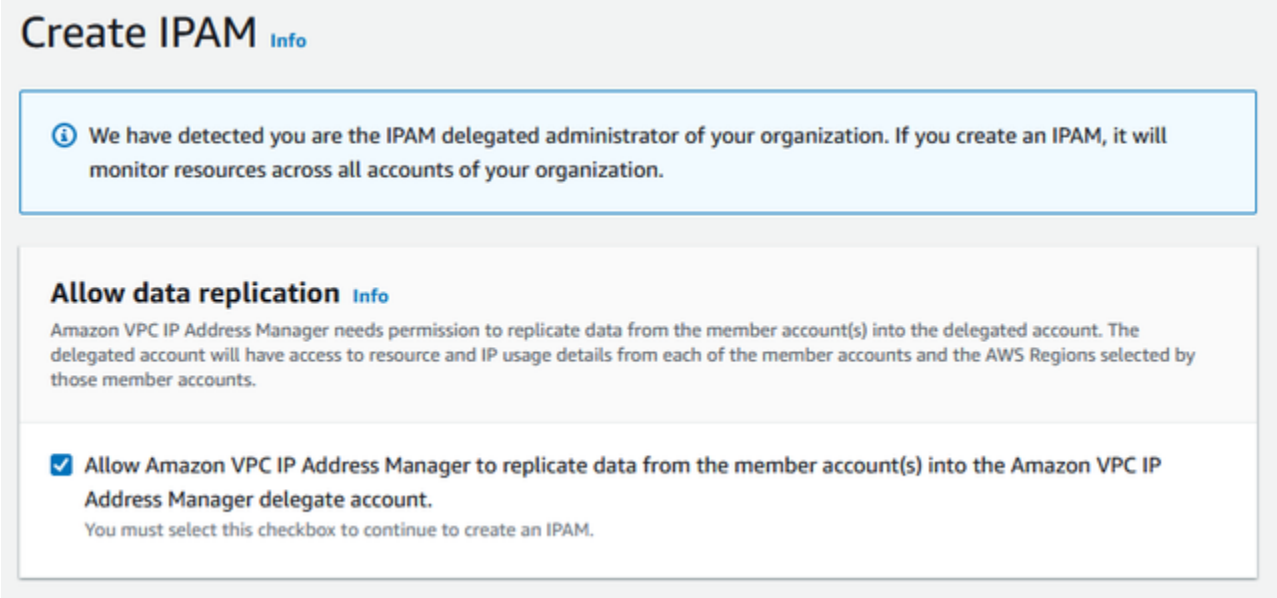
6. Pilih Save changes (Simpan perubahan). Informasi administrator yang didelegasikan diisi dengan detail yang terkait dengan akun anggota.

Langkah 2: Buat IPAM

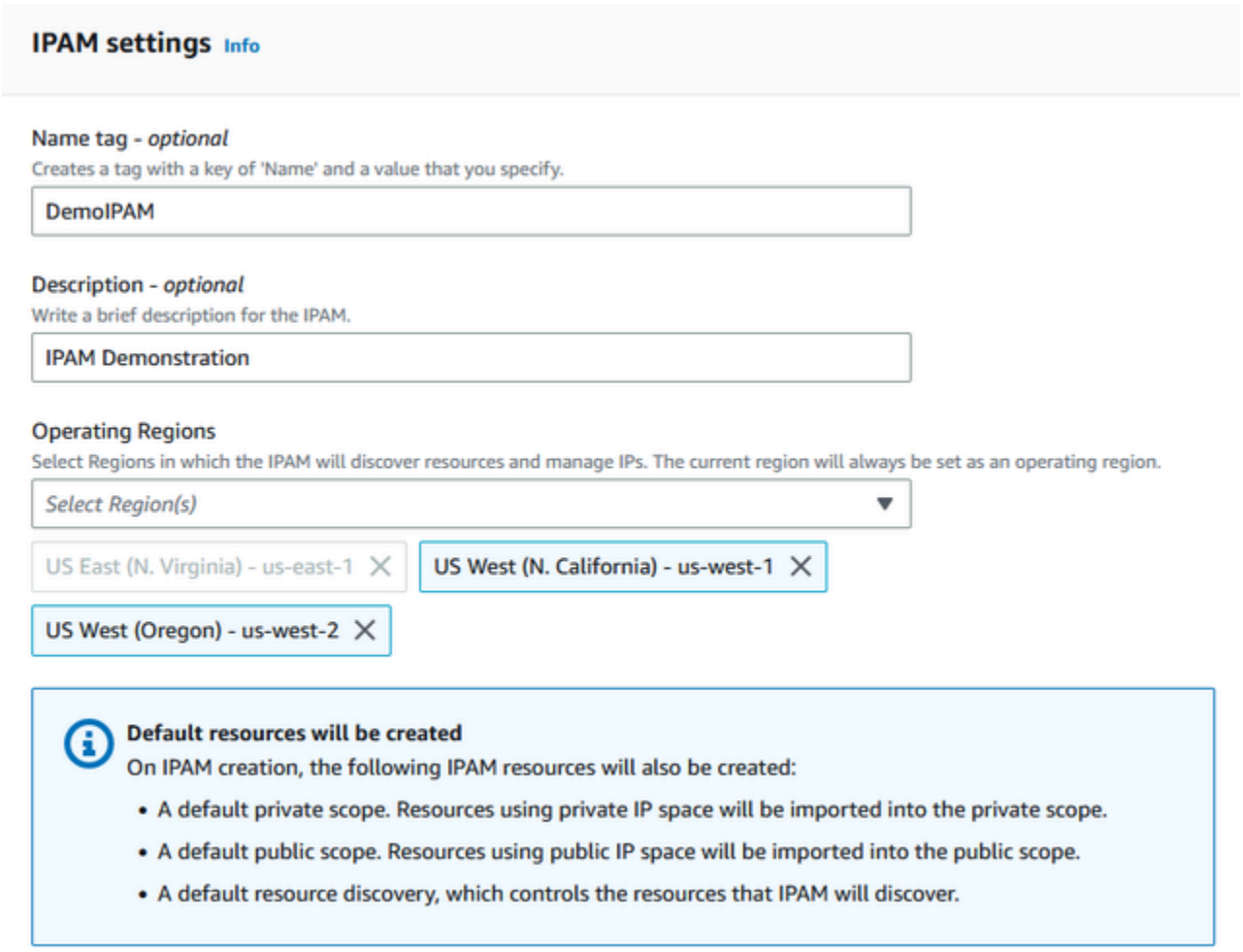
Pada langkah ini Anda akan membuat IPAM. Saat Anda membuat IPAM, IPAM secara otomatis membuat dua cakupan untuk IPAM: ruang lingkup pribadi yang ditujukan untuk semua ruang pribadi, dan ruang lingkup publik yang ditujukan untuk semua ruang publik. Cakupan, bersama dengan kumpulan dan alokasi, adalah komponen kunci dari IPAM Anda. Untuk informasi selengkapnya, lihat Cara kerja IPAM.

Untuk membuat IPAM

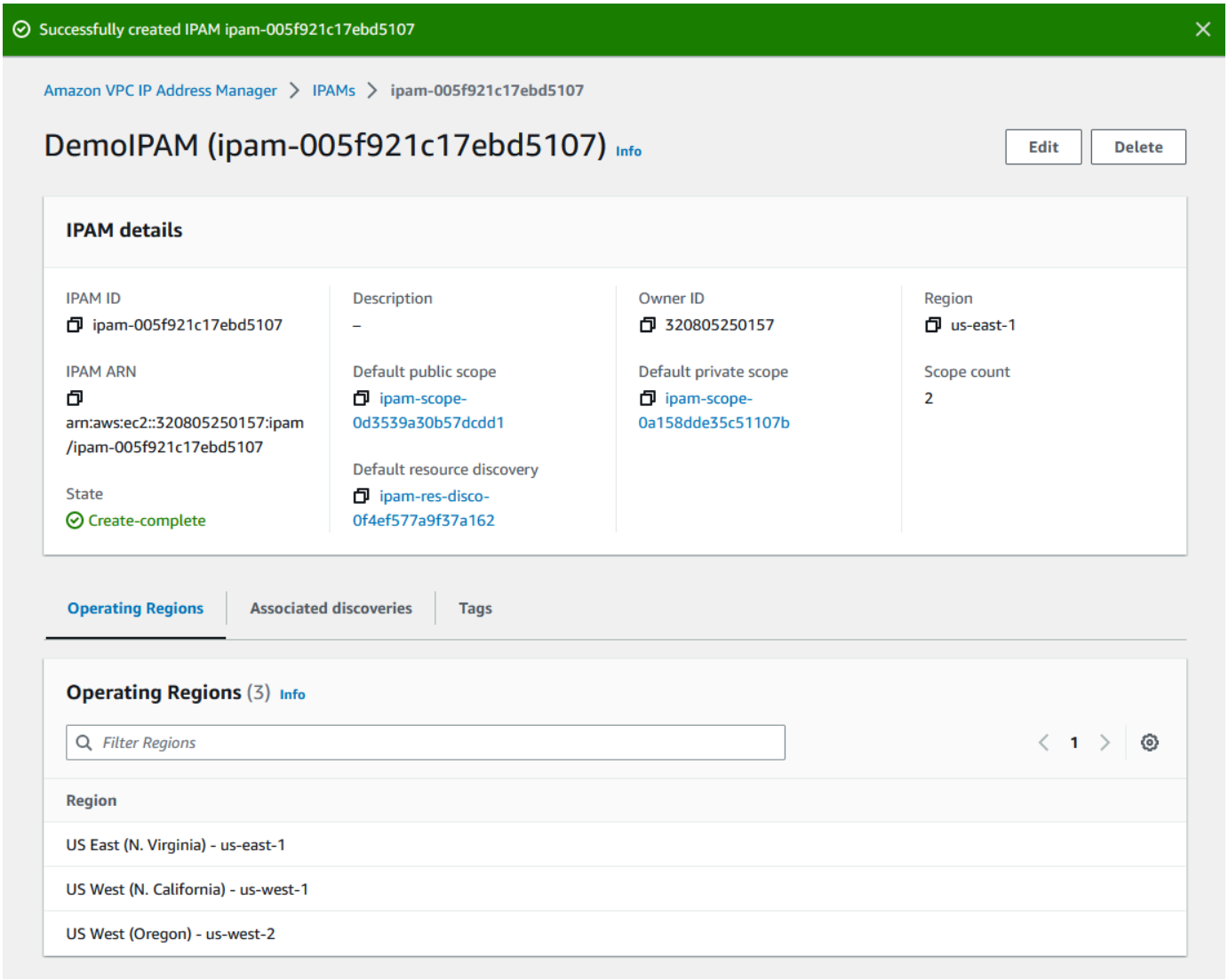
1. Menggunakan akun AWS Organizations anggota yang didelegasikan sebagai admin IPAM pada langkah sebelumnya, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di Konsol AWS Manajemen, pilih AWS Wilayah tempat Anda ingin membuat IPAM. Buat IPAM di Wilayah operasi utama Anda.
3. Pada halaman beranda layanan, pilih Buat IPAM.
4. Pilih Izinkan Pengelola Alamat IP VPC Amazon untuk mereplikasi data dari akun sumber ke akun delegasi IPAM. Jika Anda tidak memilih opsi ini, Anda tidak dapat membuat IPAM.



5. Di bawah Wilayah Operasi, pilih AWS Wilayah di mana IPAM ini dapat mengelola dan menemukan sumber daya. AWSWilayah di mana Anda membuat IPAM Anda secara otomatis dipilih sebagai salah satu Wilayah operasi. Dalam tutorial ini, Wilayah rumah IPAM kami adalah us-east-1, jadi kami akan memilih us-west-1 dan us-west-2 sebagai Wilayah operasi tambahan. Jika Anda lupa Wilayah operasi, Anda dapat mengedit pengaturan IPAM Anda nanti dan menambah atau menghapus Wilayah.



6. Pilih Buat IPAM.



Langkah 3: Buat kolam IPAM tingkat atas

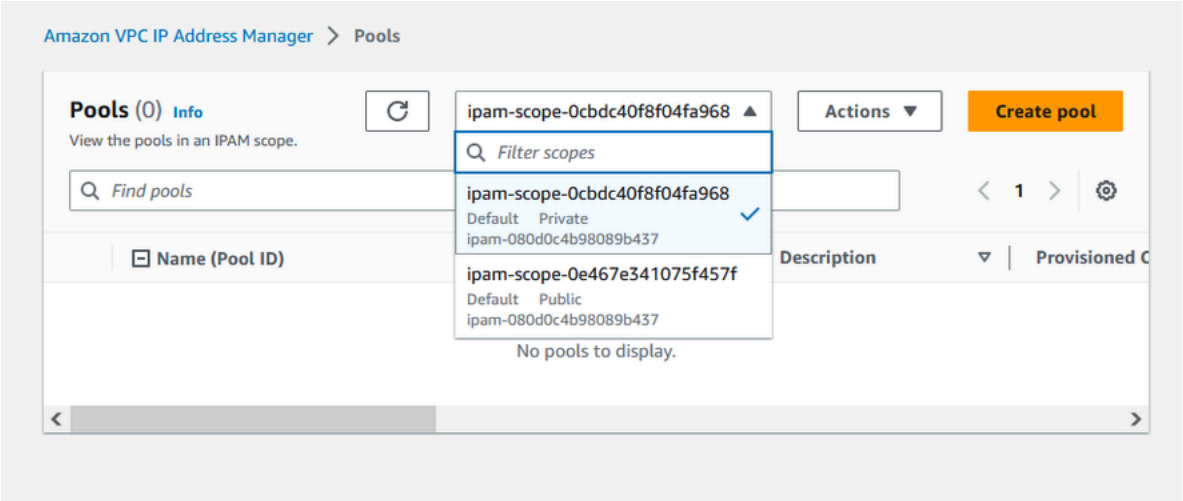
Dalam tutorial ini, Anda membuat hierarki pool dimulai dengan kolam IPAM tingkat atas. Pada langkah selanjutnya, Anda akan membuat sepasang kolam Regional dan kolam pengembangan pra-produksi di salah satu kolam regional.

Untuk informasi selengkapnya tentang hierarki kumpulan yang dapat Anda buat dengan IPAM, lihat. Contoh rencana kolam IPAM

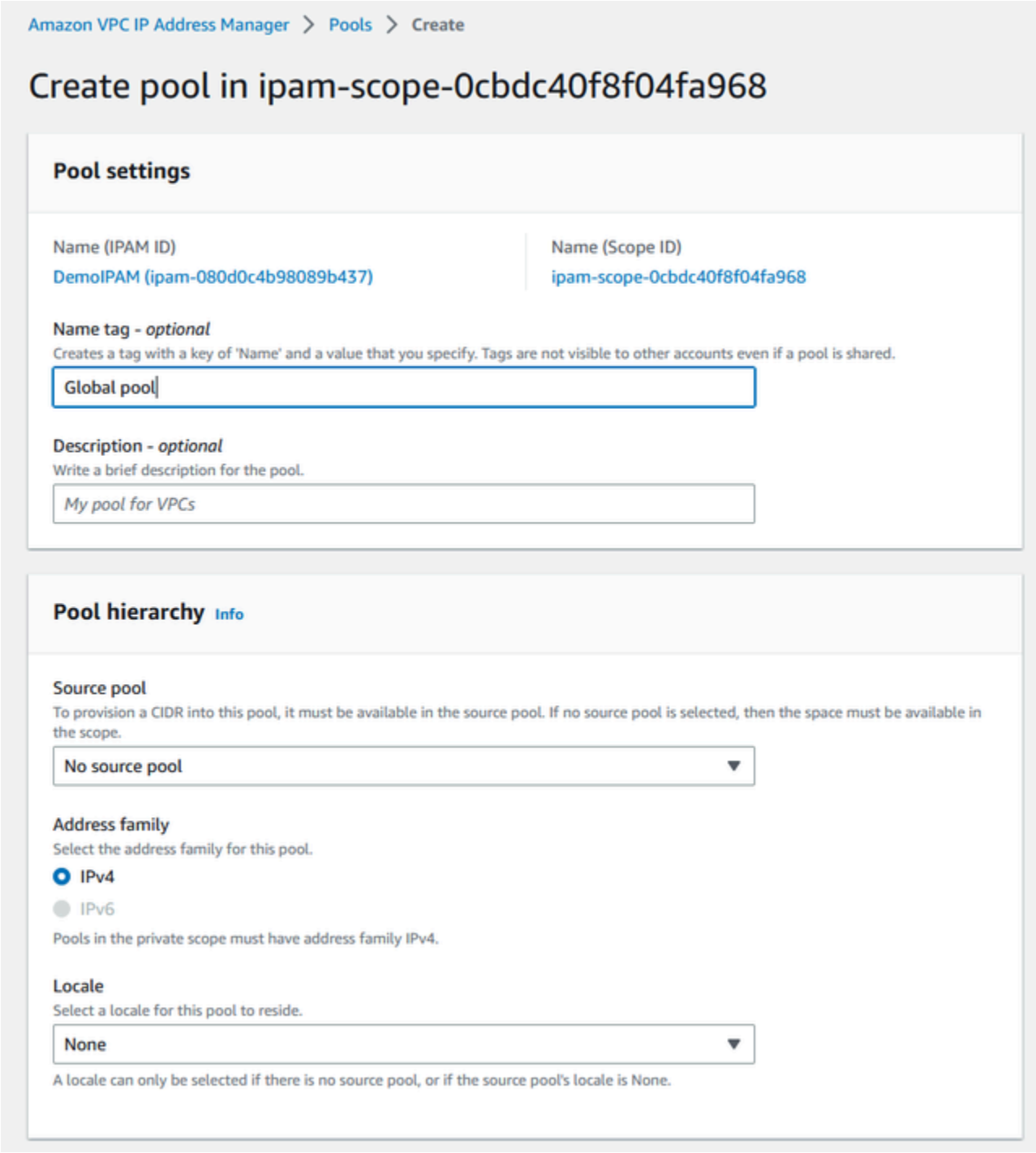
Untuk membuat kolam tingkat atas

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.

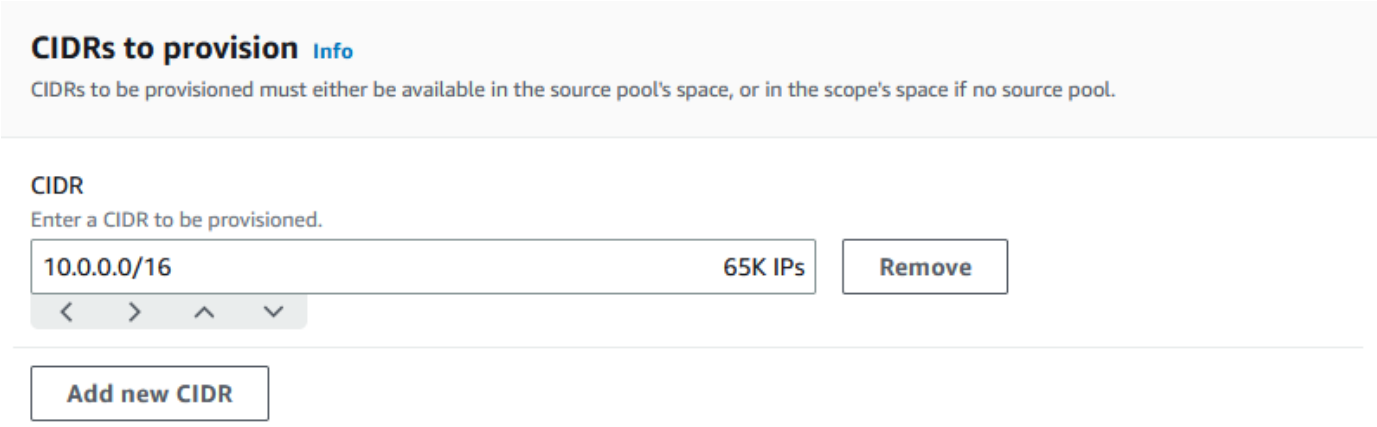
3. Pilih ruang lingkup pribadi.



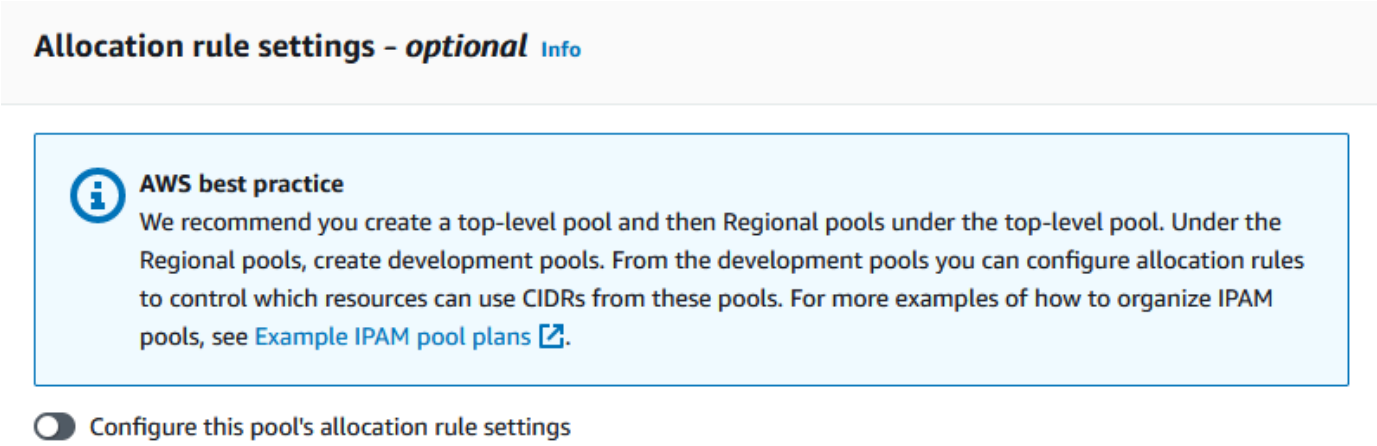
4. Pilih Buat kolam.
5. Di bawah lingkup IPAM, biarkan ruang lingkup pribadi dipilih.
6. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool, seperti “Global pool”.
7. Di bawah Sumber, pilih cakupan IPAM. Karena ini adalah kolam tingkat atas kami, itu tidak akan memiliki kolam sumber.
8. Di bawah Keluarga alamat, pilih IPv4.
9. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
10. Untuk Locale, pilih None. Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Anda akan mengatur lokal untuk kolam Regional yang Anda buat di bagian berikutnya dari tutorial ini.



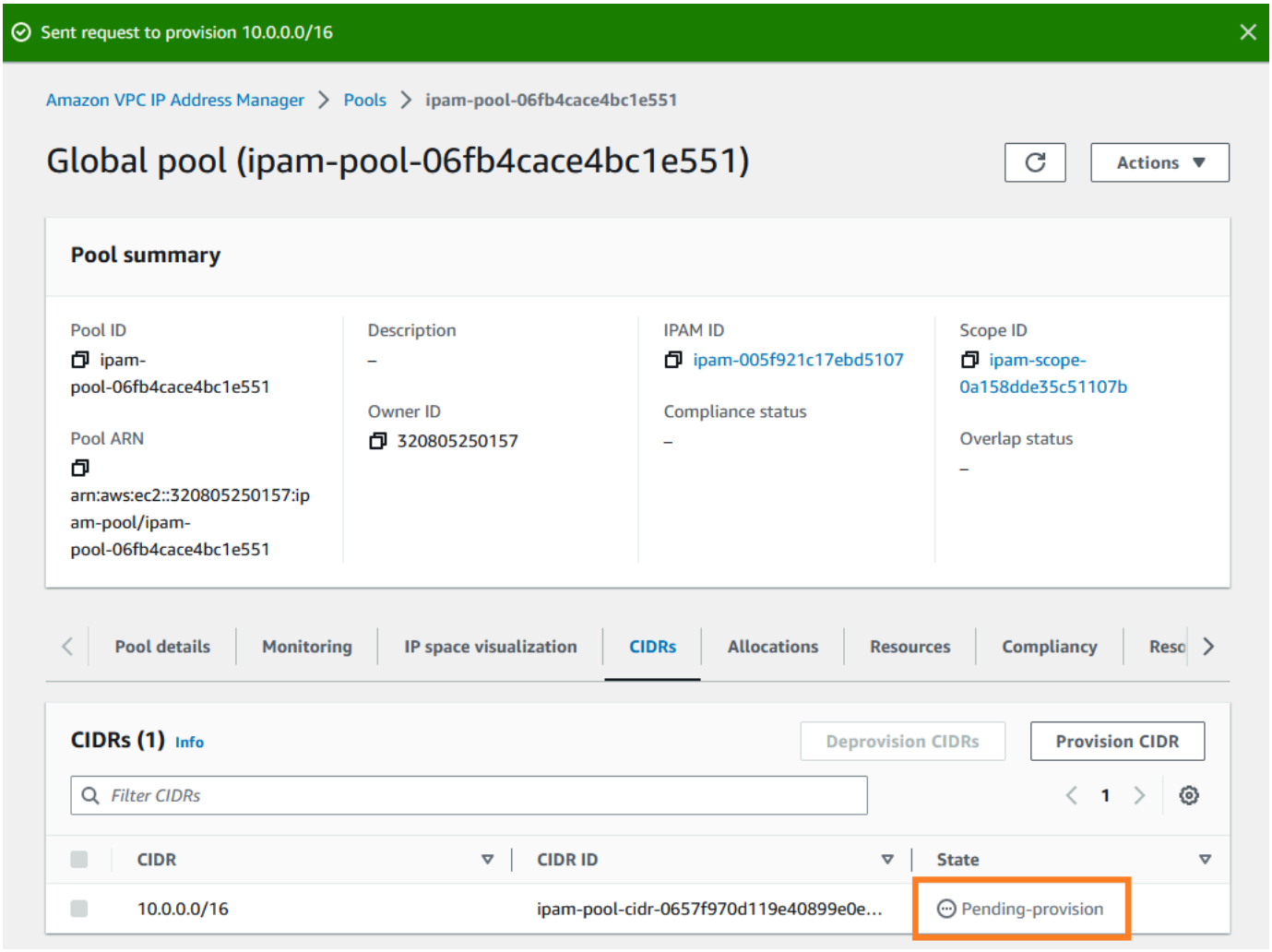
11. Pilih CIDR untuk penyediaan kolam renang. Dalam contoh ini, kami menyediakan 10.0.0.0/16.



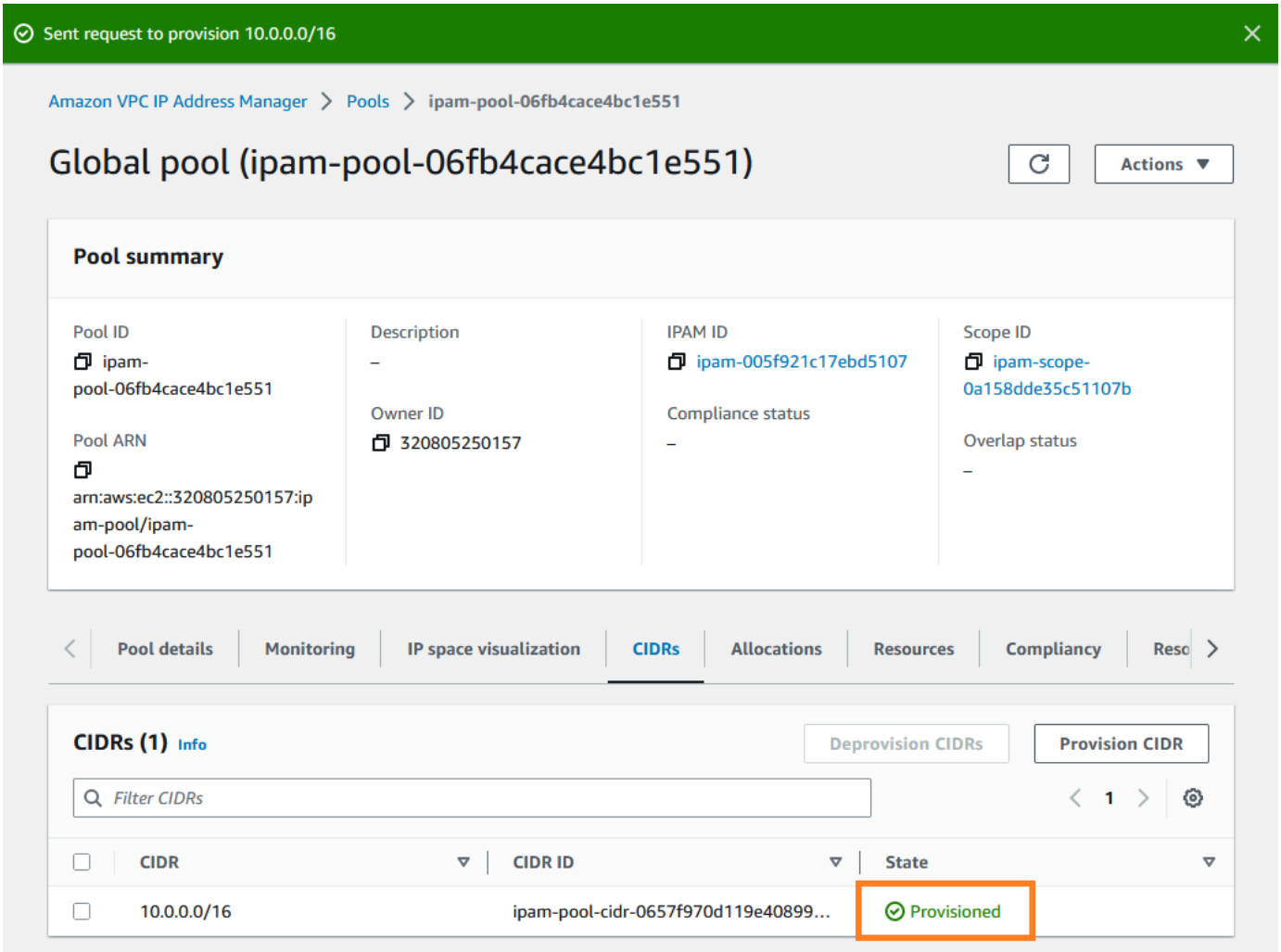
12. Biarkan Konfigurasi pengaturan aturan alokasi kumpulan ini dinonaktifkan. Ini adalah kolam tingkat atas kami, dan Anda tidak akan mengalokasikan CIDR ke VPC langsung dari kolam ini. Sebagai gantinya, Anda akan mengalokasikannya dari sub-pool yang Anda buat dari kolam ini.



13. Pilih Buat kolam. Pool dibuat dan CIDR berada dalam status Ketentuan Pending:



14. Tunggu status yang akan Disediakan sebelum Anda melanjutkan ke langkah berikutnya.



Sekarang setelah Anda membuat kolam tingkat atas, Anda akan membuat kumpulan Regional di us-barat-1 dan us-barat-2.

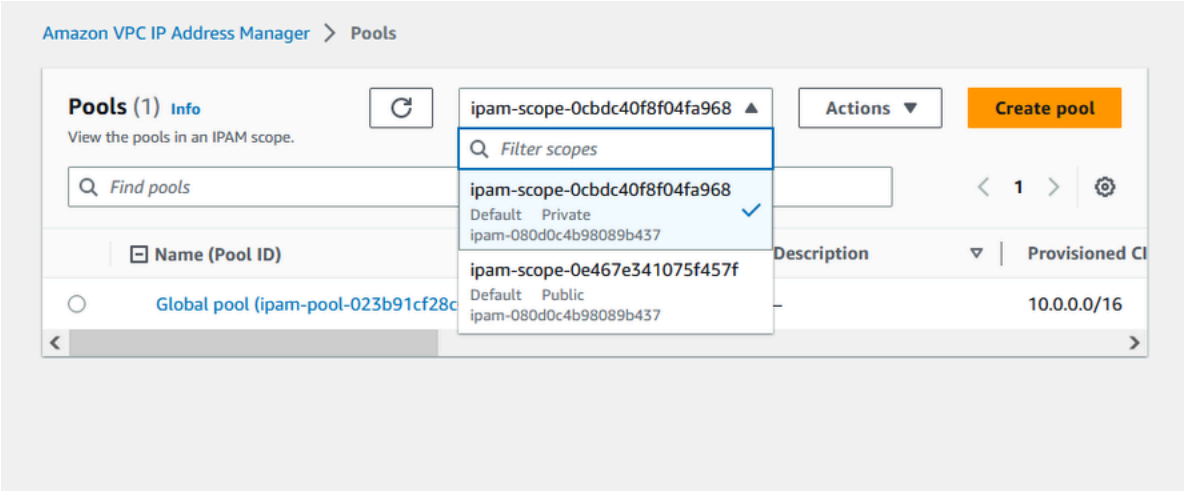
Langkah 4: Buat kolam IPAM Regional

Bagian ini menunjukkan cara mengatur alamat IP Anda menggunakan dua kumpulan Regional. Dalam tutorial ini, kami mengikuti salah satu contoh rencana kolam IPAM dan membuat dua kumpulan Regional yang dapat digunakan oleh akun anggota di organisasi Anda untuk mengalokasikan CIDR ke VPC mereka.

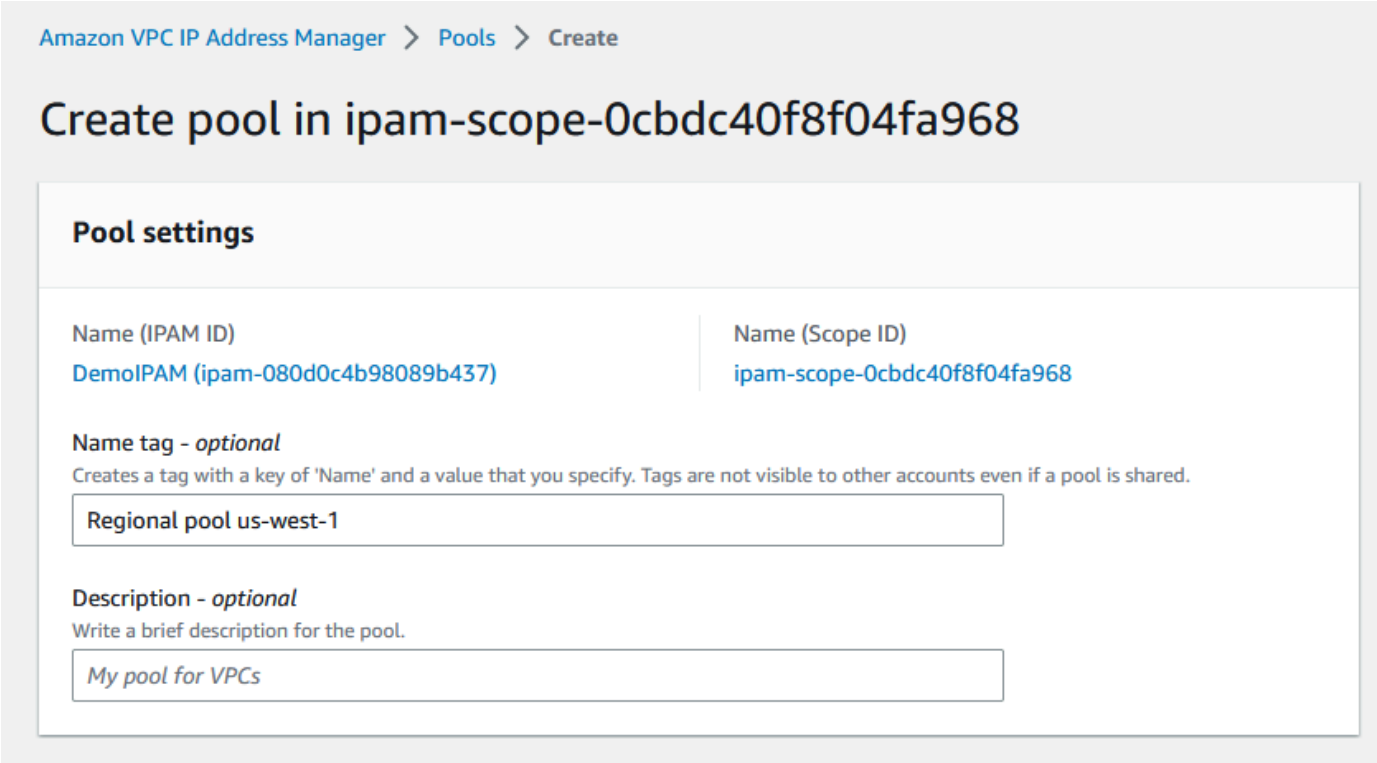
Untuk membuat kolam Regional

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.

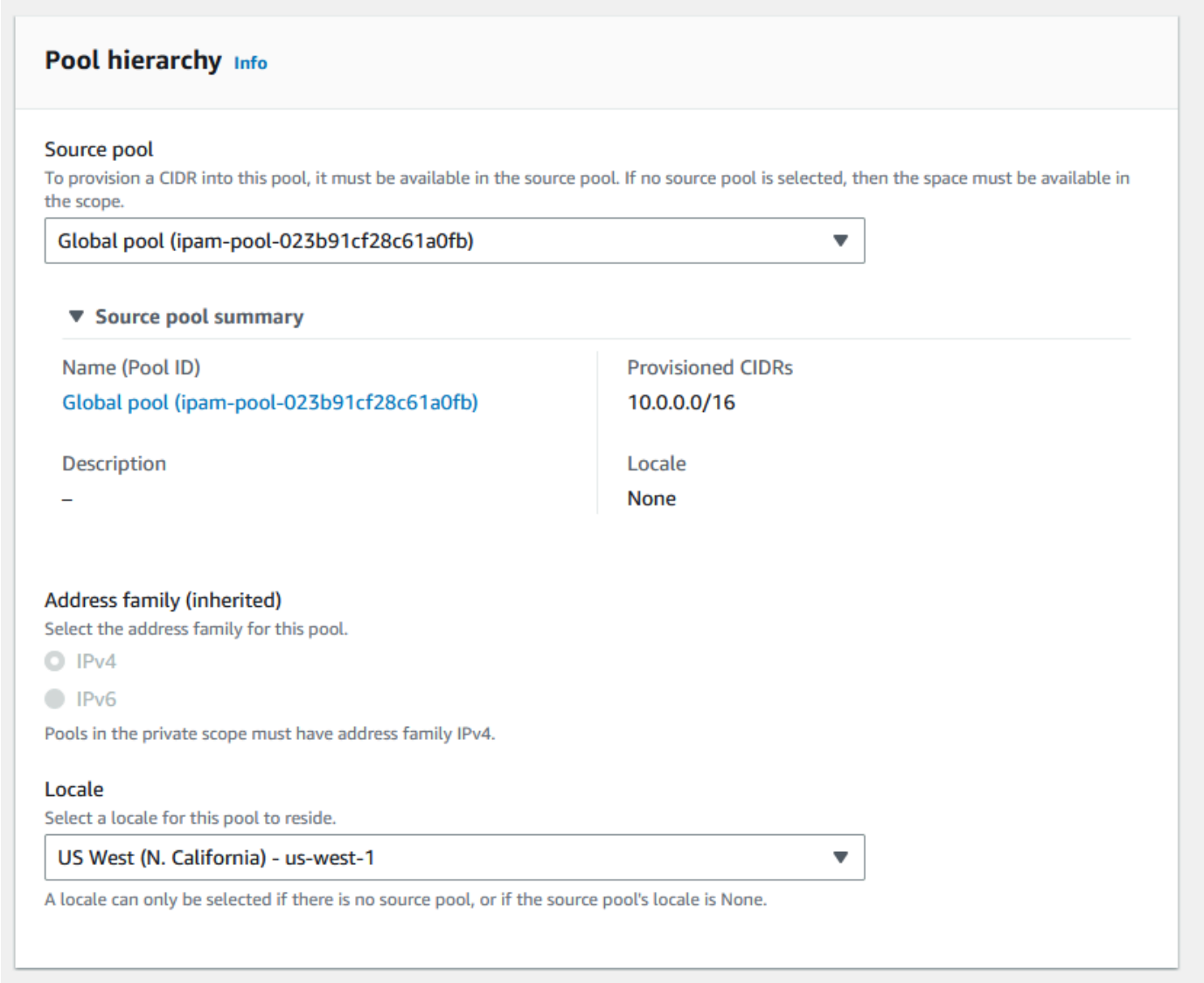
3. Pilih ruang lingkup pribadi.



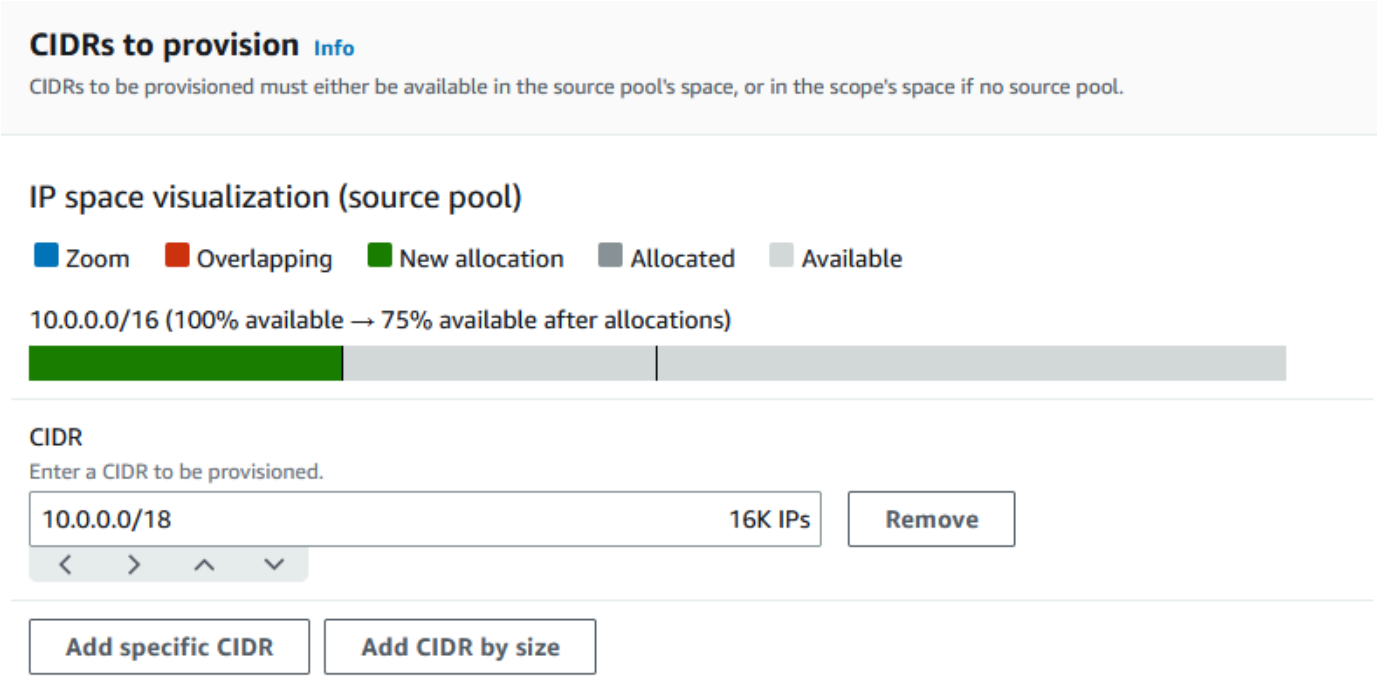
4. Pilih Buat kolam.
5. Di bawah lingkup IPAM, biarkan ruang lingkup pribadi dipilih.
6. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool, seperti Regional pool us-west-1.



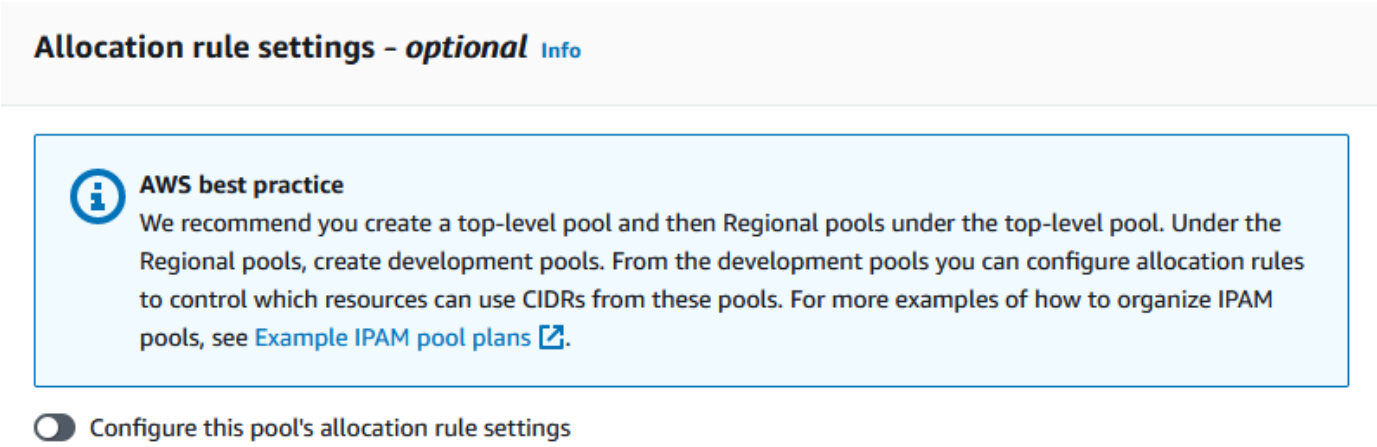
7. Di bawah Sumber, pilih kolam IPAM dan pilih kolam tingkat atas (“Kolam global”) yang Anda buat. Langkah 3: Buat kolam IPAM tingkat atas Kemudian, di bawah Locale, pilih us-west-1.



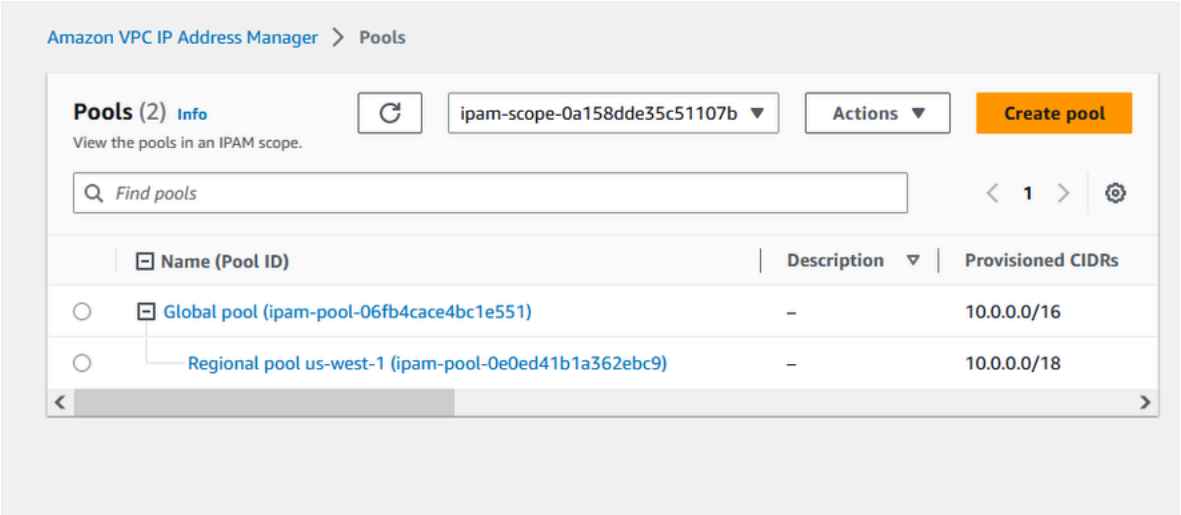
8. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
9. Di bawah CIDR untuk penyediaan, masukkan 10.0.0.0/18, yang akan memberikan kumpulan ini sekitar 16.000 alamat IP yang tersedia.



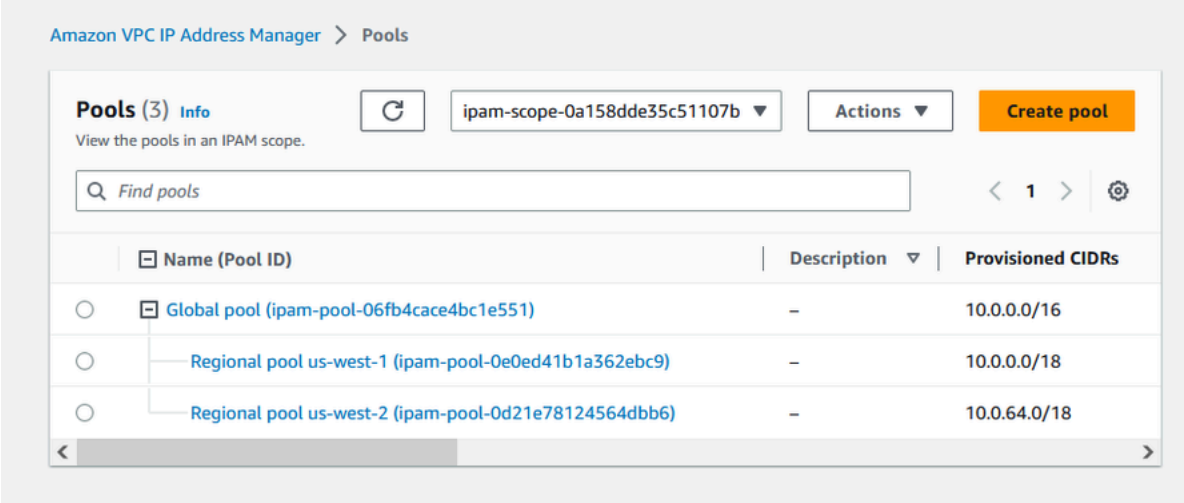
10. Biarkan Konfigurasi pengaturan aturan alokasi kumpulan ini dinonaktifkan. Anda tidak akan mengalokasikan CIDR ke VPC langsung dari kolam ini. Sebagai gantinya, Anda akan mengalokasikannya dari sub-pool yang Anda buat dari kolam ini.



11. Pilih Buat kolam.
12. Kembali ke tampilan Pools untuk melihat hierarki kolam IPAM yang telah Anda buat.



13. Ulangi langkah-langkah di bagian ini dan buat kumpulan Regional kedua di lokal us-barat-2 dengan CIDR 10.0.64.0/18 disediakan untuk itu. Saat Anda menyelesaikan proses itu, Anda akan memiliki tiga kumpulan dalam hierarki yang mirip dengan yang ini:

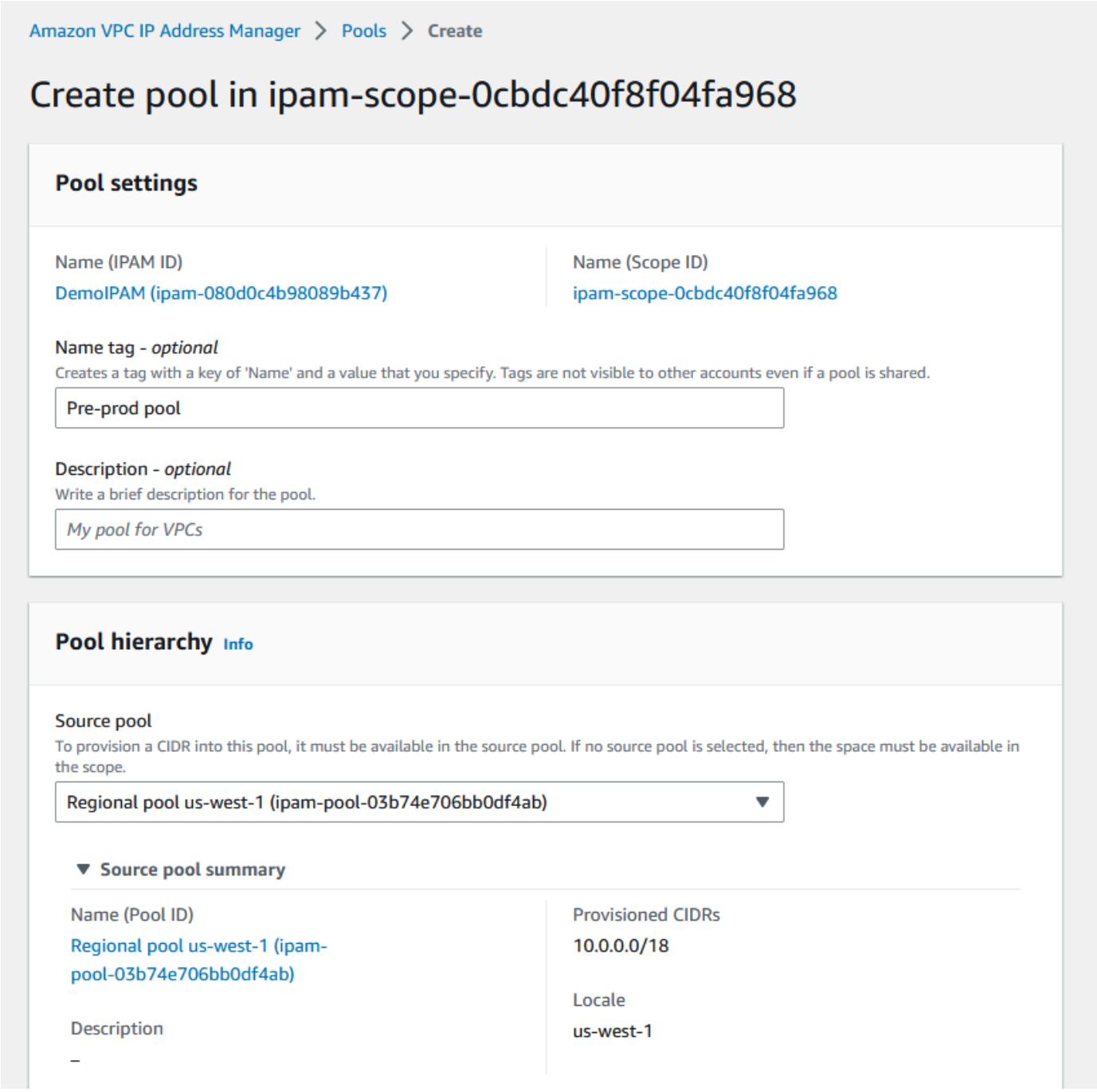


Langkah 5: Buat kumpulan pengembangan pra-produksi

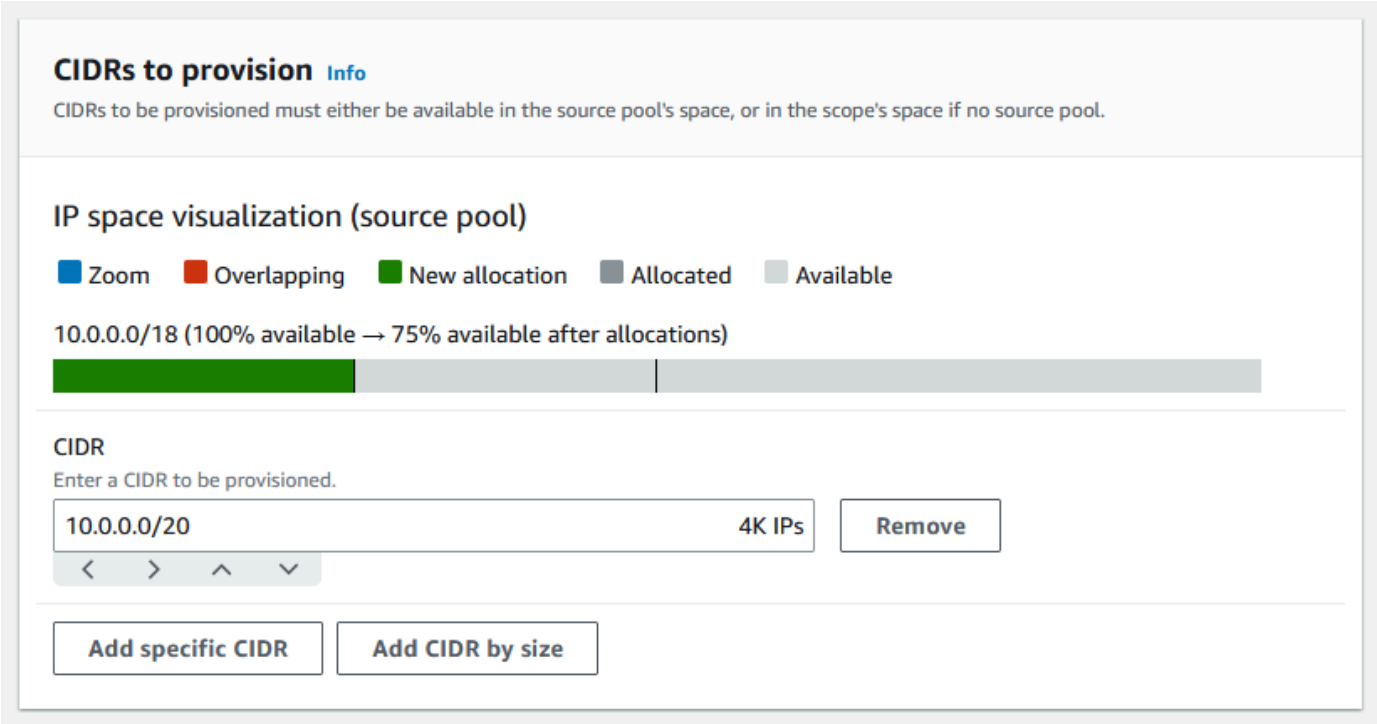
Ikuti langkah-langkah di bagian ini untuk membuat kumpulan pengembangan untuk sumber daya pra-produksi dalam salah satu kumpulan Regional Anda.

Untuk membuat kolam pengembangan pra-produksi

1. Dengan cara yang sama seperti yang Anda lakukan di bagian sebelumnya, menggunakan akun admin IPAM, buat pool yang disebut Pre-Prod pool, tapi kali ini gunakan Regional pool us-west-1 sebagai source pool.

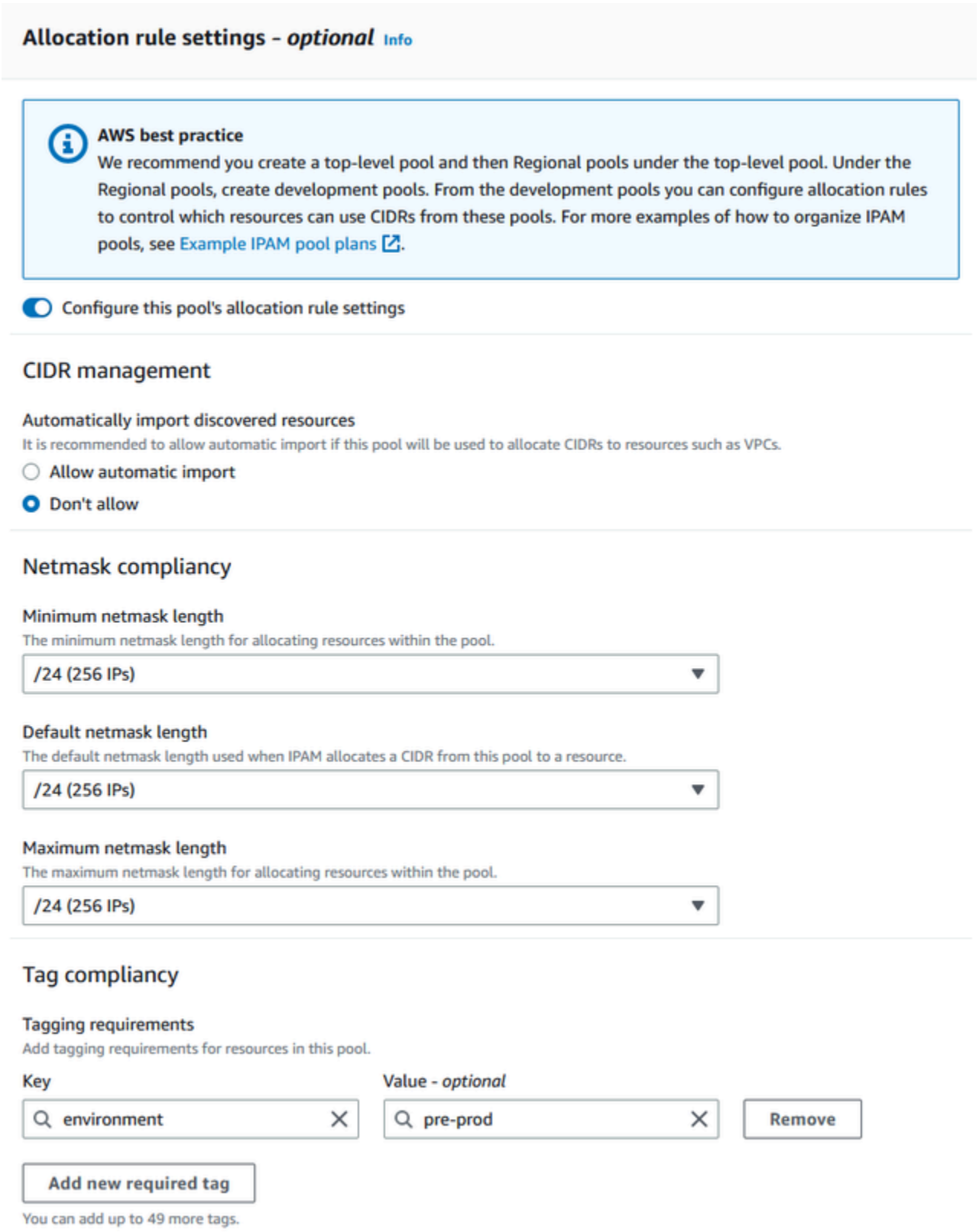


2. Tentukan CIDR 10.0.0.0/20 ke ketentuan, yang akan memberikan kumpulan ini sekitar 4.000 alamat IP.



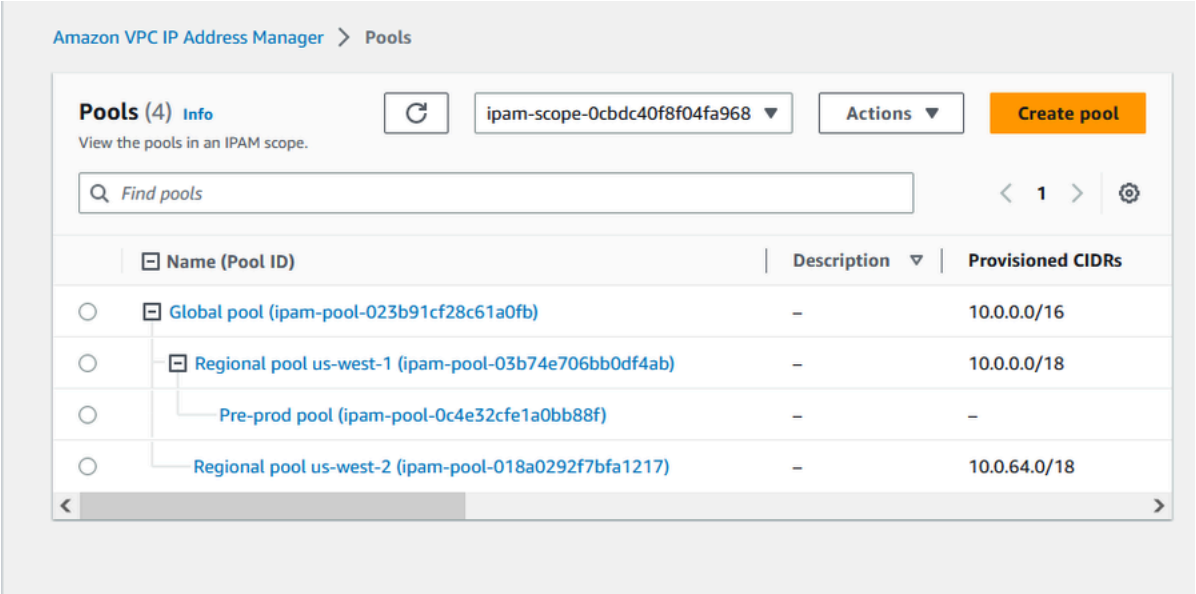
3. Alihkan opsi untuk Mengonfigurasi pengaturan aturan alokasi kumpulan ini. Lakukan hal berikut:

    1. Di bawah manajemen CIDR, untuk Mengimpor sumber daya yang ditemukan secara otomatis, biarkan opsi default Jangan izinkan dipilih. Opsi ini akan memungkinkan IPAM untuk secara otomatis mengimpor CIDR sumber daya yang ditemukannya di lokal kumpulan. Penjelasan rinci tentang opsi ini berada di luar cakupan tutorial ini, tetapi Anda dapat membaca lebih lanjut tentang opsi diBuat kolam IPv4 tingkat atas.
    2. Di bawah kepatuhan Netmask, pilih /24 untuk panjang netmask minimum, default, dan maksimum. Penjelasan rinci tentang opsi ini berada di luar cakupan tutorial ini, tetapi Anda dapat membaca lebih lanjut tentang opsi diBuat kolam IPv4 tingkat atas. Yang penting untuk dicatat adalah bahwa VPC yang Anda buat nanti dengan CIDR dari kumpulan ini akan dibatasi hingga /24 berdasarkan apa yang kami tetapkan di sini.
    3. Di bawah Kepatuhan Tag, masukkan lingkungan/pra-prod. Tag ini akan diperlukan untuk VPC untuk mengalokasikan ruang dari kolam. Kami akan menunjukkan nanti bagaimana ini bekerja.



4. Pilih Buat kolam.

5. Hirarki pool sekarang mencakup subpool tambahan di bawah Regional pool us-west-1:



Sekarang Anda siap untuk berbagi kumpulan IPAM dengan akun anggota lain di organisasi Anda dan mengaktifkan akun tersebut untuk mengalokasikan CIDR dari kumpulan untuk membuat VPC.

Langkah 6: Bagikan kolam IPAM

Ikuti langkah-langkah di bagian ini untuk berbagi kolam IPAM pra-produksi menggunakan AWS Resource Access Manager (RAM).

Bagian ini terdiri dari dua subbagian:

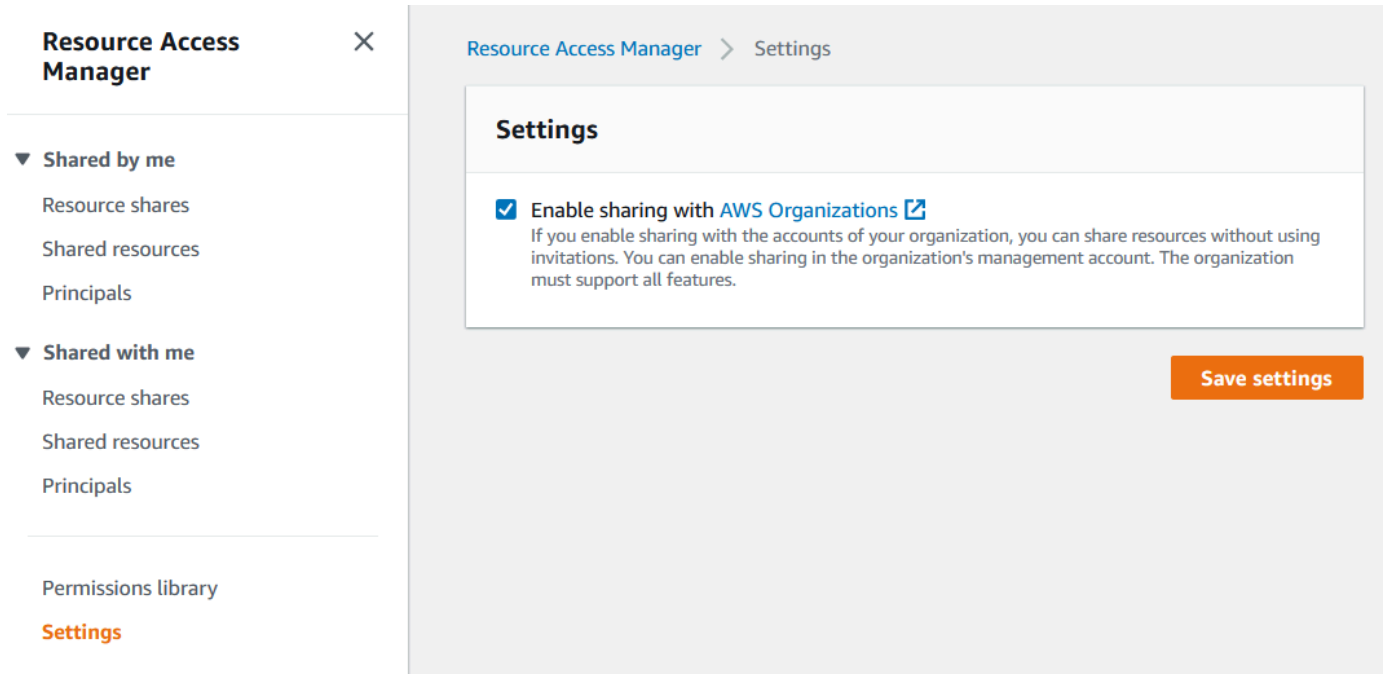
- Langkah 6.1. Aktifkan berbagi sumber daya di AWS RAM: Langkah ini harus dilakukan oleh akun AWS Organizations manajemen.
- Langkah 6.2. Bagikan kolam IPAM menggunakan AWS RAM: Langkah ini harus dilakukan oleh admin IPAM.

Langkah 6.1. Aktifkan berbagi sumber daya di AWS RAM

Setelah membuat IPAM, Anda akan ingin berbagi kumpulan alamat IP dengan akun lain di organisasi Anda. Sebelum Anda berbagi kolam IPAM, selesaikan langkah-langkah di bagian ini untuk mengaktifkan berbagi AWS RAM sumber daya.

Untuk mengaktifkan berbagi sumber daya

1. Menggunakan akun AWS Organizations manajemen, buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Di panel navigasi kiri, pilih Pengaturan, pilih Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.



Anda sekarang dapat berbagi kolam IPAM dengan anggota organisasi lainnya.

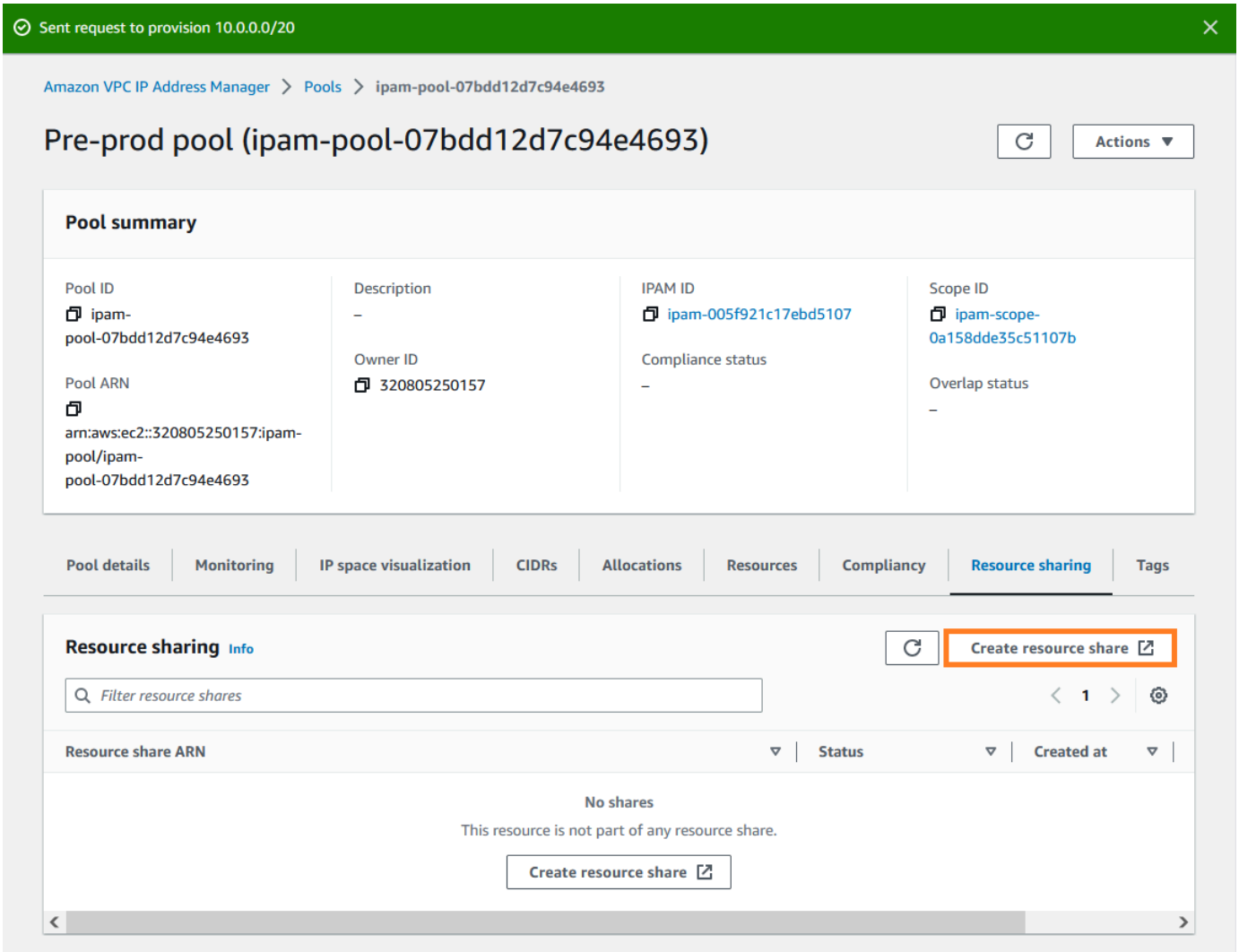
Langkah 6.2. Bagikan kolam IPAM menggunakan AWS RAM

Di bagian ini Anda akan membagikan kumpulan pengembangan pra-produksi dengan akun AWS Organizations anggota lain. Untuk petunjuk lengkap tentang berbagi kumpulan IPAM, termasuk informasi tentang izin IAM yang diperlukan, lihat. Membagikan kumpulan IPAM menggunakanAWS RAM

Untuk berbagi kolam IPAM menggunakan AWS RAM

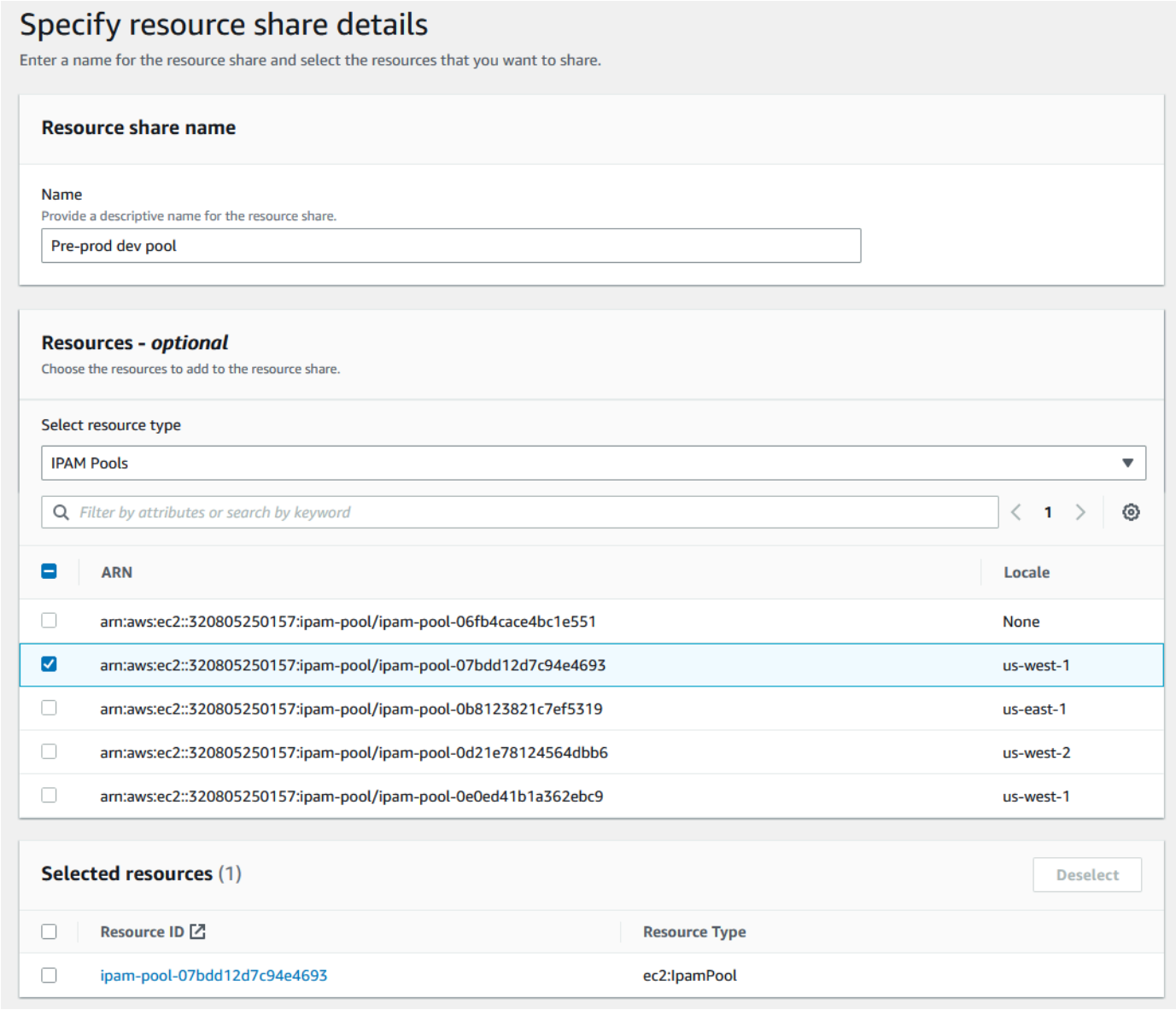
1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi, pilih kolam IPAM pra-produksi, dan pilih Tindakan > Lihat detail.
4. Di bawah Berbagi sumber daya, pilih Buat berbagi sumber daya. AWS RAMKonsol terbuka. Anda akan berbagi kolam menggunakanAWS RAM.

5. Pilih Buat berbagi sumber daya.

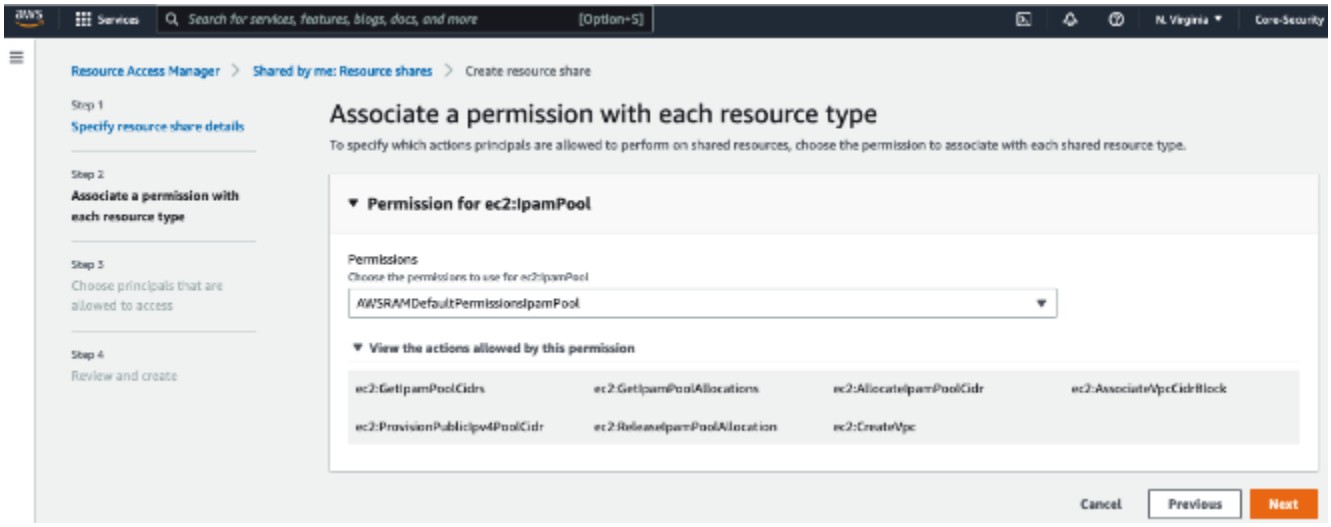


AWS RAMKonsol terbuka.

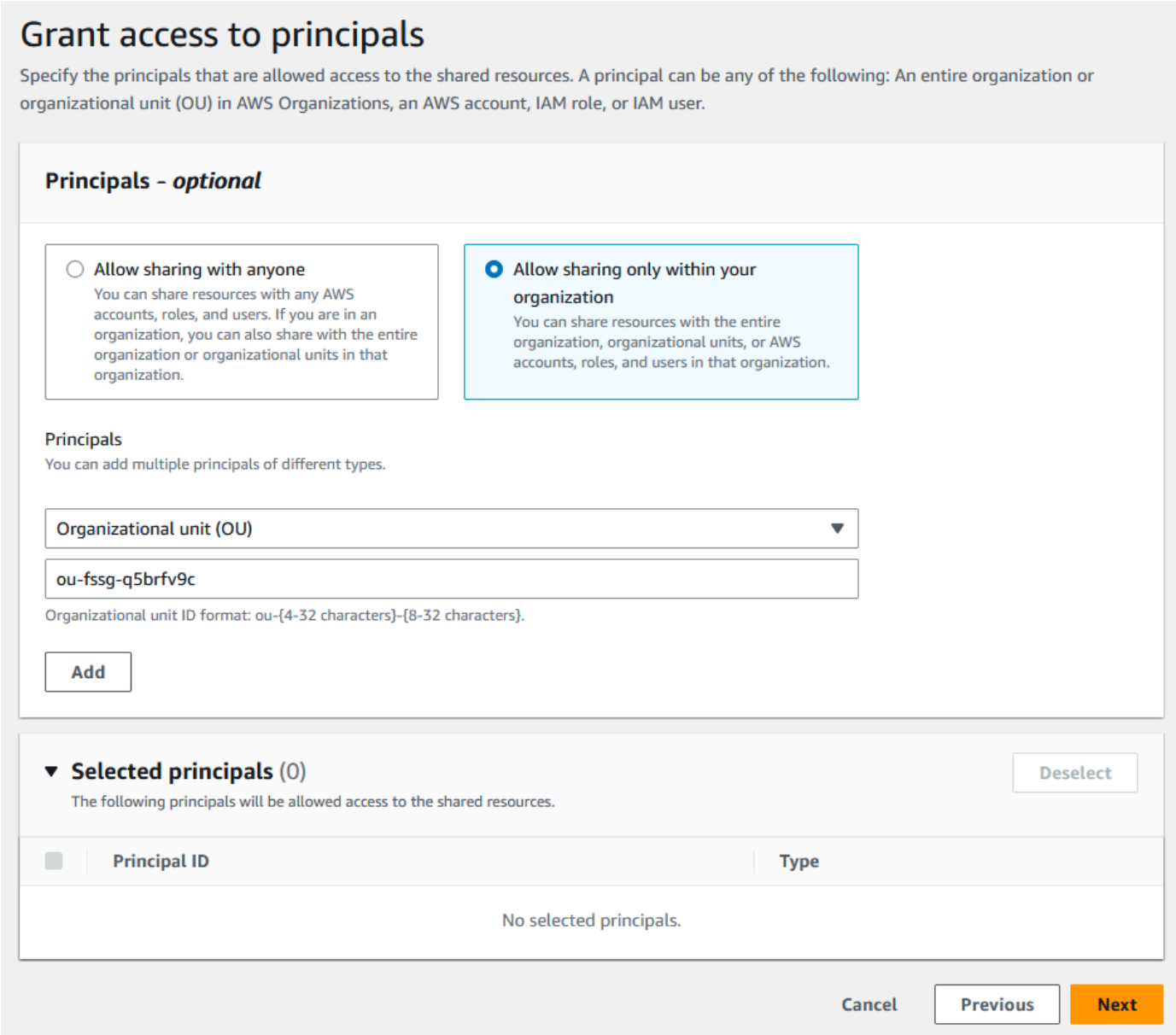
6. Di AWS RAM konsol, pilih Buat berbagi sumber daya lagi.
7. Tambahkan Nama untuk kolam bersama.
8. Di bawah Pilih jenis sumber daya, pilih kolam IPAM, lalu pilih ARN dari kumpulan pengembangan pra-produksi.



9. Pilih Selanjutnya.
10. Biarkan AWSRAMDefaultPermissionsIpamPoolizin default dipilih. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini di[Membagikan kumpulan IPAM menggunakanAWS RAM](#).



11. Pilih Selanjutnya.
12. Di bawah Prinsipal, pilih Izinkan berbagi hanya dalam organisasi Anda. Masukkan ID unit AWS Organizations organisasi Anda (seperti yang disebutkan dalamBagaimana AWS Organizations terintegrasi dengan IPAM, lalu pilih Tambah.



13. Pilih Selanjutnya.
14. Tinjau opsi berbagi sumber daya dan prinsipal yang akan Anda bagikan, lalu pilih Buat.

Sekarang setelah pool telah dibagikan, lanjutkan ke langkah berikutnya untuk membuat VPC dengan CIDR yang dialokasikan dari kolam IPAM.

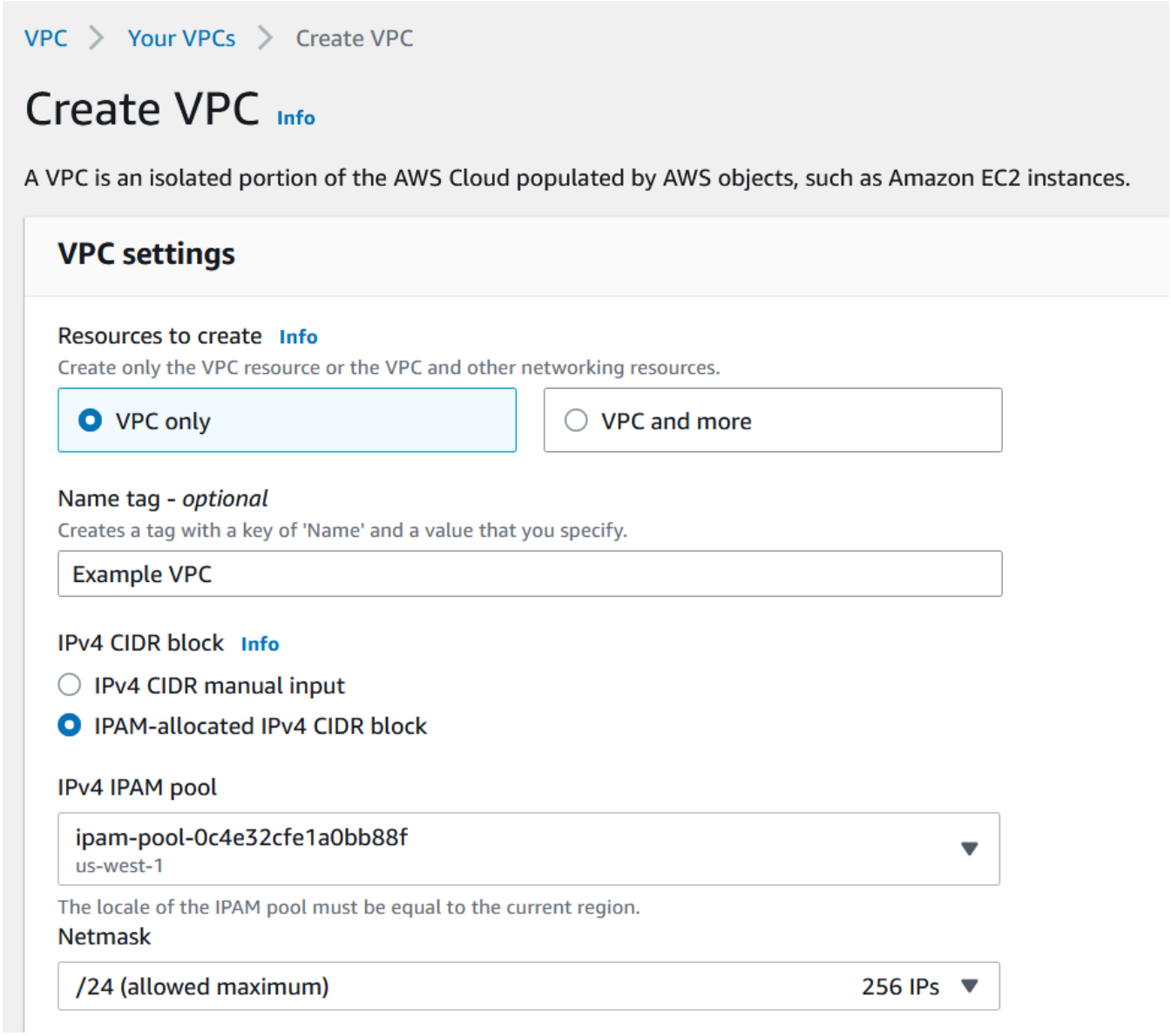
Langkah 7: Buat VPC dengan CIDR yang dialokasikan dari kolam IPAM

Ikuti langkah-langkah di bagian ini untuk membuat VPC dengan CIDR yang dialokasikan dari kumpulan pra-produksi. Langkah ini harus diselesaikan oleh akun anggota di OU tempat kolam IPAM dibagikan di bagian sebelumnya (disebut example-member-account-2 inBagaimana AWS

Organizations terintegrasi dengan IPAM). Untuk informasi selengkapnya tentang izin IAM yang diperlukan untuk membuat VPC, lihat contoh kebijakan Amazon VPC di Panduan Pengguna Amazon VPC.

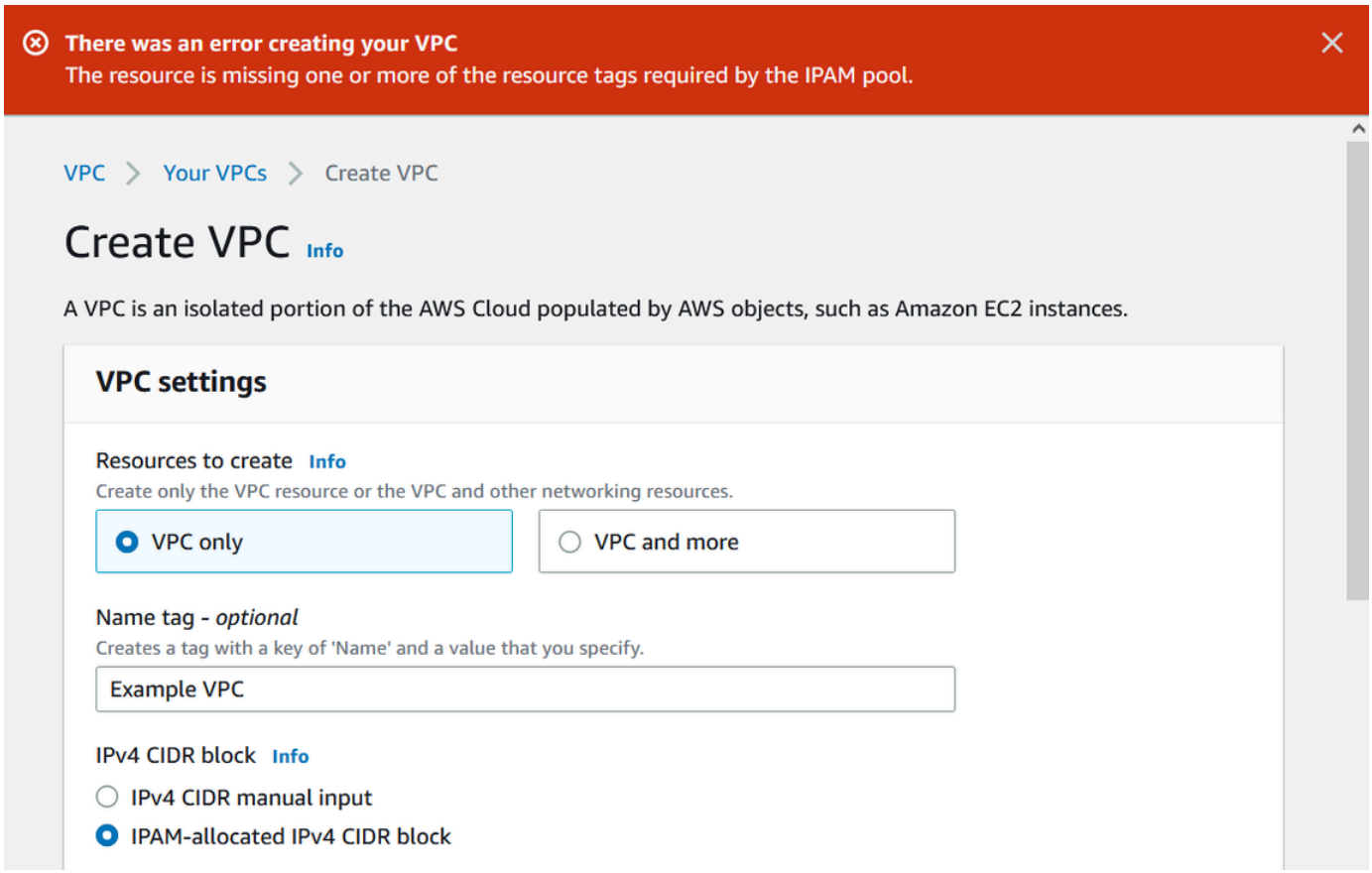
Untuk membuat VPC dengan CIDR yang dialokasikan dari kolam IPAM

1. Menggunakan akun anggota, buka konsol VPC di https://console.aws.amazon.com/vpc/ sebagai akun anggota yang akan Anda gunakan sebagai akun pengembang.
2. Pilih Buat VPC.
3. Lakukan hal berikut:
    1. Masukkan nama, seperti Contoh VPC.
    2. Pilih blok IPv4 CIDR yang dialokasikan IPAM.
    3. Di bawah IPv4 IPAM pool, pilih ID dari kolam pra-produksi.
    4. Pilih panjang Netmask. Karena Anda membatasi panjang netmask yang tersedia untuk kumpulan ini menjadi /24 (inLangkah 5: Buat kumpulan pengembangan pra-produksi), satu-satunya opsi netmask yang tersedia adalah /24.

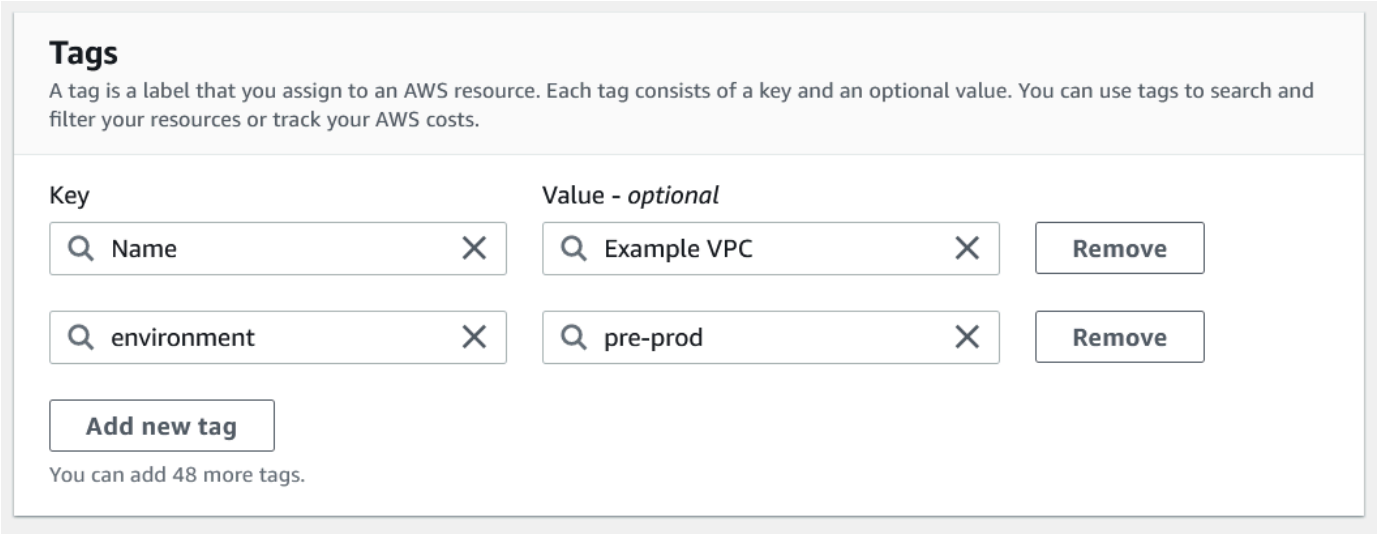


4. Untuk tujuan demonstrasi, di bawah Tag, jangan menambahkan tag tambahan saat ini. Saat Anda membuat kolam pra-prod (dalam 5. Buat kumpulan pengembangan pra-produksi), Anda menambahkan aturan alokasi yang mengharuskan VPC apa pun yang dibuat dengan CIDR dari kumpulan ini untuk memiliki tag lingkungan/pra-prod. Biarkan tag lingkungan/pra-prod untuk saat ini sehingga Anda dapat melihat bahwa kesalahan muncul yang memberi tahu Anda bahwa tag yang diperlukan tidak ditambahkan.
5. Pilih Buat VPC.
6. Kesalahan muncul memberi tahu Anda bahwa tag yang diperlukan tidak ditambahkan. Kesalahan muncul karena Anda menetapkan aturan alokasi saat Anda membuat kumpulan pra-prod (in). Langkah 5: Buat kumpulan pengembangan pra-produksi Aturan alokasi mengharuskan

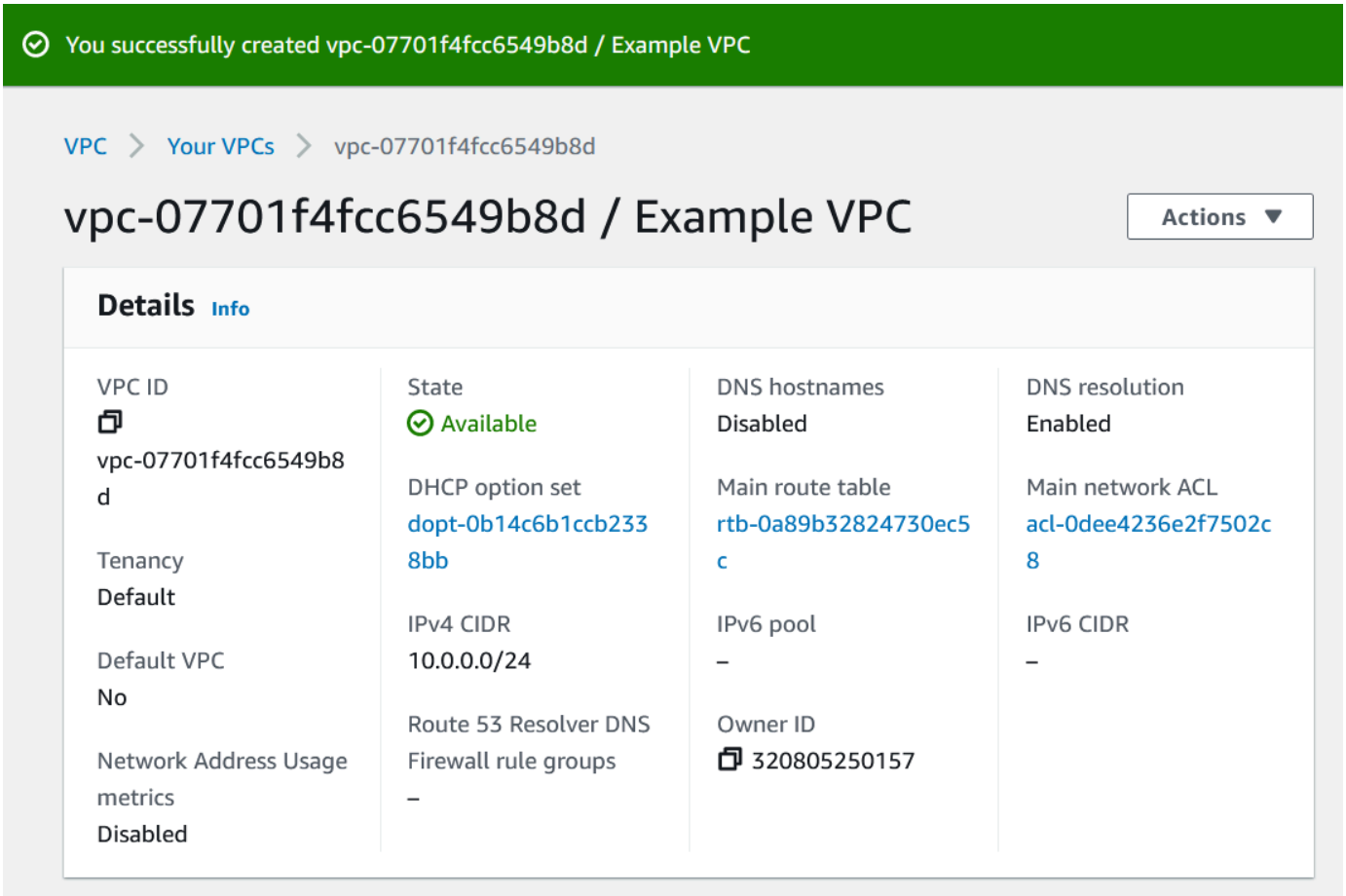
VPC apa pun yang dibuat dengan CIDR dari kumpulan ini untuk memiliki tag lingkungan/pra-prod.



7. Sekarang, di bawah Tag, tambahkan tag environment/pre-prod dan pilih Create VPC lagi.



8. VPC berhasil dibuat, dan VPC mematuhi aturan tag pada kumpulan pra-produksi:



Di panel Sumber Daya konsol IPAM, admin IPAM akan dapat melihat dan mengelola VPC dan CIDR yang dialokasikan. Perhatikan bahwa VPC membutuhkan beberapa waktu untuk muncul di panel Resources.

Langkah 8: Pembersihan

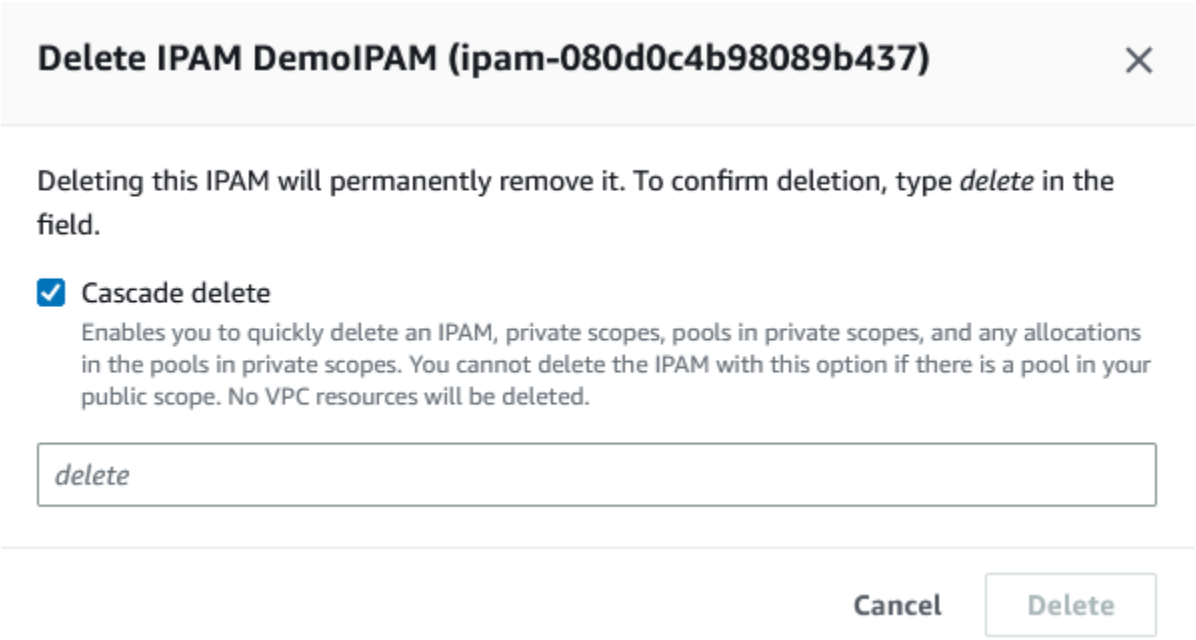
Dalam tutorial ini, Anda membuat IPAM dengan admin yang didelegasikan, membuat beberapa pool, dan mengaktifkan akun anggota di organisasi Anda untuk mengalokasikan CIDR VPC dari pool.

Ikuti langkah-langkah di bagian ini untuk membersihkan sumber daya yang Anda buat dalam tutorial ini.

Untuk membersihkan sumber daya yang dibuat dalam tutorial ini

1. Menggunakan akun anggota yang membuat contoh VPC, hapus VPC. Untuk petunjuk selengkapnya, lihat Menghapus VPC Anda di Panduan Pengguna Amazon Virtual Private Cloud.

2. Menggunakan akun admin IPAM, hapus contoh berbagi sumber daya di AWS RAM konsol. Untuk petunjuk terperinci, lihat Menghapus bagian sumber daya AWSAWS RAM di Panduan AWS Resource Access Manager Pengguna.
3. Menggunakan akun admin IPAM, masuk ke konsol RAM dan nonaktifkan berbagi dengan AWS Organizations yang Anda aktifkan. Langkah 6.1. Aktifkan berbagi sumber daya di AWS RAM
4. Menggunakan akun admin IPAM, hapus contoh IPAM dengan memilih IPAM di konsol IPAM dan kemudian memilih Actions > Delete. Untuk instruksi detail, lihat Menghapus IPAM.
5. Ketika Anda diminta untuk menghapus IPAM, pilih Cascade delete. Ini akan menghapus semua cakupan dan kumpulan dalam IPAM sebelum menghapus IPAM.



6. Masukkan hapus dan kemudian pilih Hapus.
7. Menggunakan akun AWS Organizations manajemen, masuk ke konsol IPAM, pilih Pengaturan, dan hapus akun administrator yang didelegasikan.
8. (Opsional) Saat Anda mengintegrasikan IPAM denganAWS Organizations, IPAM secara otomatis membuat peran terkait layanan di setiap akun anggota. Dengan menggunakan setiap akun AWS Organizations anggota, masuk ke IAM dan hapus peran terkait AWSServiceRoleForIPAMlayanan di setiap akun anggota.
9. Pembersihan selesai.

Tutorial: Buat IPAM dan pool menggunakanAWS CLI

Ikuti langkah-langkah dalam tutorial ini untuk menggunakanAWS CLI untuk membuat IPAM, membuat kolam alamat IP, dan mengalokasikan VPC dengan CIDR dari kolam IPAM.

Berikut ini adalah contoh hirarki struktur pool yang akan Anda buat dengan mengikuti langkah-langkah di bagian ini:

- IPAM beroperasi diAWS Wilayah 1,AWS Wilayah 2
  - Lingkup pribadi
    - Kolam tingkat atas
      - Kolam renang regional diAWS Wilayah 2
        - Kolam pengembangan
          - Alokasi untuk VPC

> **Note**
>
> Di bagian ini, Anda akan membuat IPAM. Secara default, Anda hanya dapat membuat satu IPAM. Untuk informasi selengkapnya, lihat Kuota untuk IPAM Anda. Jika Anda telah mendelegasikan akun IPAM dan membuat IPAM, Anda dapat melewati langkah 1 dan 2.

Daftar Isi

- Langkah 1: Aktifkan IPAM di organisasi
- Langkah 2: Buat IPAM
- Langkah 3: Buat kolam alamat IPv4
- Langkah 4: Menyediakan CIDR pada pool tingkat atas
- Langkah 5. Buat kolam Regional dengan CIDR yang bersumber dari kolam renang tingkat atas
- Langkah 6: Menyediakan CIDR ke kolam Regional
- Langkah 7. Buat berbagi RAM untuk mengaktifkan penetapan IP di seluruh akun
- Langkah 8. Buat VPC
- Langkah 9. Pembersihan

Langkah 1: Aktifkan IPAM di organisasi

Langkah ini opsional. Selesaikan langkah ini untuk mengaktifkan IPAM di organisasi Anda dan konfigurasikan IPAM Anda yang didelegasikan menggunakanAWS CLI. Untuk informasi lebih lanjut tentang peran akun IPAM, lihatIntegrasikan IPAM dengan akun di Organisasi AWS.

Permintaan ini harus dibuat dari akun manajemenAWS Organizations. Saat menjalankan perintah berikut, pastikan Anda menggunakan peran dengan kebijakan IAM yang mengizinkan tindakan berikut:

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

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

Anda akan melihat output berikut, menunjukkan bahwa mengaktifkan berhasil.

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

Langkah 2: Buat IPAM

Ikuti langkah-langkah di bagian ini untuk membuat IPAM dan menampilkan informasi tambahan tentang cakupan yang dibuat. Anda akan menggunakan IPAM ini saat membuat kumpulan dan menyediakan rentang alamat IP untuk kumpulan tersebut di langkah selanjutnya.

> **Note**
>
> Opsi Wilayah operasi menentukanAWS Wilayah mana kolam IPAM dapat digunakan. Untuk informasi lebih lanjut tentang Wilayah operasi, lihatBuat IPAM.

Untuk membuat IPAM menggunakanAWS CLI

1. Jalankan perintah berikut ini untuk membuat instans IPAM.

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

   Ketika Anda membuat IPAM,AWS secara otomatis melakukan hal berikut:

   - Mengembalikan ID sumber daya yang unik secara global (`IpamId`) untuk IPAM.
   - Menciptakan lingkup publik default (`PublicDefaultScopeId`) dan lingkup pribadi default (`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. Jalankan perintah berikut ini untuk menampilkan informasi tambahan yang terkait dengan cakupan. Ruang lingkup publik ditujukan untuk alamat IP yang akan diakses melalui internet publik. Ruang lingkup pribadi ditujukan untuk alamat IP yang tidak akan diakses melalui internet publik.

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

Dalam output, Anda melihat cakupan yang tersedia. Anda akan menggunakan ID lingkup pribadi di langkah berikutnya.

```
{
    "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
        }
    ]
}
```

Langkah 3: Buat kolam alamat IPv4

Ikuti langkah-langkah di bagian ini untuk membuat kolam alamat IPv4.

Important

Anda tidak akan menggunakan`--locale` opsi di pool tingkat atas ini. Anda akan mengatur opsi lokal nanti di kolam Regional. Lokal adalah Wilayah AWS tempat Anda ingin pool tersedia untuk alokasi CIDR. Sebagai hasil dari tidak mengatur lokal pada pool tingkat atas,

lokal akan default keNone. Jika kolam memiliki lokalNone, pangkalan tidak akan tersedia untuk sumber daya VPC diAWS Wilayah mana pun. Anda hanya dapat secara manual mengalokasikan ruang alamat IP di kolam renang untuk memesan ruang.

Untuk membuat pool alamat IPv4 untuk semuaAWS sumber daya Anda menggunakanAWS CLI

1. Jalankan perintah berikut ini untuk membuat kolam alamat IPv4. Gunakan ID lingkup pribadi IPAM yang Anda buat di langkah sebelumnya.

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

   Dalam output, Anda akan melihat keadaancreate-in-progress untuk kolam renang.

```
{
    "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. Jalankan perintah berikut sampai Anda melihat keadaancreate-complete di output.

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

   Output contoh berikut menunjukkan keadaan yang benar.

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

Langkah 4: Menyediakan CIDR pada pool tingkat atas

Ikuti langkah-langkah di bagian ini untuk menyediakan CIDR ke pangkalan tingkat atas, dan kemudian verifikasi bahwa CIDR disediakan. Untuk informasi selengkapnya, lihat Menyediakan CIDR ke kolam.

Untuk menyediakan blok CIDR ke pool menggunakanAWS CLI

1. Jalankan perintah berikut ini untuk menyediakan CIDR.

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

   Dalam output, Anda dapat memverifikasi status penyediaan.

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

```
    }
}
```

2. Jalankan perintah berikut sampai Anda melihat keadaan`provisioned` di output.

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

Output contoh berikut menunjukkan keadaan yang benar.

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

Langkah 5. Buat kolam Regional dengan CIDR yang bersumber dari kolam renang tingkat atas

Ketika Anda membuat kolam IPAM, pool milikAWS Wilayah IPAM secara default. Saat Anda membuat VPC, kumpulan yang diambil VPC harus berada di Wilayah yang sama dengan VPC. Anda dapat menggunakan`--locale` opsi ketika Anda membuat pool untuk membuat pool tersedia untuk layanan di Wilayah selain Wilayah IPAM. Ikuti langkah-langkah di bagian ini untuk membuat kolam Regional di lokal lain.

Untuk membuat pool dengan CIDR yang bersumber dari pool sebelumnya menggunakanAWS CLI

1. Jalankan perintah berikut untuk membuat pool dan masukkan spasi dengan CIDR yang tersedia yang diketahui dari pool sebelumnya.

```
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
```

Pada output, Anda akan melihat ID pool yang Anda buat. Anda akan membutuhkan ID ini di langkah berikutnya.

```
{
    "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. Jalankan perintah berikut sampai Anda melihat keadaan`create-complete` di output.

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

Dalam output, Anda melihat kolam yang Anda miliki di IPAM Anda. Dalam tutorial ini, kita membuat tingkat atas dan kolam Regional, sehingga Anda akan melihat mereka berdua.

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

Langkah 6: Menyediakan CIDR ke kolam Regional

Ikuti langkah-langkah di bagian ini untuk menetapkan blok CIDR ke pangkalan, dan validasi bahwa blok tersebut telah berhasil disediakan.

Untuk menetapkan blok CIDR ke kolam Regional menggunakanAWS CLI

1. Jalankan perintah berikut ini untuk menyediakan CIDR.

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

   Dalam output, Anda melihat keadaan kolam renang.

```
{
    "IpamPoolCidr": {
```

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

2. Jalankan perintah berikut sampai Anda melihat keadaan`provisioned` di output.

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

Output contoh berikut menunjukkan keadaan yang benar.

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

3. Jalankan perintah berikut ini untuk melakukan kueri kolam tingkat atas untuk menampilkan alokasi. Kolam Regional dianggap sebagai alokasi dalam kolam renang tingkat atas.

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

Dalam output, Anda melihat kolam Regional sebagai alokasi di kolam tingkat atas.

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

Langkah 7. Buat berbagi RAM untuk mengaktifkan penetapan IP di seluruh akun

Langkah ini opsional. Anda dapat menyelesaikan langkah ini hanya jika Anda selesaiIntegrasikan IPAM dengan akun di Organisasi AWS.

Saat Anda membuat pangsaAWS RAM kumpulan IPAM, ini memungkinkan penugasan IP di seluruh akun. Berbagi RAM hanya tersedia diAWS Wilayah rumah Anda. Perhatikan bahwa Anda membuat bagian ini di Wilayah yang sama dengan IPAM, bukan di Wilayah lokal untuk pangkalan. Semua operasi administratif pada sumber daya IPAM dilakukan melalui Wilayah asal IPAM Anda. Contoh dalam tutorial ini menciptakan satu share untuk satu pool, tetapi Anda dapat menambahkan beberapa pool ke satu share. Untuk informasi lebih lanjut, termasuk penjelasan tentang opsi yang harus Anda masukkan, lihatMembagikan kumpulan IPAM menggunakanAWS RAM.

Jalankan perintah berikut ini untuk membuat share sumber daya.

```
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
```

Output menunjukkan bahwa kolam telah dibuat.

```
{
    "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
    }
}
```

Langkah 8. Buat VPC

Jalankan perintah berikut untuk membuat VPC dan menetapkan blok CIDR ke VPC dari pool di IPAM yang baru dibuat.

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

Output menunjukkan bahwa VPC telah dibuat.

```
{
    "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
    }
}
```

Langkah 9. Pembersihan

Ikuti langkah-langkah di bagian ini untuk menghapus sumber IPAM yang telah Anda buat dalam tutorial ini.

1. Hapus VPC.

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

2. Hapus pangsa RAM kolam IPAM.

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

3. Deprovision pool CIDR dari kolam Regional.

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

4. Deprovision pool CIDR dari kolam tingkat atas.

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

5. Hapus IPAM

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

Tutorial: Lihat riwayat alamat IP menggunakanAWS CLI

Skenario di bagian ini menunjukkan cara untuk melakukannya dengan cara untuk melakukannya dengan menggunakanAWS CLI. Untuk informasi umum tentang penggunaanAWS CLI, lihat MenggunakanAWS CLI di Panduan Pengguna Antarmuka BarisAWS Perintah.

Daftar Isi

- Gambaran Umum
- Skenario

Gambaran Umum

IPAM secara otomatis menyimpan data pemantauan alamat IP Anda hingga tiga tahun. Anda dapat menggunakan data historis untuk menganalisis dan mengaudit keamanan jaringan dan kebijakan perutean Anda. Anda dapat mencari wawasan sejarah untuk jenis sumber berikut:

- VPC
- Subnet VPC
- Alamat IP elastis
- Instans EC2 yang sedang berjalan
- Antarmuka jaringan EC2 yang dilampirkan ke instans

> **Important**
>
> Meskipun IPAM tidak memantau instans Amazon EC2 atau antarmuka jaringan EC2 yang terpasang pada instans, Anda dapat menggunakan fitur Riwayat IP Pencarian untuk mencari data historis pada instans EC2 dan CIDR antarmuka jaringan.

> **Note**
>
> - Perintah dalam tutorial ini harus dijalankan menggunakan akun yang memiliki IPAM danAWS Wilayah yang menjadi tuan rumah IPAM.
> - Catatan perubahan pada CIDR diambil dalam snapshot periodik, yang berarti bahwa perlu beberapa waktu untuk catatan muncul atau diperbarui, dan nilai untukSampledStartTime danSampledEndTime dapat berbeda dari waktu aktual mereka terjadi.

Skenario

Skenario di bagian ini menunjukkan cara untuk melakukannya dengan cara untuk melakukannya dengan menggunakanAWS CLI. Untuk informasi lebih lanjut tentang nilai-nilai yang disebutkan dalam tutorial ini seperti waktu akhir sampel dan waktu mulai, lihatLihat riwayat alamat IP.

Skenario 1: Sumber daya apa yang dikaitkan**`10.2.1.155/32`** antara pukul 01.00 hingga 21.00 pada 27 Desember 2021 (UTC)?

1. Jalankan perintah berikut:

```
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. Lihat hasil analisis. Pada contoh di bawah ini, CIDR dialokasikan ke antarmuka jaringan dan contoh EC2 selama periode waktu. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi lebih lanjut tentang nilai-nilai yang ditunjukkan di output berikut, lihatLihat riwayat alamat 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"
        }
    ]
}
```

Jika ID pemilik instans yang dilampirkan antarmuka jaringan berbeda dari ID pemilik antarmuka jaringan (seperti halnya gateway NAT, antarmuka jaringan Lambda di VPC, danAWS layanan lainnya),`ResourceOwnerId`damazon-aws bukan ID akun pemilik antarmuka jaringan. Contoh berikut menunjukkan catatan untuk CIDR terkait dengan 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"
        }
    ]
}
```

Skenario 2: Sumber daya apa yang dikaitkan dengan**10.2.1.0/24** dari 1 Desember 2021 hingga 27 Desember 2021 (UTC)?

1. Jalankan perintah berikut:

```
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. Lihat hasil analisis. Pada contoh di bawah ini, CIDR dialokasikan ke subnet dan VPC selama periode waktu. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi lebih lanjut tentang nilai-nilai yang ditunjukkan di output berikut, lihatLihat riwayat alamat 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"
```

```
        }
    ]
}
```

Skenario 3: Sumber daya apa yang dikaitkan dengan**2605:9cc0:409::/56** dari 1 Desember 2021 hingga 27 Desember 2021 (UTC)?

1. Jalankan perintah berikut, di mana -region adalah IPAM home Region:

```
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. Lihat hasil analisis. Pada contoh di bawah ini, CIDR dialokasikan untuk dua VPC yang berbeda selama periode waktu di suatu Wilayah di luar Wilayah asal IPAM. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi lebih lanjut tentang nilai-nilai yang ditunjukkan di output berikut, lihatLihat riwayat alamat 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"
        }
    ]
}
```

Skenario 4: Sumber daya apa yang dikaitkan**10.0.0.0/24** dalam 24 jam terakhir (dengan asumsi waktu saat ini adalah tengah malam pada 27 Desember 2021 (UTC))?

1. Jalankan perintah berikut:

```
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. Lihat hasil analisis. Pada contoh di bawah ini, CIDR telah dialokasikan untuk banyak subnet dan VPC selama periode waktu. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi lebih lanjut tentang nilai-nilai yang ditunjukkan di output berikut, lihatLihat riwayat alamat 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"
        }
    ]
}
```


Skenario 5: Sumber daya mana yang saat ini terkait**`10.2.1.155/32`**?

1. Jalankan perintah berikut:

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

2. Lihat hasil analisis. Pada contoh di bawah ini, CIDR dialokasikan ke antarmuka jaringan dan instans EC2 selama periode waktu. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi lebih lanjut tentang nilai-nilai yang ditunjukkan di output berikut, lihatLihat riwayat alamat 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"
        }
    ]
}
```


Skenario 6: Sumber daya mana yang saat ini terkait**`10.2.1.0/24`**?

1. Jalankan perintah berikut:

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

2. Lihat hasil analisis. Pada contoh di bawah ini, CIDR dialokasikan ke VPC dan subnet selama periode waktu. Hanya hasil yang cocok dengan/24 CIDR ini yang dikembalikan, tidak semua/32 dalam/24 CIDR. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi lebih lanjut tentang nilai-nilai yang ditunjukkan di output berikut, lihatLihat riwayat alamat 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"
        }
    ]
}
```

Skenario 7: Sumber daya mana yang saat ini terkait**54.0.0.9/32**?

Dalam contoh ini,54.0.0.9/32 ditugaskan ke alamat IP elastis yang bukan bagian dariAWS Organisasi yang terintegrasi dengan IPAM Anda.

1. Jalankan perintah berikut:

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

2. Karena54.0.0.9/32 ditugaskan ke alamat IP elastis yang bukan bagian dariAWS Organisasi yang terintegrasi dengan IPAM dalam contoh ini, tidak ada catatan yang dikembalikan.

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

Tutorial: Bawa ASN Anda ke IPAM

Jika aplikasi Anda menggunakan alamat IP tepercaya dan Nomor Sistem Otonom (ASN) yang diizinkan oleh mitra atau pelanggan Anda yang terdaftar di jaringan mereka, Anda dapat menjalankan aplikasi ini AWS tanpa mengharuskan mitra atau pelanggan Anda untuk mengubah daftar izin mereka.

Autonomous System Number (ASN) adalah nomor unik global yang memungkinkan sekelompok jaringan diidentifikasi melalui internet dan bertukar data routing dengan jaringan lain secara dinamis menggunakan Border Gateway Protocol. Penyedia layanan Internet (ISP), misalnya, menggunakan ASN untuk mengidentifikasi sumber lalu lintas jaringan. Tidak semua organisasi membeli ASN mereka sendiri, tetapi untuk organisasi yang melakukannya, mereka dapat membawa ASN mereka. AWS

Bawa nomor sistem otonom Anda sendiri (BYOASN) memungkinkan Anda untuk mengiklankan alamat IP yang Anda bawa AWS dengan ASN publik Anda sendiri alih-alih ASN. AWS Saat Anda menggunakan BYOASN, lalu lintas yang berasal dari alamat IP Anda membawa ASN Anda alih-alih AWS ASN, dan beban kerja Anda dapat dijangkau oleh pelanggan atau mitra yang telah mengizinkan lalu lintas terdaftar berdasarkan alamat IP dan ASN Anda.

⚠ Important

- Lengkapi tutorial ini menggunakan akun admin IPAM di Region rumah IPAM Anda.
- Tutorial ini mengasumsikan Anda memiliki ASN publik yang ingin Anda bawa ke IPAM dan bahwa Anda telah membawa BYOIP CIDR dan menyediakannya ke kolam di AWS ruang lingkup publik Anda. Anda dapat membawa ASN ke IPAM kapan saja, tetapi untuk menggunakannya, Anda harus mengaitkan dengan CIDR yang telah Anda bawa ke akun Anda. AWS Tutorial ini mengasumsikan bahwa Anda telah melakukan itu. Untuk informasi selengkapnya, lihat Tutorial: Bawa alamat IP Anda ke IPAM.
- Anda dapat mengubah antara iklan Anda ASN Anda sendiri atau AWS ASN tanpa penundaan, tetapi Anda terbatas untuk mengubah dari ASN ke AWS ASN Anda sendiri sekali per jam.
- Jika BYOIP CIDR Anda saat ini diiklankan, Anda tidak perlu menariknya dari iklan untuk dikaitkan dengan ASN Anda.

Prasyarat orientasi untuk ASN Anda

Anda akan memerlukan yang berikut untuk menyelesaikan tutorial ini:

- ASN 2-byte atau 4-byte publik Anda.
- Jika Anda sudah membawa rentang alamat IP ke AWS withTutorial: Bawa alamat IP Anda ke IPAM, Anda memerlukan rentang CIDR alamat IP. Anda juga memerlukan kunci pribadi. Anda dapat menggunakan kunci pribadi yang Anda buat saat membawa rentang CIDR alamat IP AWS atau Anda dapat membuat kunci pribadi baru seperti yang dijelaskan dalam Buat kunci pribadi dan buat sertifikat X.509 di Panduan Pengguna EC2.
- Saat Anda membawa rentang alamat IP ke AWS withTutorial: Bawa alamat IP Anda ke IPAM, Anda membuat sertifikat X.509 dan mengunggah sertifikat X.509 ke catatan RDAP di RIR Anda. Anda harus mengunggah sertifikat yang sama yang Anda buat ke catatan RDAP di RIR Anda untuk ASN. Pastikan untuk memasukkan string `-----BEGIN CERTIFICATE-----` dan `-----END CERTIFICATE-----` sebelum dan sesudah bagian yang dikodekan. Semua konten ini harus dalam satu baris panjang. Prosedur untuk memperbarui RDAP tergantung pada RIR Anda:
  - Untuk ARIN, gunakan portal Manajer Akun untuk menambahkan sertifikat di bagian “Komentar Publik” untuk objek “Informasi Jaringan” yang mewakili ASN Anda dengan menggunakan opsi “Ubah ASN”. Jangan menambahkannya ke bagian komentar untuk organisasi Anda.
  - Untuk RIPE, tambahkan sertifikat sebagai bidang “descr” baru ke objek “aut-num” yang mewakili ASN Anda. Ini biasanya dapat ditemukan di bagian “Sumber Daya Saya” dari

    Portal Database RIPE. Jangan menambahkannya ke bagian komentar untuk organisasi Anda atau bidang “komentar” dari objek “aut-num”.
  - Untuk APNIC, kirim email sertifikat ke helpdesk@apnic.net untuk menambahkannya secara manual ke bidang “komentar” untuk ASN Anda. Kirim email menggunakan kontak resmi APNIC untuk ASN.

Langkah-langkah tutorial

Selesaikan langkah-langkah di bawah ini menggunakan AWS konsol atau AWS CLI.

AWS Management Console

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi kiri, pilih iPAMS.

3. Pilih IPAM Anda.
4. Pilih tab ByoAsns dan pilih Provision ByoAsns.
5. Masukkan ASN. Akibatnya, bidang Pesan secara otomatis diisi dengan pesan yang Anda perlukan untuk masuk pada langkah berikutnya.

   - Format pesan adalah sebagai berikut, di mana AKUN adalah nomor AWS akun Anda, ASN adalah ASN yang Anda bawa ke IPAM, dan YYYYMMDD adalah tanggal kedaluwarsa pesan (yang default ke hari terakhir bulan berikutnya). Contoh:

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

6. Salin pesan dan ganti tanggal kedaluwarsa dengan nilai Anda sendiri jika Anda mau.
7. Tanda tangani pesan menggunakan kunci pribadi. Contoh:

   ```
   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. Di bawah Tanda Tangan, masukkan tanda tangan.
9. (Opsional) Untuk menyediakan ASN lain, pilih Ketentuan ASN lain. Anda dapat menyediakan hingga 5 ASN. Untuk meningkatkan kuota ini, lihatKuota untuk IPAM Anda.
10. Pilih Ketentuan.
11. Lihat proses penyediaan di tab ByoAsns. Tunggu Negara berubah dari Pending-provisioned menjadi Provisioned. BYOASNS dalam status Failed-provision secara otomatis dihapus setelah 7 hari. Setelah ASN berhasil disediakan, Anda dapat mengaitkannya dengan BYOIP CIDR.
12. Di panel navigasi kiri, pilih Pools.
13. Pilih ruang lingkup publik Anda. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
14. Pilih kolam regional yang memiliki BYOIP CIDR yang disediakan untuknya. Pool harus memiliki Service yang disetel ke EC2 dan harus memiliki lokal yang dipilih.
15. Pilih tab CIDR dan pilih CIDR BYOIP.
16. Pilih Tindakan > Kelola asosiasi BYOASN.
17. Di bawah Associated BYOASNS, pilih ASN yang Anda bawa. AWS Jika Anda memiliki beberapa ASN, Anda dapat mengaitkan beberapa ASN ke BYOIP CIDR. Anda dapat mengaitkan ASN sebanyak yang dapat Anda bawa ke IPAM. Perhatikan bahwa Anda dapat

membawa hingga 5 ASN ke IPAM secara default. Untuk informasi selengkapnya, lihat Kuota untuk IPAM Anda.

18. Pilih Kaitkan.
19. Tunggu asosiasi ASN selesai. Setelah ASN berhasil dikaitkan dengan BYOIP CIDR, Anda dapat mengiklankan BYOIP CIDR lagi.
20. Pilih tab CIDR kolam.
21. Pilih CIDR BYOIP dan pilih Actions > Advertise. Akibatnya, opsi ASN Anda ditampilkan: Amazon ASN dan ASN apa pun yang Anda bawa ke IPAM.
22. Pilih ASN yang Anda bawa ke IPAM dan pilih Iklan CIDR. Akibatnya, CIDR BYOIP diiklankan dan nilai di kolom Iklan berubah dari Ditarik ke Iklan. Kolom Autonomous System Number menampilkan ASN yang terkait dengan CIDR.
23. (opsional) Jika Anda memutuskan ingin mengubah asosiasi ASN kembali ke Amazon ASN, pilih CIDR BYOIP dan pilih Tindakan > Beriklan lagi. Kali ini, pilih Amazon ASN. Anda dapat menukar kembali ke Amazon ASN kapan saja, tetapi Anda hanya dapat mengubah ke ASN khusus setiap jam sekali.

Tutorialnya selesai.

Pembersihan

1. Putuskan ASN dari BYOIP CIDR
   - Untuk menarik BYOIP CIDR dari iklan, di kolam Anda di ruang lingkup publik, pilih CIDR BYOIP dan pilih Tindakan > Penarikan dari iklan.
   - Untuk memisahkan ASN dari CIDR, pilih Tindakan > Kelola asosiasi BYOASN.
2. Penundaan ASN
   - Untuk menghentikan ASN, di tab ByoAsns, pilih ASN dan pilih Deprovision ASN. Akibatnya, ASN dibatalkan. ByoAsns dalam keadaan Deprovisioned secara otomatis dihapus setelah 7 hari.

Pembersihan selesai.

Command line

1. Menyediakan ASN Anda dengan menyertakan ASN dan pesan otorisasi Anda. Tanda tangan adalah pesan yang ditandatangani dengan kunci pribadi Anda.

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

2. Jelaskan ASN Anda untuk melacak proses penyediaan. Jika permintaan berhasil, Anda akan melihat ProvisionStatusset ke provisioned setelah beberapa menit.

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

3. Kaitkan ASN Anda dengan BYOIP CIDR Anda. ASN kustom apa pun yang ingin Anda iklankan harus terlebih dahulu dikaitkan dengan CIDR Anda.

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

4. Jelaskan CIDR Anda untuk melacak proses asosiasi.

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

5. Iklankan CIDR Anda dengan ASN Anda. Jika CIDR sudah diiklankan, ini akan menukar ASN asal dari Amazon ke milik Anda.

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

6. Jelaskan CIDR Anda untuk melihat perubahan status ASN dari terkait ke yang diiklankan.

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

Tutorialnya selesai.

Pembersihan

1. Lakukan salah satu hal berikut ini:

   - Untuk menarik hanya iklan ASN Anda dan kembali menggunakan ASN Amazon sambil tetap mengiklankan CIDR, Anda harus menelepon advertise-byoip-cidr dengan AWS nilai khusus untuk parameter asn. Anda dapat menukar kembali ke Amazon ASN kapan saja, tetapi Anda hanya dapat mengubah ke ASN khusus setiap jam sekali.

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

- Untuk menarik iklan CIDR dan ASN Anda secara bersamaan, Anda dapat menelepon. withdraw-byoip-cidr

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

2. Untuk membersihkan ASN Anda, Anda harus terlebih dahulu memisahkannya dari BYOIP CIDR Anda.

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

3. Setelah ASN Anda dipisahkan dari semua CIDR BYOIP yang Anda kaitkan, Anda dapat membatasinya.

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

4. BYOIP CIDR juga dapat dideprovisioned setelah semua asosiasi ASN dihapus.

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

5. Konfirmasikan deprovisioning.

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

Pembersihan selesai.

Tutorial: Bawa alamat IP Anda ke IPAM

Tutorial di bagian ini memandu Anda melalui proses membawa ruang alamat IP publik ke AWS dan mengelola ruang dengan IPAM.

Mengelola ruang alamat IP publik dengan IPAM memiliki manfaat sebagai berikut:

- Meningkatkan penggunaan alamat IP publik di seluruh organisasi Anda: Anda dapat menggunakan IPAM untuk berbagi ruang alamat IP di seluruh AWS akun. Tanpa menggunakan IPAM, Anda tidak dapat membagikan ruang IP publik Anda di seluruh akun AWS Organizations.
- Menyederhanakan proses membawa ruang IP publik ke AWS: Anda dapat menggunakan IPAM untuk onboard ruang alamat IP publik sekali, dan kemudian menggunakan IPAM untuk

mendistribusikan IP publik Anda di seluruh Wilayah. Tanpa IPAM, Anda harus memasukkan IP publik Anda untuk setiap Wilayah. AWS

Important

- Sebelum Anda memulai tutorial ini, selesaikan langkah-langkah dalam prasyarat Onboarding untuk rentang alamat BYOIP Anda di Panduan Pengguna Amazon EC2.

  Saat Anda membuat ROA, untuk IPv4 CIDR Anda harus mengatur panjang maksimum awalan alamat IP ke. `/24` Untuk IPv6 CIDR, jika Anda menambahkannya ke kolam yang dapat diiklankan, panjang maksimum prefiks alamat IP harus. `/48` Ini memastikan bahwa Anda memiliki fleksibilitas penuh untuk membagi alamat IP publik Anda di seluruh AWS Wilayah. IPAM memberlakukan panjang maksimum yang Anda tetapkan. Panjang maksimum adalah pengumuman panjang awalan terkecil yang akan Anda izinkan untuk rute ini. Misalnya, jika Anda membawa blok `/20` CIDR ke AWS, dengan menyetel panjang maksimum`/24`, Anda dapat membagi blok yang lebih besar dengan cara apa pun yang Anda suka (seperti dengan`/21`,`/22`, atau`/24`) dan mendistribusikan blok CIDR yang lebih kecil itu ke Wilayah mana pun. Jika Anda menetapkan panjang maksimum`/23`, Anda tidak akan dapat membagi dan mengiklankan a `/24` dari blok yang lebih besar. Juga, perhatikan bahwa itu `/24` adalah blok IPv4 terkecil dan `/48` merupakan blok IPv6 terkecil yang dapat Anda iklankan dari Wilayah ke internet.
- Setelah Anda membawa rentang alamat IPv4 AWS, Anda dapat menggunakan semua alamat IP dalam rentang tersebut, termasuk alamat pertama (alamat jaringan) dan alamat terakhir (alamat siaran).

Konten

- Bawa IPv4 CIDR publik Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS
- Bawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS

Bawa IPv4 CIDR publik Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS

Ikuti langkah-langkah ini untuk membawa IPv4 atau IPv6 CIDR ke IPAM menggunakan Management AWS Console dan CLI. AWS

Important

- Sebelum Anda memulai tutorial ini, selesaikan langkah-langkah dalam prasyarat Onboarding untuk rentang alamat BYOIP Anda di Panduan Pengguna Amazon EC2.

  Saat Anda membuat ROA, untuk IPv4 CIDR Anda harus mengatur panjang maksimum awalan alamat IP. `/24` Untuk IPv6 CIDR, jika Anda menambahkannya ke kolam yang dapat diiklankan, panjang maksimum prefiks alamat IP harus. `/48` Ini memastikan bahwa Anda memiliki fleksibilitas penuh untuk membagi alamat IP publik Anda di seluruh AWS Wilayah. IPAM memberlakukan panjang maksimum yang Anda tetapkan. Panjang maksimum adalah pengumuman panjang awalan terkecil yang akan Anda izinkan untuk rute ini. Misalnya, jika Anda membawa blok `/20` CIDR ke AWS, dengan menyetel panjang maksimum`/24`, Anda dapat membagi blok yang lebih besar dengan cara apa pun yang Anda suka (seperti dengan`/21`,`/22`, atau`/24`) dan mendistribusikan blok CIDR yang lebih kecil itu ke Wilayah mana pun. Jika Anda menetapkan panjang maksimum`/23`, Anda tidak akan dapat membagi dan mengiklankan a `/24` dari blok yang lebih besar. Juga, perhatikan bahwa itu `/24` adalah blok IPv4 terkecil dan `/48` merupakan blok IPv6 terkecil yang dapat Anda iklankan dari Wilayah ke internet.
- Setelah Anda membawa rentang alamat IPv4 AWS, Anda dapat menggunakan semua alamat IP dalam rentang tersebut, termasuk alamat pertama (alamat jaringan) dan alamat terakhir (alamat siaran).

Konten

- Bawa IPv4 CIDR Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS
- Bawa IPv6 CIDR Anda sendiri ke IPAM menggunakan Management Console AWS

Bawa IPv4 CIDR Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS

Ikuti langkah-langkah ini untuk membawa IPv4 CIDR ke IPAM dan mengalokasikan alamat IP Elastis (EIP) menggunakan Management AWS Console dan CLI. AWS

Important

- Anda tidak dapat menyediakan atau mengiklankan rentang alamat BYOIP di Local Zones saat ini.
- Tutorial ini mengasumsikan Anda telah menyelesaikan langkah-langkah di bagian berikut:
  - Integrasikan IPAM dengan akun di Organisasi AWS.
  - Buat IPAM.
- Setiap langkah tutorial ini harus dilakukan oleh salah satu dari tiga akun AWS Organizations:
  - Akun manajemen.
  - Akun anggota dikonfigurasi untuk menjadi administrator IPAM Anda diIntegrasikan IPAM dengan akun di Organisasi AWS. Dalam tutorial ini, akun ini akan disebut akun IPAM.
  - Akun anggota di organisasi Anda yang akan mengalokasikan CIDR dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

- Langkah 1: Buat profil AWS CLI bernama dan peran IAM
- Langkah 2: Buat kolam IPAM tingkat atas
- Langkah 3. Buat kolam Regional di dalam kolam tingkat atas
- Langkah 4. Bagikan kolam Regional
- Langkah 5: Buat kolam IPv4 publik
- Langkah 6: Menyediakan IPv4 CIDR publik ke kolam IPv4 publik Anda
- Langkah 7: Buat alamat IP Elastis dari kolam IPv4 publik
- Langkah 8: Kaitkan alamat IP Elastis dengan instans EC2
- Langkah 9: Iklankan CIDR
- Langkah 10: Pembersihan

Langkah 1: Buat profil AWS CLI bernama dan peran IAM

Untuk menyelesaikan tutorial ini sebagai AWS pengguna tunggal, Anda dapat menggunakan profil AWS CLI bernama untuk beralih dari satu peran IAM ke peran lainnya. Profil bernama adalah kumpulan pengaturan dan kredensional yang Anda rujuk saat menggunakan `--profile` opsi dengan. AWS CLI Untuk informasi selengkapnya tentang cara membuat peran IAM dan profil bernama untuk AWS akun, lihat Menggunakan peran IAM di AWS CLI di Panduan Pengguna AWS Identity and Access Management.

Buat satu peran dan satu profil bernama untuk masing-masing dari tiga AWS akun yang akan Anda gunakan dalam tutorial ini:

- Sebuah profil yang disebut `management-account` untuk akun manajemen AWS Organizations.
- Profil yang dipanggil `ipam-account` untuk akun anggota AWS Organizations yang dikonfigurasi untuk menjadi administrator IPAM Anda.
- Profil yang dipanggil `member-account` untuk akun anggota AWS Organizations di organisasi Anda yang akan mengalokasikan CIDR dari kolam IPAM.

Setelah Anda membuat peran IAM dan profil bernama, kembali ke halaman ini dan lanjutkan ke langkah berikutnya. Anda akan melihat sepanjang sisa tutorial ini bahwa AWS CLI perintah sampel menggunakan `--profile` opsi dengan salah satu profil bernama untuk menunjukkan akun mana yang harus menjalankan perintah.

Langkah 2: Buat kolam IPAM tingkat atas

Selesaikan langkah-langkah di bagian ini untuk membuat kolam IPAM tingkat atas.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk membuat kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Pilih ruang lingkup publik. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Pilih Buat kolam.
5. (Opsional) Tambahkan tag Nama untuk kolam dan Deskripsi untuk kolam.

6. Di bawah Sumber, pilih cakupan IPAM.
7. Di bawah Keluarga alamat, pilih IPv4.
8. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
9. Di bawah Lokal, pilih Tidak Ada.

   Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP.

   Integrasi IPAM dengan BYOIP mengharuskan lokal diatur pada kumpulan mana pun yang akan digunakan untuk BYOIP CIDR. Karena kita akan membuat kolam IPAM tingkat atas dengan kolam Regional di dalamnya, dan kita akan mengalokasikan ruang ke alamat IP Elastis dari kolam Regional, Anda akan mengatur lokal di kolam Regional dan bukan kolam tingkat atas. Anda akan menambahkan lokal ke kolam Regional saat membuat kumpulan Regional di langkah selanjutnya.

   > **Note**
   >
   > Jika Anda membuat kolam tunggal saja dan bukan kolam tingkat atas dengan kolam Regional di dalamnya, Anda ingin memilih Lokal untuk kolam ini sehingga kolam tersedia untuk alokasi.

10. Di bawah Sumber IP Publik, pilih salah satu opsi berikut:

    - BYOIP: Anda membawa rentang alamat IPv4 atau IPv6 (BYOIP) Anda sendiri ke kolam ini.
    - Milik Amazon: Anda ingin Amazon menyediakan rentang alamat IPv6 ke kumpulan ini.

11. Lakukan salah satu hal berikut ini:

    - Jika Anda memilih BYOIP pada langkah sebelumnya, di bawah CIDR untuk menyediakan, pilih CIDR untuk disediakan untuk kumpulan. Perhatikan bahwa saat menyediakan IPv4 CIDR ke kolam dalam kumpulan tingkat atas, IPv4 CIDR minimum yang dapat Anda berikan adalah`/24`; CIDR yang lebih spesifik (seperti) tidak diizinkan. `/25` Anda harus menyertakan

CIDR dan pesan BYOIP dan tanda tangan sertifikat dalam permintaan sehingga kami dapat memverifikasi bahwa Anda memiliki ruang publik. Untuk daftar prasyarat BYOIP termasuk cara mendapatkan pesan BYOIP ini dan tanda tangan sertifikat, lihat. Bawa IPv4 CIDR publik Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS

> **Important**
>
> Meskipun sebagian besar penyediaan akan selesai dalam waktu dua jam, mungkin diperlukan waktu hingga satu minggu untuk menyelesaikan proses penyediaan untuk rentang yang dapat diiklankan secara publik.

- Jika Anda memilih milik Amazon, di bawah panjang Netmask pilih panjang netmask dari ke`/40`. `/52` Default-nya adalah `/52`.

12. Biarkan Konfigurasi pengaturan aturan alokasi kumpulan ini tidak dipilih.
13. (Opsional) Pilih Tag untuk kolam.
14. Pilih Buat kolam.

Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan di tab CIDR di halaman detail kumpulan.

Langkah 3. Buat kolam Regional di dalam kolam tingkat atas

Buat kolam Regional di dalam kolam tingkat atas. Integrasi IPAM dengan BYOIP mengharuskan lokal diatur pada kumpulan mana pun yang akan digunakan untuk BYOIP CIDR. Anda akan menambahkan lokal ke kolam Regional saat membuat kumpulan Regional di bagian ini. `Locale`Harus menjadi salah satu Wilayah operasi yang Anda konfigurasikan saat Anda membuat IPAM.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk membuat kolam Regional dalam kolam tingkat atas

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Jika Anda tidak ingin menggunakan cakupan pribadi default, dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.

4. Pilih Buat kolam.
5. (Opsional) Tambahkan tag Nama untuk kolam dan Deskripsi untuk kolam.
6. Di bawah Sumber, pilih kumpulan tingkat atas yang Anda buat di bagian sebelumnya.
7. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
8. Di bawah Locale, pilih lokasi untuk kolam renang. Dalam tutorial ini, kita akan menggunakan `us-east-2` sebagai lokal untuk kolam Regional. Opsi yang tersedia berasal dari Wilayah operasi yang Anda pilih saat Anda membuat IPAM Anda.

   Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP. Memilih lokal memastikan tidak ada dependensi lintas wilayah antara kumpulan Anda dan sumber daya yang dialokasikan darinya.
9. Di bawah Layanan, pilih EC2 (EIP/VPC). Layanan yang Anda pilih menentukan AWS layanan di mana CIDR akan dapat diiklankan. Saat ini, satu-satunya pilihan adalah EC2 (EIP/VPC), yang berarti bahwa CIDR yang dialokasikan dari kumpulan ini akan dapat diiklankan untuk layanan Amazon EC2 (untuk alamat IP Elastis) dan layanan VPC Amazon (untuk CIDR yang terkait dengan VPC).
10. Di bawah CIDR untuk penyediaan, pilih CIDR untuk disediakan untuk kolam. Perhatikan bahwa saat menyediakan CIDR ke kolam dalam kumpulan tingkat atas, IPv4 CIDR minimum yang dapat Anda berikan adalah`/24`; CIDR yang lebih spesifik (seperti) tidak diizinkan. `/25` Setelah Anda membuat kolam regional pertama, Anda dapat membuat kolam yang lebih kecil (seperti`/25`) di dalam kolam regional.
11. Aktifkan Konfigurasi pengaturan aturan alokasi kumpulan ini. Anda memiliki opsi aturan alokasi yang sama di sini seperti yang Anda lakukan saat membuat kumpulan tingkat atas. Lihat Buat kolam IPv4 tingkat atas penjelasan tentang opsi yang tersedia saat Anda membuat kumpulan. Aturan alokasi untuk kolam Regional tidak diwarisi dari kolam tingkat atas. Jika Anda tidak menerapkan aturan apa pun di sini, tidak akan ada aturan alokasi yang ditetapkan untuk kumpulan.
12. (Opsional) Pilih Tag untuk kolam.
13. Setelah selesai mengonfigurasi pool, pilih Create pool.

Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan di tab CIDR di halaman detail kumpulan.

Langkah 4. Bagikan kolam Regional

Ikuti langkah-langkah di bagian ini untuk berbagi kolam IPAM menggunakan AWS Resource Access Manager (RAM).

Aktifkan berbagi sumber daya di AWS RAM

Setelah membuat IPAM, Anda akan ingin berbagi kumpulan regional dengan akun lain di organisasi Anda. Sebelum Anda berbagi kolam IPAM, selesaikan langkah-langkah di bagian ini untuk mengaktifkan berbagi AWS RAM sumber daya. Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`management-account`** opsi.

Untuk mengaktifkan berbagi sumber daya

1. Menggunakan akun AWS Organizations manajemen, buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Di panel navigasi kiri, pilih Pengaturan, pilih Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

Anda sekarang dapat berbagi kolam IPAM dengan anggota organisasi lainnya.

Bagikan kolam IPAM menggunakan AWS RAM

Di bagian ini Anda akan membagikan kumpulan regional dengan akun AWS Organizations anggota lain. Untuk petunjuk lengkap tentang berbagi kumpulan IPAM, termasuk informasi tentang izin IAM yang diperlukan, lihat. Membagikan kumpulan IPAM menggunakanAWS RAM Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`ipam-account`** opsi.

Untuk berbagi kolam IPAM menggunakan AWS RAM

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi, pilih kolam IPAM, dan pilih Tindakan > Lihat detail.
4. Di bawah Berbagi sumber daya, pilih Buat berbagi sumber daya. AWS RAM Konsol terbuka. Anda berbagi kolam menggunakan AWS RAM.

5. Pilih Buat berbagi sumber daya.
6. Di AWS RAM konsol, pilih Buat berbagi sumber daya lagi.
7. Tambahkan Nama untuk kolam bersama.
8. Di bawah Pilih jenis sumber daya, pilih kolam IPAM, lalu pilih ARN dari kumpulan yang ingin Anda bagikan.
9. Pilih Selanjutnya.
10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diMembagikan kumpulan IPAM menggunakanAWS RAM.
11. Pilih Selanjutnya.
12. Di bawah Prinsipal > Pilih tipe utama, pilih AWS akun dan masukkan ID akun akun yang akan membawa rentang alamat IP ke IPAM dan pilih Tambah.
13. Pilih Selanjutnya.
14. Tinjau opsi berbagi sumber daya dan prinsipal yang akan Anda bagikan, lalu pilih Buat.
15. Untuk memungkinkan **`member-account`** akun mengalokasikan CIDRS alamat IP dari kolam IPAM, buat berbagi sumber daya kedua dengan `AWSRAMDefaultPermissionsIpamPool` dan buat berbagi sumber daya kedua. Nilai untuk `--resource-arns` adalah ARN dari kolam IPAM yang Anda buat di bagian sebelumnya. Nilai untuk `--principals` adalah ID akun dari**`member-account`**. Nilai untuk `--permission-arns` adalah ARN izin. `AWSRAMDefaultPermissionsIpamPool`

Langkah 5: Buat kolam IPv4 publik

Membuat kolam IPv4 publik adalah langkah yang diperlukan untuk membawa alamat IPv4 publik AWS untuk dikelola dengan IPAM. Langkah ini harus dilakukan oleh akun anggota yang akan memberikan alamat IP Elastis.

⚠ Important

- Langkah ini harus dilakukan oleh akun anggota menggunakan AWS CLI.
- Kolam IPv4 publik dan kolam IPAM dikelola oleh sumber daya yang berbeda di. AWS Pool IPv4 publik adalah sumber daya akun tunggal yang memungkinkan Anda mengonversi CIDR milik publik ke alamat IP Elastis. Kolam IPAM dapat digunakan untuk mengalokasikan ruang publik Anda ke kolam IPv4 publik.

Untuk membuat kolam IPv4 publik menggunakan AWS CLI

- Jalankan perintah berikut untuk menyediakan CIDR. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `Locale` opsi yang Anda pilih saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

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

  Dalam output, Anda akan melihat ID kolam IPv4 publik. Anda akan membutuhkan ID ini di langkah berikutnya.

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

Langkah 6: Menyediakan IPv4 CIDR publik ke kolam IPv4 publik Anda

Menyediakan IPv4 CIDR publik ke kolam IPv4 publik Anda. Nilai untuk `--region` harus sesuai dengan `Locale` nilai yang Anda pilih ketika Anda membuat pool yang akan digunakan untuk BYOIP CIDR. `--netmask-length`Ini adalah jumlah ruang dari kolam IPAM yang ingin Anda bawa ke kolam renang umum Anda. Nilai tidak boleh lebih besar dari panjang netmask dari kolam IPAM. Prefiks IPv4 paling tidak spesifik yang dapat Anda bawa adalah. `/24`

> **Note**
>
> Jika Anda membawa rentang `/24` CIDR ke IPAM untuk dibagikan di seluruh AWS Organisasi, Anda dapat memberikan awalan yang lebih kecil ke beberapa kumpulan IPAM, katakanlah `/27` (menggunakan`-- netmask-length 27`), daripada menyediakan seluruh `/24` CIDR (menggunakan`-- netmask-length 24`) seperti yang ditunjukkan dalam tutorial ini.

> **Important**
>
> Langkah ini harus dilakukan oleh akun anggota menggunakan AWS CLI.

Untuk membuat kolam IPv4 publik menggunakan AWS CLI

1. Jalankan perintah berikut untuk menyediakan 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
```

   Dalam output, Anda akan melihat CIDR yang disediakan.

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

2. Jalankan perintah berikut untuk melihat CIDR yang disediakan di kolam IPv4 publik.

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

   Dalam output, Anda akan melihat CIDR yang disediakan. Secara default CIDR tidak diiklankan, yang berarti tidak dapat diakses publik melalui internet. Anda akan memiliki kesempatan untuk mengatur CIDR ini untuk diiklankan di langkah terakhir tutorial ini.

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

Setelah Anda membuat kolam IPv4 publik, untuk melihat kolam IPv4 publik yang dialokasikan di kolam Regional IPAM, buka konsol IPAM dan lihat alokasi di kolam Regional di bawah Alokasi atau Sumber Daya.

Langkah 7: Buat alamat IP Elastis dari kolam IPv4 publik

Selesaikan langkah-langkah di Alokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk membuat alamat IP Elastis (EIP) dari kolam IPv4 publik. Saat Anda membuka EC2 di konsol AWS Manajemen, AWS Wilayah tempat Anda mengalokasikan EIP harus sesuai dengan `Locale` opsi yang Anda pilih saat membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

Langkah ini harus dilakukan oleh akun anggota. Jika Anda menggunakan AWS CLI, gunakan `--profile` **`member-account`** opsi.

Langkah 8: Kaitkan alamat IP Elastis dengan instans EC2

Selesaikan langkah-langkah di Kaitkan alamat IP Elastis dengan instans atau antarmuka jaringan di Panduan Pengguna Amazon EC2 untuk mengaitkan EIP dengan instans EC2. Saat Anda membuka EC2 di konsol AWS Manajemen, AWS Wilayah tempat Anda mengaitkan EIP harus sesuai dengan `Locale` opsi yang Anda pilih saat membuat kumpulan yang akan digunakan untuk CIDR BYOIP. Dalam tutorial ini, kolam itu adalah kolam Regional.

Langkah ini harus dilakukan oleh akun anggota. Jika Anda menggunakan AWS CLI, gunakan `--profile` **`member-account`** opsi.

Langkah 9: Iklankan CIDR

Langkah-langkah di bagian ini harus dilakukan oleh akun IPAM. Setelah Anda mengaitkan alamat IP Elastis (EIP) dengan instance atau Elastic Load Balancer, Anda kemudian dapat mulai mengiklankan CIDR yang Anda bawa AWS ke kolam yang memiliki Service EC2 (EIP/VPC) yang dikonfigurasi. Dalam tutorial ini, itu adalah kumpulan Regional Anda. Secara default CIDR tidak diiklankan, yang berarti tidak dapat diakses publik melalui internet.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk mengiklankan CIDR

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Pilih ruang lingkup publik. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Pilih kolam Regional yang Anda buat dalam tutorial ini.
5. Pilih tab CIDR.
6. Pilih CIDR BYOIP dan pilih Actions > Advertise.
7. Pilih Iklan CIDR.

Akibatnya, CIDR BYOIP diiklankan dan nilai di kolom Iklan berubah dari Ditarik ke Iklan.

Langkah 10: Pembersihan

Ikuti langkah-langkah di bagian ini untuk membersihkan sumber daya yang telah Anda sediakan dan buat dalam tutorial ini.

Langkah 1: Tarik CIDR dari iklan

Langkah ini harus dilakukan oleh akun IPAM.

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Pilih ruang lingkup publik.
4. Pilih kolam Regional yang Anda buat dalam tutorial ini.
5. Pilih tab CIDR.
6. Pilih CIDR BYOIP dan pilih Actions > Withdraw from advertising.
7. Pilih Tarik CIDR.

Akibatnya, CIDR BYOIP tidak lagi diiklankan dan nilai di kolom Iklan berubah dari Diiklankan menjadi Ditarik.

Langkah 2: Putuskan alamat IP Elastis

Langkah ini harus dilakukan oleh akun anggota. Jika Anda menggunakan AWS CLI, gunakan `--profile` **`member-account`** opsi.

- Selesaikan langkah-langkah dalam Memutuskan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk memisahkan EIP. Saat Anda membuka EC2 di konsol AWS Manajemen, AWS Wilayah tempat Anda memisahkan EIP harus sesuai dengan `Locale` opsi yang Anda pilih saat membuat kumpulan yang akan digunakan untuk CIDR BYOIP. Dalam tutorial ini, kolam itu adalah kolam Regional.

Langkah 3: Lepaskan alamat IP Elastis

Langkah ini harus dilakukan oleh akun anggota. Jika Anda menggunakan AWS CLI, gunakan `--profile` **`member-account`** opsi.

- Selesaikan langkah-langkah dalam Rilis alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk merilis alamat IP Elastis (EIP) dari kolam IPv4 publik. Saat Anda membuka EC2 di konsol AWS Manajemen, AWS Wilayah tempat Anda mengalokasikan EIP harus sesuai dengan `Locale` opsi yang Anda pilih saat membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

Langkah 4: Membatalkan IPv4 CIDR publik dari kolam IPv4 publik Anda

> **Important**
>
> Langkah ini harus dilakukan oleh akun anggota menggunakan AWS CLI.

1. Lihat CIDR BYOIP Anda.

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

Dalam output, Anda akan melihat alamat IP di BYOIP CIDR Anda.

```
{
    "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. Jalankan perintah berikut untuk melepaskan alamat IP terakhir di CIDR dari kolam IPv4 publik. Masukkan alamat IP dengan netmask dari. `/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
```

Dalam output, Anda akan melihat CIDR yang telah di-deprovisioned.

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

> **Important**
>
> Anda harus menjalankan kembali perintah ini untuk setiap alamat IP dalam rentang CIDR. Jika CIDR Anda adalah a`/24`, Anda harus menjalankan perintah ini untuk menghentikan penyediaan masing-masing 256 alamat IP di CIDR. `/24`

3. Lihat CIDR BYOIP Anda lagi dan pastikan tidak ada lagi alamat yang disediakan. Ketika Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus cocok dengan Wilayah IPAM Anda.

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

Dalam output, Anda akan melihat jumlah alamat IP di kolam IPv4 publik Anda.

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

> **Note**
>
> Perlu beberapa waktu bagi IPAM untuk menemukan bahwa alokasi kolam IPv4 publik telah dihapus. Anda tidak dapat terus membersihkan dan menghentikan penyediaan CIDR kolam IPAM sampai Anda melihat bahwa alokasi telah dihapus dari IPAM.

Langkah 5: Hapus kolam IPv4 publik

Langkah ini harus dilakukan oleh akun anggota.

- Jalankan perintah berikut untuk menghapus kolam IPv4 publik CIDR. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `Locale` opsi yang Anda pilih saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP. Dalam tutorial ini, kolam itu adalah kolam Regional. Langkah ini harus dilakukan dengan menggunakan AWS CLI.

```
aws ec2 delete-public-ipv4-pool --region us-east-2 --pool-id ipv4pool-
ec2-09037ce61cf068f9a --profile member-account
```

Dalam output, Anda akan melihat nilai kembali benar.

```
{
"ReturnValue": true
}
```

Setelah Anda menghapus kumpulan, untuk melihat alokasi yang tidak dikelola oleh IPAM, buka konsol IPAM dan lihat detail kumpulan Regional di bawah Alokasi.

Langkah 6: Hapus semua pembagian RAM dan nonaktifkan integrasi RAM dengan AWS Organizations

Langkah ini harus dilakukan oleh akun IPAM dan akun manajemen masing-masing. Jika Anda menggunakan AWS CLI untuk menghapus berbagi RAM dan menonaktifkan integrasi RAM, gunakan `--profile management-account` opsi `--profile ipam-account` dan.

- Selesaikan langkah-langkah dalam Menghapus berbagi sumber daya di AWS RAM dan Menonaktifkan berbagi sumber daya dengan AWS Organizations dalam Panduan Pengguna AWS RAM, dalam urutan itu, untuk menghapus berbagi RAM dan menonaktifkan integrasi RAM dengan Organizations. AWS

Langkah 7: Membatalkan CIDR dari kolam Regional dan kolam tingkat atas

Langkah ini harus dilakukan oleh akun IPAM. Jika Anda menggunakan AWS CLI untuk berbagi kolam, gunakan `--profile ipam-account` opsi.

- Selesaikan langkah-langkah Deprovision CIDR dari kolam untuk menghentikan penyediaan CIDR dari kolam Regional dan kemudian kolam tingkat atas, dalam urutan itu.

Langkah 8: Hapus kolam Regional dan kolam tingkat atas

Langkah ini harus dilakukan oleh akun IPAM. Jika Anda menggunakan AWS CLI untuk berbagi kolam, gunakan `--profile ipam-account` opsi.

- Selesaikan langkah-langkah Menghapus kolam kolam kolam kolam kolam kolam renang untuk menghapus kolam Regional dan kemudian kolam tingkat atas, dalam urutan itu.

Bawa IPv6 CIDR Anda sendiri ke IPAM menggunakan Management Console AWS

Ikuti langkah-langkah dalam tutorial ini untuk membawa IPv6 CIDR ke IPAM dan mengalokasikan VPC dengan CIDR menggunakan Management Console dan. AWS AWS CLI

Important

- Anda tidak dapat menyediakan atau mengiklankan rentang alamat BYOIP di Local Zones saat ini.
- Tutorial ini mengasumsikan Anda telah menyelesaikan langkah-langkah di bagian berikut:
  - Integrasikan IPAM dengan akun di Organisasi AWS.
  - Buat IPAM.
- Setiap langkah tutorial ini harus dilakukan oleh salah satu dari tiga akun AWS Organizations:
  - Akun manajemen.
  - Akun anggota dikonfigurasi untuk menjadi administrator IPAM Anda diIntegrasikan IPAM dengan akun di Organisasi AWS. Dalam tutorial ini, akun ini akan disebut akun IPAM.
  - Akun anggota di organisasi Anda yang akan mengalokasikan CIDR dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

- Langkah 1: Buat kolam IPAM tingkat atas
- Langkah 2. Buat kolam Regional di dalam kolam tingkat atas
- Langkah 3. Bagikan kolam Regional
- Langkah 4: Buat VPC
- Langkah 5: Iklankan CIDR
- Langkah 6: Pembersihan

Langkah 1: Buat kolam IPAM tingkat atas

Karena Anda akan membuat kolam IPAM tingkat atas dengan kolam Regional di dalamnya, dan kami akan mengalokasikan ruang untuk sumber daya dari kolam Regional, Anda akan mengatur lokal di kolam Regional dan bukan kolam tingkat atas. Anda akan menambahkan lokal ke kolam Regional saat membuat kumpulan Regional di langkah selanjutnya. Integrasi IPAM dengan BYOIP mengharuskan lokal diatur pada kumpulan mana pun yang akan digunakan untuk BYOIP CIDR.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk membuat kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Pilih ruang lingkup publik. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Pilih Buat kolam.
5. (Opsional) Tambahkan tag Nama untuk kolam dan Deskripsi untuk kolam.
6. Di bawah Sumber, pilih cakupan IPAM.
7. Di bawah Keluarga alamat, pilih IPv6.

   Saat Anda memilih IPv6, opsi sakelar muncul yang memungkinkan Anda mengontrol jika AWS bisa untuk mengiklankan CIDR secara publik di kumpulan ini. Biarkan opsi ini diaktifkan.
8. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
9. Pastikan Izinkan CIDR di kolam ini agar dapat diiklankan secara publik dipilih.
10. Di bawah Lokal, pilih Tidak Ada. Anda akan mengatur lokal di kolam Regional.

    Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP.

> **Note**
>
> Jika Anda membuat kolam tunggal saja dan bukan kolam tingkat atas dengan kolam Regional di dalamnya, Anda ingin memilih Lokal untuk kolam ini sehingga kolam tersedia untuk alokasi.

11. Di bawah sumber IP Publik, BYOIP dipilih secara default.
12. Di bawah CIDR untuk penyediaan, pilih CIDR untuk disediakan untuk kolam. Perhatikan bahwa saat menyediakan IPv6 CIDR ke kolam dalam kumpulan tingkat atas, rentang alamat IPv6 paling spesifik yang dapat Anda bawa adalah/48 untuk CIDR yang dapat diiklankan secara publik dan /60 untuk CIDR yang tidak dapat diiklankan secara publik. Anda harus menyertakan CIDR dan pesan BYOIP dan tanda tangan sertifikat dalam permintaan sehingga kami dapat memverifikasi bahwa Anda memiliki ruang publik. Untuk daftar prasyarat BYOIP termasuk cara mendapatkan pesan BYOIP ini dan tanda tangan sertifikat, lihat. Bawa IPv4 CIDR publik Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS

> **Important**
>
> Meskipun sebagian besar penyediaan akan selesai dalam waktu dua jam, mungkin diperlukan waktu hingga satu minggu untuk menyelesaikan proses penyediaan untuk rentang yang dapat diiklankan secara publik.

13. Biarkan Konfigurasi pengaturan aturan alokasi kumpulan ini tidak dipilih.
14. (Opsional) Pilih Tag untuk kolam renang.
15. Pilih Buat kolam.

Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan di tab CIDR di halaman detail kumpulan.

Langkah 2. Buat kolam Regional di dalam kolam tingkat atas

Buat kolam Regional di dalam kolam tingkat atas. Lokal diperlukan di kolam dan itu harus menjadi salah satu Wilayah operasi yang Anda konfigurasikan saat Anda membuat IPAM.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk membuat kolam Regional dalam kolam tingkat atas

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Jika Anda tidak ingin menggunakan cakupan pribadi default, dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Pilih Buat kolam.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.
6. Di bawah Sumber, pilih kumpulan tingkat atas yang Anda buat di bagian sebelumnya.
7. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
8. Pilih lokasi untuk kolam renang. Memilih lokal memastikan tidak ada dependensi lintas wilayah antara kumpulan Anda dan sumber daya yang dialokasikan darinya. Opsi yang tersedia berasal dari Wilayah operasi yang Anda pilih saat Anda membuat IPAM Anda. Dalam tutorial ini, kita akan menggunakan `us-east-2` sebagai lokal untuk kolam Regional.

   Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP.
9. Di bawah Layanan, pilih EC2 (EIP/VPC). Layanan yang Anda pilih menentukan AWS layanan di mana CIDR akan dapat diiklankan. Saat ini, satu-satunya pilihan adalah EC2 (EIP/VPC), yang berarti bahwa CIDR yang dialokasikan dari kumpulan ini akan dapat diiklankan untuk layanan Amazon EC2 dan layanan Amazon VPC (untuk CIDR yang terkait dengan VPC).
10. Di bawah CIDR untuk penyediaan, pilih CIDR untuk disediakan untuk kolam. Perhatikan bahwa saat menyediakan IPv6 CIDR ke kolam dalam kumpulan tingkat atas, rentang alamat IPv6 paling spesifik yang dapat Anda bawa adalah/48 untuk CIDR yang dapat diiklankan secara publik dan /60 untuk CIDR yang tidak dapat diiklankan secara publik.
11. Aktifkan Konfigurasi pengaturan aturan alokasi kumpulan ini dan pilih aturan alokasi opsional untuk kumpulan ini:

- Impor sumber daya yang ditemukan secara otomatis: Opsi ini tidak tersedia jika Lokal disetel ke Tidak Ada. Jika dipilih, IPAM akan terus mencari sumber daya dalam rentang CIDR kumpulan ini dan secara otomatis mengimpornya sebagai alokasi ke IPAM Anda. Perhatikan hal berikut:
  - CIDR yang akan dialokasikan untuk sumber daya ini tidak boleh dialokasikan ke sumber daya lain agar impor berhasil.
  - IPAM akan mengimpor CIDR terlepas dari kepatuhannya dengan aturan alokasi kumpulan, sehingga sumber daya dapat diimpor dan kemudian ditandai sebagai tidak patuh.
  - Jika IPAM menemukan beberapa CIDR yang tumpang tindih, IPAM akan mengimpor CIDR terbesar saja.
  - Jika IPAM menemukan beberapa CIDR dengan CIDR yang cocok, IPAM akan mengimpor salah satunya secara acak saja.
- Panjang netmask minimum: Panjang netmask minimum yang diperlukan untuk alokasi CIDR di kolam IPAM ini agar sesuai dan blok CIDR ukuran terbesar yang dapat dialokasikan dari kolam. Panjang netmask minimum harus kurang dari panjang netmask maksimum. Kemungkinan panjang netmask untuk alamat IPv4 adalah -. `0` `32` Kemungkinan panjang netmask untuk alamat IPv6 adalah -. `0` `128`
- Panjang netmask default: Panjang netmask default untuk alokasi ditambahkan ke pool ini.
- Panjang netmask maksimum: Panjang netmask maksimum yang akan diperlukan untuk alokasi CIDR di kolam ini. Nilai ini menentukan blok CIDR ukuran terkecil yang dapat dialokasikan dari kolam. Pastikan nilai ini minimum**`/48`**.
- Persyaratan penandaan: Tag yang diperlukan untuk sumber daya untuk mengalokasikan ruang dari kolam. Jika tag sumber daya diubah setelah mereka mengalokasikan ruang atau jika aturan penandaan alokasi diubah pada kumpulan, sumber daya dapat ditandai sebagai tidak sesuai.
- Lokal: Lokal yang akan dibutuhkan untuk sumber daya yang menggunakan CIDR dari kumpulan ini. Sumber daya yang diimpor secara otomatis yang tidak memiliki lokal ini akan ditandai tidak sesuai. Sumber daya yang tidak secara otomatis diimpor ke kolam tidak akan diizinkan mengalokasikan ruang dari kolam kecuali mereka berada di lokal ini.

12. (Opsional) Pilih Tag untuk kolam renang.
13. Setelah selesai mengonfigurasi pool, pilih Create pool.

Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan di tab CIDR di halaman detail kumpulan.

Langkah 3. Bagikan kolam Regional

Ikuti langkah-langkah di bagian ini untuk berbagi kolam IPAM menggunakan AWS Resource Access Manager (RAM).

Aktifkan berbagi sumber daya di AWS RAM

Setelah membuat IPAM, Anda akan ingin berbagi kumpulan regional dengan akun lain di organisasi Anda. Sebelum Anda berbagi kolam IPAM, selesaikan langkah-langkah di bagian ini untuk mengaktifkan berbagi AWS RAM sumber daya. Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`management-account`** opsi.

Untuk mengaktifkan berbagi sumber daya

1. Menggunakan akun AWS Organizations manajemen, buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Di panel navigasi kiri, pilih Pengaturan, pilih Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

Anda sekarang dapat berbagi kolam IPAM dengan anggota organisasi lainnya.

Bagikan kolam IPAM menggunakan AWS RAM

Di bagian ini Anda akan membagikan kumpulan regional dengan akun AWS Organizations anggota lain. Untuk petunjuk lengkap tentang berbagi kumpulan IPAM, termasuk informasi tentang izin IAM yang diperlukan, lihat. Membagikan kumpulan IPAM menggunakanAWS RAM Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`ipam-account`** opsi.

Untuk berbagi kolam IPAM menggunakan AWS RAM

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi, pilih kolam IPAM, dan pilih Tindakan > Lihat detail.
4. Di bawah Berbagi sumber daya, pilih Buat berbagi sumber daya. AWS RAM Konsol terbuka. Anda berbagi kolam menggunakan AWS RAM.

5. Pilih Buat berbagi sumber daya.
6. Di AWS RAM konsol, pilih Buat berbagi sumber daya lagi.
7. Tambahkan Nama untuk kolam bersama.
8. Di bawah Pilih jenis sumber daya, pilih kolam IPAM, lalu pilih ARN dari kumpulan yang ingin Anda bagikan.
9. Pilih Selanjutnya.
10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diMembagikan kumpulan IPAM menggunakanAWS RAM.
11. Pilih Selanjutnya.
12. Di bawah Prinsipal > Pilih tipe utama, pilih AWS akun dan masukkan ID akun akun yang akan membawa rentang alamat IP ke IPAM dan pilih Tambah.
13. Pilih Selanjutnya.
14. Tinjau opsi berbagi sumber daya dan prinsipal yang akan Anda bagikan, lalu pilih Buat.
15. Untuk memungkinkan **`member-account`** akun mengalokasikan CIDRS alamat IP dari kolam IPAM, buat berbagi sumber daya kedua dengan `AWSRAMDefaultPermissionsIpamPool` dan buat berbagi sumber daya kedua. Nilai untuk `--resource-arns` adalah ARN dari kolam IPAM yang Anda buat di bagian sebelumnya. Nilai untuk `--principals` adalah ID akun dari**`member-account`**. Nilai untuk `--permission-arns` adalah ARN izin. `AWSRAMDefaultPermissionsIpamPool`

Langkah 4: Buat VPC

Selesaikan langkah-langkah dalam Membuat VPC di Panduan Pengguna Amazon VPC.

Langkah ini harus dilakukan oleh akun anggota.

> **Note**
>
> - Saat Anda membuka VPC di konsol AWS Manajemen, AWS Wilayah tempat Anda membuat VPC harus sesuai dengan `Locale` opsi yang Anda pilih saat membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

- Ketika Anda mencapai langkah untuk memilih CIDR untuk VPC, Anda akan memiliki opsi untuk menggunakan CIDR dari kolam IPAM. Pilih kolam Regional yang Anda buat dalam tutorial ini.

Saat Anda membuat VPC, AWS mengalokasikan CIDR di kolam IPAM ke VPC. Anda dapat melihat alokasi di IPAM dengan memilih kumpulan di panel konten konsol IPAM dan melihat tab Alokasi untuk kumpulan.

Langkah 5: Iklankan CIDR

Langkah-langkah di bagian ini harus dilakukan oleh akun IPAM. Setelah Anda membuat VPC, Anda kemudian dapat mulai mengiklankan CIDR yang Anda bawa ke kolam AWS yang memiliki Layanan EC2 (EIP/VPC) yang dikonfigurasi. Dalam tutorial ini, itu adalah kumpulan Regional Anda. Secara default CIDR tidak diiklankan, yang berarti tidak dapat diakses publik melalui internet.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk mengiklankan CIDR

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Pilih ruang lingkup publik. Untuk informasi lebih lanjut tentang cakupan, lihatCara kerja IPAM.
4. Pilih kolam Regional yang Anda buat dalam tutorial ini.
5. Pilih tab CIDR.
6. Pilih CIDR BYOIP dan pilih Actions > Advertise.
7. Pilih Iklan CIDR.

Akibatnya, CIDR BYOIP diiklankan dan nilai di kolom Iklan berubah dari Ditarik ke Iklan.

Langkah 6: Pembersihan

Ikuti langkah-langkah di bagian ini untuk membersihkan sumber daya yang telah Anda sediakan dan buat dalam tutorial ini.

Langkah 1: Tarik CIDR dari iklan

Langkah ini harus dilakukan oleh akun IPAM.

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Pilih ruang lingkup publik.
4. Pilih kolam Regional yang Anda buat dalam tutorial ini.
5. Pilih tab CIDR.
6. Pilih CIDR BYOIP dan pilih Actions > Withdraw from advertising.
7. Pilih Tarik CIDR.

Akibatnya, CIDR BYOIP tidak lagi diiklankan dan nilai di kolom Iklan berubah dari Diiklankan menjadi Ditarik.

Langkah 2: Hapus VPC

Langkah ini harus dilakukan oleh akun anggota.

- Selesaikan langkah-langkah dalam Menghapus VPC di Panduan Pengguna Amazon VPC untuk menghapus VPC. Saat Anda membuka VPC di konsol AWS Manajemen, AWS Wilayah menghapus VPC dari harus cocok dengan `Locale` opsi yang Anda pilih saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP. Dalam tutorial ini, kolam itu adalah kolam Regional.

  Saat Anda menghapus VPC, perlu waktu bagi IPAM untuk menemukan bahwa sumber daya telah dihapus dan mengalokasikan CIDR yang dialokasikan ke VPC. Anda tidak dapat melanjutkan ke langkah berikutnya dalam pembersihan sampai Anda melihat bahwa IPAM telah menghapus alokasi dari kumpulan di tab Alokasi detail kumpulan.

Langkah 3: Hapus berbagi RAM dan nonaktifkan integrasi RAM dengan AWS Organizations

Langkah ini harus dilakukan oleh akun IPAM dan akun manajemen masing-masing.

- Selesaikan langkah-langkah dalam Menghapus berbagi sumber daya di AWS RAM dan Menonaktifkan berbagi sumber daya dengan AWS Organizations dalam Panduan Pengguna AWS RAM, dalam urutan itu, untuk menghapus berbagi RAM dan menonaktifkan integrasi RAM dengan Organizations. AWS

Langkah 4: Singkirkan CIDR dari kolam Regional dan kolam tingkat atas

Langkah ini harus dilakukan oleh akun IPAM.

- Selesaikan langkah-langkah Deprovision CIDR dari kolam untuk menghentikan penyediaan CIDR dari kolam Regional dan kemudian kolam tingkat atas, dalam urutan itu.

Langkah 5: Hapus kolam Regional dan kolam tingkat atas

Langkah ini harus dilakukan oleh akun IPAM.

- Selesaikan langkah-langkah Menghapus kolam kolam kolam kolam kolam kolam renang untuk menghapus kolam Regional dan kemudian kolam tingkat atas, dalam urutan itu.

Bawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS

Ikuti langkah-langkah ini untuk membawa IPv4 atau IPv6 CIDR ke IPAM hanya menggunakan CLI. AWS

Important

- Sebelum Anda memulai tutorial ini, selesaikan langkah-langkah dalam prasyarat Onboarding untuk rentang alamat BYOIP Anda di Panduan Pengguna Amazon EC2.

  Saat Anda membuat ROA, untuk IPv4 CIDR Anda harus mengatur panjang maksimum awalan alamat IP ke. `/24` Untuk IPv6 CIDR, jika Anda menambahkannya ke kolam yang dapat diiklankan, panjang maksimum prefiks alamat IP harus. `/48` Ini memastikan bahwa Anda memiliki fleksibilitas penuh untuk membagi alamat IP publik Anda di seluruh AWS Wilayah. IPAM memberlakukan panjang maksimum yang Anda tetapkan. Panjang maksimum adalah pengumuman panjang awalan terkecil yang akan Anda izinkan untuk rute ini. Misalnya, jika Anda membawa blok `/20` CIDR ke AWS, dengan menyetel panjang maksimum`/24`, Anda dapat membagi blok yang lebih besar dengan cara apa pun yang Anda suka (seperti dengan`/21`,`/22`, atau`/24`) dan mendistribusikan blok CIDR yang lebih kecil itu ke Wilayah mana pun. Jika Anda menetapkan panjang maksimum`/23`, Anda tidak akan dapat membagi dan mengiklankan a `/24` dari blok yang lebih besar. Juga, perhatikan bahwa itu `/24` adalah blok IPv4 terkecil dan `/48` merupakan blok IPv6 terkecil yang dapat Anda iklankan dari Wilayah ke internet.

- Setelah Anda membawa rentang alamat IPv4 AWS, Anda dapat menggunakan semua alamat IP dalam rentang tersebut, termasuk alamat pertama (alamat jaringan) dan alamat terakhir (alamat siaran).

Konten

- Bawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS
- Bawa IPv6 CIDR Anda sendiri ke IPAM hanya menggunakan CLI AWS

Bawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS

Ikuti langkah-langkah ini untuk membawa IPv4 CIDR ke IPAM dan mengalokasikan alamat IP Elastis (EIP) dengan CIDR hanya menggunakan. AWS CLI

⚠ Important

- Anda tidak dapat menyediakan atau mengiklankan rentang alamat BYOIP di Local Zones saat ini.
- Tutorial ini mengasumsikan Anda telah menyelesaikan langkah-langkah di bagian berikut:
  - Integrasikan IPAM dengan akun di Organisasi AWS.
  - Buat IPAM.
- Setiap langkah tutorial ini harus dilakukan oleh salah satu dari tiga akun AWS Organizations:
  - Akun manajemen.
  - Akun anggota dikonfigurasi untuk menjadi administrator IPAM Anda diIntegrasikan IPAM dengan akun di Organisasi AWS. Dalam tutorial ini, akun ini akan disebut akun IPAM.
  - Akun anggota di organisasi Anda yang akan mengalokasikan CIDR dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

- Langkah 1: Buat profil AWS CLI bernama dan peran IAM
- Langkah 2: Buat IPAM
- Langkah 3: Buat kolam IPAM tingkat atas

- Langkah 4: Menyediakan CIDR ke kolam tingkat atas
- Langkah 5: Buat kolam Regional di dalam kolam tingkat atas
- Langkah 6: Menyediakan CIDR ke kolam Regional
- Langkah 7. Bagikan kolam Regional
- Langkah 8: Buat kolam IPv4 publik
- Langkah 9: Menyediakan IPv4 CIDR publik ke kolam IPv4 publik Anda
- Langkah 10: Buat alamat IP Elastis dari kolam IPv4 publik
- Langkah 11: Iklankan CIDR
- Langkah 12: Pembersihan

Langkah 1: Buat profil AWS CLI bernama dan peran IAM

Untuk menyelesaikan tutorial ini sebagai AWS pengguna tunggal, Anda dapat menggunakan profil AWS CLI bernama untuk beralih dari satu peran IAM ke peran lainnya. Profil bernama adalah kumpulan pengaturan dan kredensional yang Anda rujuk saat menggunakan `--profile` opsi dengan. AWS CLI Untuk informasi selengkapnya tentang cara membuat peran IAM dan profil bernama untuk AWS akun, lihat Menggunakan peran IAM di AWS CLI di Panduan Pengguna AWS Identity and Access Management.

Buat satu peran dan satu profil bernama untuk masing-masing dari tiga AWS akun yang akan Anda gunakan dalam tutorial ini:

- Profil yang disebut `management-account` akun manajemen AWS Organizations.
- Profil yang dipanggil `ipam-account` untuk akun anggota AWS Organizations yang dikonfigurasi untuk menjadi administrator IPAM Anda.
- Profil yang dipanggil `member-account` untuk akun anggota AWS Organizations di organisasi Anda yang akan mengalokasikan CIDR dari kolam IPAM.

Setelah Anda membuat peran IAM dan profil bernama, kembali ke halaman ini dan lanjutkan ke langkah berikutnya. Anda akan melihat sepanjang sisa tutorial ini bahwa AWS CLI perintah sampel menggunakan `--profile` opsi dengan salah satu profil bernama untuk menunjukkan akun mana yang harus menjalankan perintah.

Langkah 2: Buat IPAM

Langkah ini bersifat opsional. Jika Anda sudah memiliki IPAM yang dibuat dengan Wilayah operasi `us-east-1` dan `us-west-2` dibuat, Anda dapat melewati langkah ini. Buat IPAM dan tentukan wilayah operasi `us-east-1` dan`us-west-2`. Anda harus memilih wilayah operasi sehingga Anda dapat menggunakan opsi lokal ketika Anda membuat kolam IPAM Anda. Integrasi IPAM dengan BYOIP mengharuskan lokal diatur pada kumpulan mana pun yang akan digunakan untuk BYOIP CIDR.

Langkah ini harus dilakukan oleh akun IPAM.

Jalankan perintah berikut:

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

Dalam output, Anda akan melihat IPAM yang telah Anda buat. Perhatikan nilai untuk `PublicDefaultScopeId`. Anda akan memerlukan ID lingkup publik Anda di langkah berikutnya. Anda menggunakan ruang lingkup publik karena BYOIP CIDR adalah alamat IP publik, yang dimaksudkan untuk ruang lingkup publik.

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

Langkah 3: Buat kolam IPAM tingkat atas

Selesaikan langkah-langkah di bagian ini untuk membuat kolam IPAM tingkat atas.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk membuat kumpulan alamat IPv4 untuk semua AWS sumber daya Anda menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat kolam IPAM. Gunakan ID lingkup publik IPAM yang Anda buat pada langkah sebelumnya.

   Langkah ini harus dilakukan oleh akun 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
   ```

   Dalam output, Anda akan melihat`create-in-progress`, yang menunjukkan bahwa pembuatan pool sedang berlangsung.

   ```
   {
       "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. Jalankan perintah berikut sampai Anda melihat status `create-complete` dalam output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Contoh output berikut menunjukkan keadaan kolam.

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

Langkah 4: Menyediakan CIDR ke kolam tingkat atas

Menyediakan blok CIDR ke kolam tingkat atas. Perhatikan bahwa saat menyediakan IPv4 CIDR ke kolam dalam kumpulan tingkat atas, IPv4 CIDR minimum yang dapat Anda berikan adalah`/24`; CIDR yang lebih spesifik (seperti) tidak diizinkan. `/25` Anda harus menyertakan CIDR dan pesan BYOIP dan tanda tangan sertifikat dalam permintaan sehingga kami dapat memverifikasi bahwa Anda memiliki ruang publik. Untuk daftar prasyarat BYOIP termasuk cara mendapatkan pesan BYOIP ini dan tanda tangan sertifikat, lihat. Bawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS

Langkah ini harus dilakukan oleh akun IPAM.

> **Important**
>
> Anda hanya perlu menambahkan `--cidr-authorization-context` ketika Anda menyediakan BYOIP CIDR ke kolam tingkat atas. Untuk kolam Regional dalam kolam tingkat atas, Anda dapat menghilangkan opsi. `--cidr-authorization-context` Setelah Anda memasukkan BYOIP Anda ke IPAM, Anda tidak diharuskan untuk melakukan validasi kepemilikan saat Anda membagi BYOIP di seluruh Wilayah dan akun.

Untuk menyediakan blok CIDR ke kolam menggunakan AWS CLI

1. Jalankan perintah berikut untuk menyediakan CIDR.

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

   Dalam output, Anda akan melihat ketentuan CIDR yang tertunda.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan.

> **Important**
>
> Meskipun sebagian besar penyediaan akan selesai dalam waktu dua jam, mungkin diperlukan waktu hingga satu minggu untuk menyelesaikan proses penyediaan untuk rentang yang dapat diiklankan secara publik.

Jalankan perintah berikut sampai Anda melihat status `provisioned` dalam output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Contoh output berikut menunjukkan keadaan.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

Langkah 5: Buat kolam Regional di dalam kolam tingkat atas

Buat kolam Regional di dalam kolam tingkat atas. `--locale`diperlukan di kolam renang dan itu harus menjadi salah satu Wilayah operasi yang Anda konfigurasikan saat Anda membuat IPAM. Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari kolam IPAM yang berbagi lokal dengan Wilayah VPC. Perhatikan bahwa ketika Anda telah memilih lokal untuk kolam, Anda tidak dapat memodifikasinya. Jika wilayah asal IPAM tidak tersedia karena pemadaman dan kolam memiliki lokal yang berbeda dari wilayah asal IPAM, kolam masih dapat digunakan untuk mengalokasikan alamat IP.

Langkah ini harus dilakukan oleh akun IPAM.

Memilih lokal memastikan tidak ada dependensi lintas wilayah antara kumpulan Anda dan sumber daya yang dialokasikan darinya. Opsi yang tersedia berasal dari Wilayah operasi yang Anda pilih saat

Anda membuat IPAM Anda. Dalam tutorial ini, kita akan menggunakan `us-west-2` sebagai lokal untuk kolam Regional.

> **Important**
>
> Saat Anda membuat kolam, Anda harus menyertakan`--aws-service ec2`. Layanan yang Anda pilih menentukan AWS layanan di mana CIDR akan dapat diiklankan. Saat ini, satu-satunya pilihan adalah`ec2`, yang berarti bahwa CIDR yang dialokasikan dari kumpulan ini akan dapat diiklankan untuk layanan Amazon EC2 (untuk alamat IP Elastis) dan layanan Amazon VPC (untuk CIDR yang terkait dengan VPC).

Untuk membuat kolam Regional menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat pool.

```
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
```

   Dalam output, Anda akan melihat IPAM membuat pool.

```
{
     "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. Jalankan perintah berikut sampai Anda melihat status `create-complete` dalam output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Dalam output, Anda melihat pool yang Anda miliki di IPAM Anda. Dalam tutorial ini, kami membuat top-level dan pool Regional, sehingga Anda akan melihat keduanya.

Langkah 6: Menyediakan CIDR ke kolam Regional

Menyediakan blok CIDR ke kolam Regional. Perhatikan bahwa saat menyediakan CIDR ke kolam dalam kumpulan tingkat atas, IPv4 CIDR minimum yang dapat Anda berikan adalah`/24`; CIDR yang lebih spesifik (seperti) tidak diizinkan. `/25` Setelah Anda membuat kolam regional pertama, Anda dapat membuat kolam yang lebih kecil (seperti`/25`) di dalam kolam regional.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk menetapkan blok CIDR ke kumpulan Regional menggunakan AWS CLI

1. Jalankan perintah berikut untuk menyediakan 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
```

Dalam output, Anda akan melihat ketentuan CIDR yang tertunda.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Jalankan perintah berikut sampai Anda melihat status `provisioned` dalam output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Contoh output berikut menunjukkan keadaan yang benar.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

Langkah 7. Bagikan kolam Regional

Ikuti langkah-langkah di bagian ini untuk berbagi kolam IPAM menggunakan AWS Resource Access Manager (RAM).

Aktifkan berbagi sumber daya di AWS RAM

Setelah membuat IPAM, Anda akan ingin berbagi kumpulan regional dengan akun lain di organisasi Anda. Sebelum Anda berbagi kolam IPAM, selesaikan langkah-langkah di bagian ini untuk mengaktifkan berbagi AWS RAM sumber daya. Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`management-account`** opsi.

Untuk mengaktifkan berbagi sumber daya

1. Menggunakan akun AWS Organizations manajemen, buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Di panel navigasi kiri, pilih Pengaturan, pilih Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

Anda sekarang dapat berbagi kolam IPAM dengan anggota organisasi lainnya.

Bagikan kolam IPAM menggunakan AWS RAM

Di bagian ini Anda akan membagikan kumpulan regional dengan akun AWS Organizations anggota lain. Untuk petunjuk lengkap tentang berbagi kumpulan IPAM, termasuk informasi tentang izin

IAM yang diperlukan, lihat. Membagikan kumpulan IPAM menggunakanAWS RAM Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`ipam-account`** opsi.

Untuk berbagi kolam IPAM menggunakan AWS RAM

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi, pilih kolam IPAM, dan pilih Tindakan > Lihat detail.
4. Di bawah Berbagi sumber daya, pilih Buat berbagi sumber daya. AWS RAM Konsol terbuka. Anda berbagi kolam menggunakan AWS RAM.
5. Pilih Buat berbagi sumber daya.
6. Di AWS RAM konsol, pilih Buat berbagi sumber daya lagi.
7. Tambahkan Nama untuk kolam bersama.
8. Di bawah Pilih jenis sumber daya, pilih kolam IPAM, lalu pilih ARN dari kumpulan yang ingin Anda bagikan.
9. Pilih Selanjutnya.
10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diMembagikan kumpulan IPAM menggunakanAWS RAM.
11. Pilih Selanjutnya.
12. Di bawah Prinsipal > Pilih tipe utama, pilih AWS akun dan masukkan ID akun akun yang akan membawa rentang alamat IP ke IPAM dan pilih Tambah.
13. Pilih Selanjutnya.
14. Tinjau opsi berbagi sumber daya dan prinsipal yang akan Anda bagikan, lalu pilih Buat.
15. Untuk memungkinkan **`member-account`** akun mengalokasikan CIDRS alamat IP dari kolam IPAM, buat berbagi sumber daya kedua dengan `AWSRAMDefaultPermissionsIpamPool` dan buat berbagi sumber daya kedua. Nilai untuk `--resource-arns` adalah ARN dari kolam IPAM yang Anda buat di bagian sebelumnya. Nilai untuk `--principals` adalah ID akun dari**`member-account`**. Nilai untuk `--permission-arns` adalah ARN izin. `AWSRAMDefaultPermissionsIpamPool`

Langkah 8: Buat kolam IPv4 publik

Membuat kolam IPv4 publik adalah langkah yang diperlukan untuk membawa alamat IPv4 publik AWS untuk dikelola dengan IPAM. Langkah ini biasanya dilakukan oleh AWS akun lain yang ingin memberikan alamat IP Elastis.

Langkah ini harus dilakukan oleh akun anggota.

> **Important**
>
> Kolam IPv4 publik dan kolam IPAM dikelola oleh sumber daya yang berbeda di. AWS Pool IPv4 publik adalah sumber daya akun tunggal yang memungkinkan Anda mengonversi CIDR milik publik ke alamat IP Elastis. Kolam IPAM dapat digunakan untuk mengalokasikan ruang publik Anda ke kolam IPv4 publik.

Untuk membuat kolam IPv4 publik menggunakan AWS CLI

- Jalankan perintah berikut untuk menyediakan CIDR. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

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

  Dalam output, Anda akan melihat ID kolam IPv4 publik. Anda akan membutuhkan ID ini di langkah berikutnya.

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

Langkah 9: Menyediakan IPv4 CIDR publik ke kolam IPv4 publik Anda

Menyediakan IPv4 CIDR publik ke kolam IPv4 publik Anda. Nilai untuk `--region` harus sesuai dengan `--locale` nilai yang Anda masukkan saat Anda membuat pool yang akan digunakan untuk BYOIP CIDR.

Langkah ini harus dilakukan oleh akun anggota.

Untuk membuat kolam IPv4 publik menggunakan AWS CLI

1. Jalankan perintah berikut untuk menyediakan 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
```

   Dalam output, Anda akan melihat CIDR yang disediakan.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. Jalankan perintah berikut untuk melihat CIDR yang disediakan di kolam IPv4 publik.

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-account
```

   Dalam output, Anda akan melihat CIDR yang disediakan. Secara default CIDR tidak diiklankan, yang berarti tidak dapat diakses publik melalui internet. Anda akan memiliki kesempatan untuk mengatur CIDR ini untuk diiklankan di langkah terakhir tutorial ini.

```
{
    "ByoipCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "StatusMessage": "Cidr successfully provisioned",
            "State": "provisioned"
        }
    ]
}
```

Langkah 10: Buat alamat IP Elastis dari kolam IPv4 publik

Buat alamat IP Elastis (EIP) dari kolam IPv4 publik. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

Langkah ini harus dilakukan oleh akun anggota.

Untuk membuat EIP dari kolam IPv4 publik menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat EIP.

```
aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
ec2-0019eed22a684e0b2 --profile member-account
```

   Dalam output, Anda akan melihat alokasi.

```
{
    "PublicIp": "130.137.245.100",
    "AllocationId": "eipalloc-0db3405026756dbf6",
    "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

2. Jalankan perintah berikut untuk melihat alokasi EIP yang dikelola di IPAM.

   Langkah ini harus dilakukan oleh akun IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   Output menunjukkan alokasi di IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
```

```
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Langkah 11: Iklankan CIDR

Langkah-langkah di bagian ini harus dilakukan oleh akun IPAM. Setelah Anda mengaitkan alamat IP Elastis (EIP) dengan instance atau Elastic Load Balancer, Anda kemudian dapat mulai mengiklankan CIDR yang Anda bawa AWS ke kolam yang telah ditentukan. `--aws-service ec2` Dalam tutorial ini, itu adalah kumpulan Regional Anda. Secara default CIDR tidak diiklankan, yang berarti tidak dapat diakses publik melalui internet. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

Langkah ini harus dilakukan oleh akun IPAM.

Mulai mengiklankan CIDR menggunakan AWS CLI

- Jalankan perintah berikut untuk mengiklankan CIDR.

  ```
  aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
  profile ipam-account
  ```

  Dalam output, Anda akan melihat CIDR diiklankan.

  ```
  {
      "ByoipCidr": {
          "Cidr": "130.137.245.0/24",
          "State": "advertised"
      }
  }
  ```

Langkah 12: Pembersihan

Ikuti langkah-langkah di bagian ini untuk membersihkan sumber daya yang telah Anda sediakan dan buat dalam tutorial ini. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

Bersihkan menggunakan AWS CLI

1. Lihat alokasi EIP yang dikelola di IPAM.

   Langkah ini harus dilakukan oleh akun IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   Output menunjukkan alokasi di 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. Berhenti mengiklankan IPv4 CIDR.

   Langkah ini harus dilakukan oleh akun IPAM.

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
   profile ipam-account
   ```

   Dalam output, Anda akan melihat CIDR State telah berubah dari diiklankan ke provisioned.

   ```
   {
       "ByoipCidr": {
           "Cidr": "130.137.245.0/24",
           "State": "provisioned"
       }
   }
   ```

3. Lepaskan alamat IP Elastis.

Langkah ini harus dilakukan oleh akun anggota.

```
aws ec2 release-address --region us-west-2 --allocation-
id eipalloc-0db3405026756dbf6 --profile member-account
```

Anda tidak akan melihat output apa pun saat menjalankan perintah ini.

4. Lihat CIDR BYOIP Anda.

   Langkah ini harus dilakukan oleh akun anggota.

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

   Dalam output, Anda akan melihat alamat IP di BYOIP CIDR Anda.

   ```
   {
       "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. Lepaskan alamat IP terakhir di CIDR dari kolam IPv4 publik. Masukkan alamat IP dengan netmask /32. Anda harus menjalankan kembali perintah ini untuk setiap alamat IP dalam rentang CIDR. Jika CIDR Anda adalah a`/24`, Anda harus menjalankan perintah ini untuk menghentikan penyediaan masing-masing 256 alamat IP di CIDR. `/24` Ketika Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus cocok dengan Wilayah IPAM Anda.

Langkah ini harus dilakukan oleh akun anggota.

```
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
```

Dalam output, Anda akan melihat CIDR yang telah di-deprovisioned.

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}
```

6. Lihat CIDR BYOIP Anda lagi dan pastikan tidak ada lagi alamat yang disediakan. Ketika Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus cocok dengan Wilayah IPAM Anda.

   Langkah ini harus dilakukan oleh akun anggota.

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
   ```

   Dalam output, Anda akan melihat jumlah alamat IP di kolam IPv4 publik Anda.

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

```
}
```

7. Lihat alokasi EIP tidak lagi dikelola di IPAM. Perlu beberapa waktu bagi IPAM untuk menemukan bahwa alamat IP Elastis telah dihapus. Anda tidak dapat terus membersihkan dan menghentikan penyediaan CIDR kolam IPAM sampai Anda melihat bahwa alokasi telah dihapus dari IPAM. Ketika Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus cocok dengan opsi --locale yang Anda masukkan saat Anda membuat pool yang akan digunakan untuk CIDR BYOIP.

   Langkah ini harus dilakukan oleh akun IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   Output menunjukkan alokasi di IPAM.

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

8. Pemberhentian kolam Regional CIDR. Ketika Anda menjalankan perintah dalam langkah ini, nilai untuk `--region` harus cocok dengan Wilayah IPAM Anda.

   Langkah ini harus dilakukan oleh akun 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
   ```

   Dalam output, Anda akan melihat CIDR menunggu deprovision.

   ```
   {
       "IpamPoolCidr": {

           "Cidr": "130.137.245.0/24",

           "State": "pending-deprovision"

       }

   }
   ```

Deprovisioning membutuhkan waktu untuk menyelesaikannya. Periksa status deprovisioning.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Tunggu sampai Anda melihat deprovisioned sebelum Anda melanjutkan ke langkah berikutnya.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. Hapus berbagi RAM dan nonaktifkan integrasi RAM dengan AWS Organizations. Selesaikan langkah-langkah dalam Menghapus berbagi sumber daya di AWS RAM dan Menonaktifkan berbagi sumber daya dengan AWS Organizations dalam Panduan Pengguna AWS RAM, dalam urutan itu, untuk menghapus berbagi RAM dan menonaktifkan integrasi RAM dengan Organizations. AWS

   Langkah ini harus dilakukan oleh akun IPAM dan akun manajemen masing-masing. Jika Anda menggunakan AWS CLI untuk menghapus berbagi RAM dan menonaktifkan integrasi RAM, gunakan `--profile management-account` opsi `--profile ipam-account` dan.

10. Hapus kolam Regional. Ketika Anda menjalankan perintah dalam langkah ini, nilai untuk `--region` harus cocok dengan Region IPAM Anda.

    Langkah ini harus dilakukan oleh akun IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

    Dalam output, Anda dapat melihat status hapus.

```
{
   "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. Deprovisi kolam tingkat atas CIDR. Ketika Anda menjalankan perintah dalam langkah ini, nilai untuk `--region` harus cocok dengan Wilayah IPAM Anda.

    Langkah ini harus dilakukan oleh akun 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
    ```

    Dalam output, Anda akan melihat CIDR menunggu deprovision.

    ```
    {
        "IpamPoolCidr": {

            "Cidr": "130.137.245.0/24",

            "State": "pending-deprovision"

        }

    }
    ```

    Deprovisioning membutuhkan waktu untuk menyelesaikannya. Jalankan perintah berikut untuk memeriksa status deprovisioning.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Tunggu sampai Anda melihat deprovisioned sebelum Anda melanjutkan ke langkah berikutnya.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

12. Hapus kolam tingkat atas. Ketika Anda menjalankan perintah dalam langkah ini, nilai untuk `--region` harus cocok dengan Region IPAM Anda.

    Langkah ini harus dilakukan oleh akun IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

    Dalam output, Anda dapat melihat status hapus.

```
{
  "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. Hapus IPAM. Ketika Anda menjalankan perintah dalam langkah ini, nilai untuk `--region` harus cocok dengan Region IPAM Anda.

    Langkah ini harus dilakukan oleh akun IPAM.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    Dalam output, Anda akan melihat respon IPAM. Ini berarti IPAM telah dihapus.

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

Bawa IPv6 CIDR Anda sendiri ke IPAM hanya menggunakan CLI AWS

Ikuti langkah-langkah ini untuk membawa IPv6 CIDR ke IPAM dan mengalokasikan VPC hanya menggunakan. AWS CLI

Important

- Anda tidak dapat menyediakan atau mengiklankan rentang alamat BYOIP di Local Zones saat ini.
- Tutorial ini mengasumsikan Anda telah menyelesaikan langkah-langkah di bagian berikut:
  - Integrasikan IPAM dengan akun di Organisasi AWS.
  - Buat IPAM.
- Setiap langkah tutorial ini harus dilakukan oleh salah satu dari tiga akun AWS Organizations:
  - Akun manajemen.
  - Akun anggota dikonfigurasi untuk menjadi administrator IPAM Anda diIntegrasikan IPAM dengan akun di Organisasi AWS. Dalam tutorial ini, akun ini akan disebut akun IPAM.
  - Akun anggota di organisasi Anda yang akan mengalokasikan CIDR dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

- Langkah 1: Buat profil AWS CLI bernama dan peran IAM
- Langkah 2: Buat IPAM
- Langkah 3: Buat kolam IPAM
- Langkah 4: Menyediakan CIDR ke kolam tingkat atas
- Langkah 5: Buat kolam Regional di dalam kolam tingkat atas
- Langkah 6: Menyediakan CIDR ke kolam Regional
- Langkah 7. Bagikan kolam Regional
- Langkah 8: Buat VPC menggunakan IPv6 CIDR
- Langkah 9: Iklankan CIDR
- Langkah 10: Pembersihan

Langkah 1: Buat profil AWS CLI bernama dan peran IAM

Untuk menyelesaikan tutorial ini sebagai AWS pengguna tunggal, Anda dapat menggunakan profil AWS CLI bernama untuk beralih dari satu peran IAM ke peran lainnya. Profil bernama adalah kumpulan pengaturan dan kredensional yang Anda rujuk saat menggunakan `--profile` opsi dengan. AWS CLI Untuk informasi selengkapnya tentang cara membuat peran IAM dan profil bernama untuk AWS akun, lihat Menggunakan peran IAM di AWS CLI di Panduan Pengguna AWS Identity and Access Management.

Buat satu peran dan satu profil bernama untuk masing-masing dari tiga AWS akun yang akan Anda gunakan dalam tutorial ini:

- Sebuah profil yang disebut `management-account` untuk akun manajemen AWS Organizations.
- Profil yang dipanggil `ipam-account` untuk akun anggota AWS Organizations yang dikonfigurasi untuk menjadi administrator IPAM Anda.
- Profil yang dipanggil `member-account` untuk akun anggota AWS Organizations di organisasi Anda yang akan mengalokasikan CIDR dari kolam IPAM.

Setelah Anda membuat peran IAM dan profil bernama, kembali ke halaman ini dan lanjutkan ke langkah berikutnya. Anda akan melihat sepanjang sisa tutorial ini bahwa AWS CLI perintah sampel menggunakan `--profile` opsi dengan salah satu profil bernama untuk menunjukkan akun mana yang harus menjalankan perintah.

Langkah 2: Buat IPAM

Langkah ini bersifat opsional. Jika Anda sudah memiliki IPAM yang dibuat dengan Wilayah operasi `us-east-1` dan `us-west-2` dibuat, Anda dapat melewati langkah ini. Buat IPAM dan tentukan wilayah operasi `us-east-1` dan`us-west-2`. Anda harus memilih wilayah operasi sehingga Anda dapat menggunakan opsi lokal ketika Anda membuat kolam IPAM Anda. Integrasi IPAM dengan BYOIP mengharuskan lokal diatur pada kumpulan mana pun yang akan digunakan untuk BYOIP CIDR.

Langkah ini harus dilakukan oleh akun IPAM.

Jalankan perintah berikut:

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

Dalam output, Anda akan melihat IPAM yang telah Anda buat. Perhatikan nilai untuk `PublicDefaultScopeId`. Anda akan memerlukan ID lingkup publik Anda di langkah berikutnya.


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


Langkah 3: Buat kolam IPAM

Karena Anda akan membuat kolam IPAM tingkat atas dengan kolam Regional di dalamnya, dan kami akan mengalokasikan ruang untuk sumber daya (VPC) dari kolam Regional, Anda akan mengatur lokal di kolam Regional dan bukan kolam tingkat atas. Anda akan menambahkan lokal ke kolam Regional saat membuat kumpulan Regional di langkah selanjutnya. Integrasi IPAM dengan BYOIP mengharuskan lokal diatur pada kumpulan mana pun yang akan digunakan untuk BYOIP CIDR.

Langkah ini harus dilakukan oleh akun IPAM.

Pilih apakah Anda ingin CIDR kolam IPAM ini dapat diiklankan AWS melalui internet publik (atau). `--publicly-advertisable` `--no-publicly-advertisable`

> **Note**
>
> Perhatikan bahwa ID lingkup harus menjadi ID untuk ruang lingkup publik dan keluarga alamat harus`ipv6`.

Untuk membuat kumpulan alamat IPv6 untuk semua AWS sumber daya Anda menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat kolam IPAM. Gunakan ID lingkup publik IPAM yang Anda buat pada langkah sebelumnya.

```
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
```

Dalam output, Anda akan melihat`create-in-progress`, yang menunjukkan bahwa pembuatan pool sedang berlangsung.

```
{
    "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. Jalankan perintah berikut sampai Anda melihat status `create-complete` dalam output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Contoh output berikut menunjukkan keadaan kolam.

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

```
    }

}
```

Langkah 4: Menyediakan CIDR ke kolam tingkat atas

Menyediakan blok CIDR ke kolam tingkat atas. Perhatikan bahwa saat menyediakan IPv6 CIDR ke kolam dalam kumpulan tingkat atas, rentang alamat IPv6 paling spesifik yang dapat Anda bawa adalah/48 untuk CIDR yang dapat diiklankan secara publik dan /60 untuk CIDR yang tidak dapat diiklankan secara publik. Anda harus menyertakan CIDR dan pesan BYOIP dan tanda tangan sertifikat dalam permintaan sehingga kami dapat memverifikasi bahwa Anda memiliki ruang publik. Untuk daftar prasyarat BYOIP termasuk cara mendapatkan pesan BYOIP ini dan tanda tangan sertifikat, lihat. Bawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS

Anda hanya perlu menambahkan `--cidr-authorization-context` ketika Anda menyediakan BYOIP CIDR ke kolam tingkat atas. Untuk kolam Regional dalam kolam tingkat atas, Anda dapat menghilangkan opsi. `--cidr-authorization-context`

Langkah ini harus dilakukan oleh akun IPAM.

Untuk menyediakan blok CIDR ke kolam menggunakan AWS CLI

1. Jalankan perintah berikut untuk menyediakan CIDR.

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

Dalam output, Anda akan melihat ketentuan CIDR yang tertunda.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",
```

```
        "State": "pending-provision"

    }

}
```

2. Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan.

> **Important**
>
> Meskipun sebagian besar penyediaan akan selesai dalam waktu dua jam, mungkin diperlukan waktu hingga satu minggu untuk menyelesaikan proses penyediaan untuk rentang yang dapat diiklankan secara publik.

Jalankan perintah berikut sampai Anda melihat status `provisioned` dalam output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Contoh output berikut menunjukkan keadaan.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Langkah 5: Buat kolam Regional di dalam kolam tingkat atas

Buat kolam Regional di dalam kolam tingkat atas. `--locale`diperlukan di kolam renang dan itu harus menjadi salah satu Wilayah operasi yang Anda konfigurasikan saat Anda membuat IPAM.

Langkah ini harus dilakukan oleh akun IPAM.

> **Important**
>
> Saat Anda membuat kolam, Anda harus menyertakan`--aws-service ec2`. Layanan yang Anda pilih menentukan AWS layanan di mana CIDR akan dapat diiklankan. Saat ini, satu-satunya pilihan adalah`ec2`, yang berarti bahwa CIDR yang dialokasikan dari kumpulan ini akan dapat diiklankan untuk layanan Amazon EC2 dan layanan Amazon VPC (untuk CIDR yang terkait dengan VPC).

Untuk membuat kolam Regional menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat pool.

```
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
```

   Dalam output, Anda akan melihat IPAM membuat pool.

```
{
    "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. Jalankan perintah berikut sampai Anda melihat status `create-complete` dalam output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Dalam output, Anda melihat pool yang Anda miliki di IPAM Anda. Dalam tutorial ini, kami membuat top-level dan kolam Regional, sehingga Anda akan melihat keduanya.

Langkah 6: Menyediakan CIDR ke kolam Regional

Menyediakan blok CIDR ke kolam Regional. Perhatikan bahwa saat menyediakan CIDR ke kolam dalam kumpulan tingkat atas, rentang alamat IPv6 paling spesifik yang dapat Anda bawa adalah/48 untuk CIDR yang dapat diiklankan secara publik dan /60 untuk CIDR yang tidak dapat diiklankan secara publik.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk menetapkan blok CIDR ke kumpulan Regional menggunakan AWS CLI

1. Jalankan perintah berikut untuk menyediakan 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
```

Dalam output, Anda akan melihat ketentuan CIDR yang tertunda.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
}
```

2. Jalankan perintah berikut sampai Anda melihat status `provisioned` dalam output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Contoh output berikut menunjukkan keadaan yang benar.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Langkah 7. Bagikan kolam Regional

Ikuti langkah-langkah di bagian ini untuk berbagi kolam IPAM menggunakan AWS Resource Access Manager (RAM).

Aktifkan berbagi sumber daya di AWS RAM

Setelah membuat IPAM, Anda akan ingin berbagi kumpulan regional dengan akun lain di organisasi Anda. Sebelum Anda berbagi kolam IPAM, selesaikan langkah-langkah di bagian ini untuk mengaktifkan berbagi AWS RAM sumber daya. Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`management-account`** opsi.

Untuk mengaktifkan berbagi sumber daya

1. Menggunakan akun AWS Organizations manajemen, buka AWS RAM konsol di https://console.aws.amazon.com/ram/.
2. Di panel navigasi kiri, pilih Pengaturan, pilih Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

Anda sekarang dapat berbagi kolam IPAM dengan anggota organisasi lainnya.

Bagikan kolam IPAM menggunakan AWS RAM

Di bagian ini, Anda akan membagikan kumpulan regional dengan akun AWS Organizations anggota lain. Untuk petunjuk lengkap tentang berbagi kumpulan IPAM, termasuk informasi tentang izin IAM yang diperlukan, lihat. Membagikan kumpulan IPAM menggunakanAWS RAM Jika Anda menggunakan AWS CLI untuk mengaktifkan berbagi sumber daya, gunakan `--profile` **`ipam-account`** opsi.

Untuk berbagi kolam IPAM menggunakan AWS RAM

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi, pilih kolam IPAM, dan pilih Tindakan > Lihat detail.
4. Di bawah Berbagi sumber daya, pilih Buat berbagi sumber daya. AWS RAM Konsol terbuka. Anda berbagi kolam menggunakan AWS RAM.
5. Pilih Buat berbagi sumber daya.
6. Di AWS RAM konsol, pilih Buat berbagi sumber daya lagi.
7. Tambahkan Nama untuk kolam bersama.
8. Di bawah Pilih jenis sumber daya, pilih kolam IPAM, lalu pilih ARN dari kumpulan yang ingin Anda bagikan.
9. Pilih Selanjutnya.
10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diMembagikan kumpulan IPAM menggunakanAWS RAM.
11. Pilih Selanjutnya.
12. Di bawah Prinsipal > Pilih tipe utama, pilih AWS akun dan masukkan ID akun akun yang akan membawa rentang alamat IP ke IPAM dan pilih Tambah.
13. Pilih Selanjutnya.
14. Tinjau opsi berbagi sumber daya dan prinsipal yang akan Anda bagikan, lalu pilih Buat.
15. Untuk memungkinkan **`member-account`** akun mengalokasikan CIDRS alamat IP dari kolam IPAM, buat berbagi sumber daya kedua dengan `AWSRAMDefaultPermissionsIpamPool` dan buat berbagi sumber daya kedua. Nilai untuk `--resource-arns` adalah ARN dari kolam IPAM yang Anda buat di bagian sebelumnya. Nilai untuk `--principals` adalah ID akun dari**`member-account`**. Nilai untuk `--permission-arns` adalah ARN dari izin. `AWSRAMDefaultPermissionsIpamPool`

Langkah 8: Buat VPC menggunakan IPv6 CIDR

Buat VPC menggunakan ID kolam IPAM. Anda harus mengaitkan blok IPv4 CIDR ke VPC juga menggunakan `--cidr-block` opsi atau permintaan akan gagal. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP.

Langkah ini harus dilakukan oleh akun anggota.

Untuk membuat VPC dengan IPv6 CIDR menggunakan AWS CLI

1. Jalankan perintah berikut untuk menyediakan 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
```

   Dalam output, Anda akan melihat VPC sedang dibuat.

```
{
    "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. Lihat alokasi VPC di IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Dalam output, Anda akan melihat alokasi di IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Langkah 9: Iklankan CIDR

Setelah Anda membuat VPC dengan CIDR yang dialokasikan di IPAM, Anda kemudian dapat mulai mengiklankan CIDR yang Anda bawa ke kolam AWS yang telah ditentukan. `--aws-service ec2` Dalam tutorial ini, itulah kumpulan Regional Anda. Secara default CIDR tidak diiklankan, yang berarti tidak dapat diakses publik melalui internet. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan Regional yang akan digunakan untuk CIDR BYOIP.

Langkah ini harus dilakukan oleh akun IPAM.

Mulai mengiklankan CIDR menggunakan AWS CLI

- Jalankan perintah berikut untuk mengiklankan CIDR.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

Dalam output, Anda akan melihat CIDR diiklankan.

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "advertised"
    }
}
```

Langkah 10: Pembersihan

Ikuti langkah-langkah di bagian ini untuk membersihkan sumber daya yang telah Anda sediakan dan buat dalam tutorial ini. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan Regional yang akan digunakan untuk CIDR BYOIP.

Bersihkan menggunakan AWS CLI

1. Jalankan perintah berikut untuk melihat alokasi VPC yang dikelola di IPAM.

   Langkah ini harus dilakukan oleh akun IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   Output menunjukkan alokasi di IPAM.

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "2605:9cc0:409::/56",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
               "ResourceId": "vpc-00b5573ffc3b31a29",
               "ResourceType": "vpc",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

2. Jalankan perintah berikut untuk berhenti mengiklankan CIDR. Saat Anda menjalankan perintah di langkah ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan Regional yang akan digunakan untuk CIDR BYOIP.

   Langkah ini harus dilakukan oleh akun IPAM.

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
   profile ipam-account
   ```

   Dalam output, Anda akan melihat CIDR State telah berubah dari diiklankan ke provisioned.

   ```
   {
       "ByoipCidr": {
           "Cidr": "2605:9cc0:409::/48",
           "State": "provisioned"
       }
   }
   ```

3. Jalankan perintah berikut untuk menghapus VPC. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan Regional yang akan digunakan untuk CIDR BYOIP.

   Langkah ini harus dilakukan oleh akun anggota.

   ```
   aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
   profile member-account
   ```

   Anda tidak akan melihat output apa pun saat menjalankan perintah ini.

4. Jalankan perintah berikut untuk melihat alokasi VPC di IPAM. Perlu beberapa waktu bagi IPAM untuk menemukan bahwa VPC telah dihapus dan menghapus alokasi ini. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus sesuai dengan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan Regional yang akan digunakan untuk CIDR BYOIP.

   Langkah ini harus dilakukan oleh akun IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

Output menunjukkan alokasi di IPAM.

```
{
   "IpamPoolAllocations": [

        {

            "Cidr": "2605:9cc0:409::/56",

            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",

            "ResourceType": "vpc",

            "ResourceOwner": "123456789012"

        }

    ]

}
```

Jalankan kembali perintah dan cari alokasi yang akan dihapus. Anda tidak dapat terus membersihkan dan menghentikan penyediaan CIDR kolam IPAM sampai Anda melihat bahwa alokasi telah dihapus dari IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Output menunjukkan alokasi dihapus dari IPAM.

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

5. Hapus berbagi RAM dan nonaktifkan integrasi RAM dengan AWS Organizations. Selesaikan langkah-langkah dalam Menghapus berbagi sumber daya di AWS RAM dan Menonaktifkan berbagi sumber daya dengan AWS Organizations dalam Panduan Pengguna AWS RAM,

dalam urutan itu, untuk menghapus berbagi RAM dan menonaktifkan integrasi RAM dengan Organizations. AWS

Langkah ini harus dilakukan oleh akun IPAM dan akun manajemen masing-masing. Jika Anda menggunakan AWS CLI untuk menghapus berbagi RAM dan menonaktifkan integrasi RAM, gunakan `--profile` **`management-account`** opsi `--profile` **`ipam-account`** dan.

6. Jalankan perintah berikut untuk menghentikan penyediaan CIDR kumpulan Regional.

   Langkah ini harus dilakukan oleh akun 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
   ```

   Dalam output, Anda akan melihat CIDR menunggu deprovision.

   ```
   {
       "IpamPoolCidr": {
           "Cidr": "2605:9cc0:409::/48",
           "State": "pending-deprovision"
       }
   }
   ```

   Deprovisioning membutuhkan waktu untuk diselesaikan. Lanjutkan menjalankan perintah sampai Anda melihat status CIDR dibatalkan.

   ```
   aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
   ```

   Dalam output, Anda akan melihat CIDR menunggu deprovision.

   ```
   {
       "IpamPoolCidr": {
           "Cidr": "2605:9cc0:409::/48",
           "State": "deprovisioned"
       }
   }
   ```

7. Jalankan perintah berikut untuk menghapus kumpulan Regional.

   Langkah ini harus dilakukan oleh akun IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Dalam output, Anda dapat melihat status hapus.

```
{
    "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. Jalankan perintah berikut untuk menghentikan penyediaan CIDR kumpulan tingkat atas.

   Langkah ini harus dilakukan oleh akun 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
```

   Dalam output, Anda akan melihat CIDR menunggu deprovision.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
```

```
}
```

Deprovisioning membutuhkan waktu untuk diselesaikan. Jalankan perintah berikut untuk memeriksa status deprovisioning.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Tunggu sampai Anda melihat deprovisioned sebelum Anda melanjutkan ke langkah berikutnya.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. Jalankan perintah berikut untuk menghapus kolam tingkat atas.

   Langkah ini harus dilakukan oleh akun IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Dalam output, Anda dapat melihat status hapus.

```
{
    "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. Jalankan perintah berikut untuk menghapus IPAM.

    Langkah ini harus dilakukan oleh akun IPAM.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    Dalam output, Anda akan melihat respon IPAM. Ini berarti IPAM telah dihapus.

```
{
    "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: Transfer BYOIP IPv4 CIDR ke IPAM

Ikuti langkah-langkah ini untuk mentransfer IPv4 CIDR yang ada ke IPAM. Jika Anda sudah memiliki IPv4 BYOIP CIDR dengan AWS, Anda dapat memindahkan CIDR ke IPAM dari kolam IPv4 publik. Anda tidak dapat memindahkan IPv6 CIDR ke IPAM.

Tutorial ini mengasumsikan Anda telah berhasil membawa rentang alamat IP untuk AWS menggunakan proses yang dijelaskan dalam Bawa alamat IP Anda sendiri (BYOIP) di Amazon EC2 dan sekarang Anda ingin mentransfer rentang alamat IP itu ke IPAM. Jika Anda membawa alamat IP baru AWS untuk pertama kalinya, selesaikan langkah-langkahnyaTutorial: Bawa alamat IP Anda ke IPAM.

Jika Anda mentransfer kolam IPv4 publik ke IPAM, tidak ada dampak pada alokasi yang ada. Setelah Anda mentransfer kolam IPv4 publik ke IPAM, tergantung pada jenis sumber daya, Anda mungkin dapat memantau alokasi yang ada. Untuk informasi selengkapnya, lihat Pantau penggunaan CIDR berdasarkan sumber daya.

Important

- Tutorial ini mengasumsikan Anda telah menyelesaikan langkah-langkahnya. Buat IPAM
- Setiap langkah tutorial ini harus dilakukan oleh salah satu dari dua AWS akun:
  - Akun untuk administrator IPAM. Dalam tutorial ini, akun ini akan disebut akun IPAM.
  - Akun di organisasi Anda yang memiliki BYOIP CIDR. Dalam tutorial ini, akun ini akan disebut akun pemilik BYOIP CIDR.

Daftar Isi

- Langkah 1: Buat profil AWS CLI bernama dan peran IAM
- Langkah 2: Dapatkan ID ruang lingkup publik IPAM Anda
- Langkah 3: Buat kolam IPAM
- Langkah 4: Bagikan kolam IPAM menggunakan AWS RAM
- Langkah 5: Transfer CIDR BYOIP IPV4 yang ada ke IPAM
- Langkah 6: Lihat CIDR di IPAM
- Langkah 7: Pembersihan

Langkah 1: Buat profil AWS CLI bernama dan peran IAM

Untuk menyelesaikan tutorial ini sebagai AWS pengguna tunggal, Anda dapat menggunakan profil AWS CLI bernama untuk beralih dari satu peran IAM ke peran lainnya. Profil bernama adalah kumpulan pengaturan dan kredensional yang Anda rujuk saat menggunakan `--profile` opsi dengan. AWS CLI Untuk informasi selengkapnya tentang cara membuat peran IAM dan profil bernama untuk AWS akun, lihat Menggunakan peran IAM di AWS CLI di Panduan Pengguna AWS Identity and Access Management.

Buat satu peran dan satu profil bernama untuk masing-masing dari tiga AWS akun yang akan Anda gunakan dalam tutorial ini:

- Profil memanggil `ipam-account` AWS akun yang merupakan administrator IPAM.
- Profil memanggil `byoip-owner-account` AWS akun di organisasi Anda yang memiliki BYOIP CIDR.

Setelah Anda membuat peran IAM dan profil bernama, kembali ke halaman ini dan lanjutkan ke langkah berikutnya. Anda akan melihat sepanjang sisa tutorial ini bahwa AWS CLI perintah sampel menggunakan `--profile` opsi dengan salah satu profil bernama untuk menunjukkan akun mana yang harus menjalankan perintah.

Langkah 2: Dapatkan ID ruang lingkup publik IPAM Anda

Ikuti langkah-langkah di bagian ini untuk mendapatkan ID ruang lingkup publik IPAM Anda. Langkah ini harus dilakukan oleh **`ipam-account`** akun.

Jalankan perintah berikut untuk mendapatkan ID lingkup publik Anda.

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

Dalam output, Anda akan melihat ID lingkup publik Anda. Perhatikan nilai untuk`PublicDefaultScopeId`. Anda akan membutuhkannya di langkah berikutnya.

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

Langkah 3: Buat kolam IPAM

Ikuti langkah-langkah di bagian ini untuk membuat kolam IPAM. Langkah ini harus dilakukan oleh **`ipam-account`** akun. Kolam IPAM yang Anda buat harus berupa kumpulan tingkat atas dengan `--locale` opsi yang cocok dengan Wilayah CIDR BYOIP. AWS Anda hanya dapat mentransfer BYOIP ke kolam IPAM tingkat atas.

> **Important**
>
> Saat Anda membuat kolam, Anda harus menyertakan`--aws-service ec2`. Layanan yang Anda pilih menentukan AWS layanan di mana CIDR akan dapat diiklankan. Saat ini, satu-satunya pilihan adalah`ec2`, yang berarti bahwa CIDR yang dialokasikan dari kumpulan ini akan dapat diiklankan untuk layanan Amazon EC2 (untuk alamat IP Elastis) dan layanan Amazon VPC (untuk CIDR yang terkait dengan VPC).

Untuk membuat kumpulan alamat IPv4 untuk CIDR BYOIP yang ditransfer menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat kolam IPAM. Gunakan ID lingkup publik IPAM yang Anda ambil pada langkah sebelumnya.

```
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
```

Dalam output, Anda akan melihat`create-in-progress`, yang menunjukkan bahwa pembuatan pool sedang berlangsung.

```
{
    "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. Jalankan perintah berikut sampai Anda melihat status `create-complete` dalam output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Contoh output berikut menunjukkan keadaan kolam. Anda akan membutuhkannya OwnerIddi langkah berikutnya.

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

Langkah 4: Bagikan kolam IPAM menggunakan AWS RAM

Ikuti langkah-langkah di bagian ini untuk berbagi kolam IPAM menggunakan AWS RAM sehingga AWS akun lain dapat mentransfer CIDR BYOIP IPV4 yang ada ke kolam IPAM dan menggunakan kolam IPAM. Langkah ini harus dilakukan oleh **`ipam-account`** akun.

Untuk berbagi kumpulan alamat IPv4 menggunakan AWS CLI

1. Lihat AWS RAM izin yang tersedia untuk kolam IPAM. Anda memerlukan kedua ARN untuk menyelesaikan langkah-langkah di bagian ini.

```
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. Buat berbagi sumber daya untuk mengaktifkan **byoip-owner-account** akun mengimpor BYOIP CIDR ke IPAM. Nilai untuk `--resource-arns` adalah ARN dari kolam IPAM yang Anda buat di bagian sebelumnya. Nilai untuk `--principals` adalah ID akun dari akun pemilik BYOIP CIDR. Nilai untuk `--permission-arns` adalah ARN izin. `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. (Opsional) Jika Anda ingin mengizinkan **`byoip-owner-account`** akun mengalokasikan CIDRS alamat IP dari kolam IPAM ke kolam IPv4 publik setelah transfer selesai, salin ARN untuk dan buat pembagian sumber daya kedua. `AWSRAMDefaultPermissionsIpamPool` Nilai untuk `--resource-arns` adalah ARN dari kolam IPAM yang Anda buat di bagian sebelumnya. Nilai untuk `--principals` adalah ID akun dari akun pemilik BYOIP CIDR. Nilai untuk `--permission-arns` adalah ARN izin. `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"

        }
```

```
}
```

Sebagai hasil dari membuat pembagian sumber daya dalam RAM, byoip-owner-account akun sekarang dapat memindahkan CIDR ke IPAM.

Langkah 5: Transfer CIDR BYOIP IPV4 yang ada ke IPAM

Ikuti langkah-langkah di bagian ini untuk mentransfer CIDR BYOIP IPV4 yang ada ke IPAM. Langkah ini harus dilakukan oleh **`byoip-owner-account`** akun.

> **Important**
>
> Setelah Anda membawa rentang alamat IPv4 AWS, Anda dapat menggunakan semua alamat IP dalam rentang tersebut, termasuk alamat pertama (alamat jaringan) dan alamat terakhir (alamat siaran).

Untuk mentransfer BYOIP CIDR ke IPAM, pemilik BYOIP CIDR harus memiliki izin ini dalam kebijakan IAM mereka:

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> Anda dapat menggunakan salah satu AWS Management Console atau AWS CLI untuk langkah ini.

AWS Management Console

Untuk mentransfer BYOIP CIDR ke kolam IPAM:

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/ sebagai **`byoip-owner-account`** akun.
2. Di panel navigasi, pilih Pools.
3. Pilih kolam tingkat atas yang dibuat dan dibagikan dalam tutorial ini.

4. Pilih Tindakan > Transfer BYOIP CIDR.
5. Pilih Transfer BYOIP CIDR.
6. Pilih CIDR BYOIP Anda.
7. Pilih Ketentuan.

Command line

Gunakan AWS CLI perintah berikut mentransfer CIDR BYOIP ke kolam IPAM menggunakan: AWS CLI

1. Jalankan perintah berikut untuk mentransfer CIDR. Pastikan `--region` nilainya adalah AWS Wilayah CIDR BYOIP.

```
aws ec2 move-byoip-cidr-to-ipam --region us-west-2 --profile byoip-owner-account
 --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --ipam-pool-owner 123456789012 --
cidr 130.137.249.0/24
```

   Dalam output, Anda akan melihat ketentuan CIDR yang tertunda.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "pending-transfer"

    }

}
```

2. Pastikan CIDR telah ditransfer. Jalankan perintah berikut sampai Anda melihat status `complete-transfer` dalam output.

```
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
```

   Contoh output berikut menunjukkan keadaan.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

Langkah 6: Lihat CIDR di IPAM

Ikuti langkah-langkah di bagian ini untuk melihat CIDR di IPAM. Langkah ini harus dilakukan oleh **`ipam-account`** akun.

Untuk melihat BYOIP CIDR yang ditransfer di kolam IPAM menggunakan AWS CLI

- Jalankan perintah berikut untuk melihat alokasi yang dikelola di IPAM. Pastikan `--region` nilainya adalah AWS Wilayah CIDR BYOIP.

  ```
  aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
  ipam-pool-id ipam-pool-0d8f3646b61ca5987
  ```

  Output menunjukkan alokasi di IPAM.

  ```
  {
      "IpamPoolAllocations": [
          {
              "Cidr": "130.137.249.0/24",
              "IpamPoolAllocationId": "ipam-pool-
  alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
              "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
              "ResourceType": "ec2-public-ipv4-pool",
              "ResourceOwner": "111122223333"
          }
      ]
  }
  ```

Langkah 7: Pembersihan

Ikuti langkah-langkah di bagian ini untuk menghapus sumber daya yang Anda buat dalam tutorial ini. Langkah ini harus dilakukan oleh **`ipam-account`** akun.

Untuk membersihkan sumber daya yang dibuat dalam tutorial ini menggunakan AWS CLI

1. Untuk menghapus sumber daya bersama kolam IPAM, jalankan perintah berikut untuk mendapatkan ARN berbagi sumber daya pertama:

```
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. Salin ARN berbagi sumber daya dan gunakan untuk menghapus berbagi sumber daya kolam 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. Jika Anda membuat pembagian sumber daya tambahanLangkah 4: Bagikan kolam IPAM menggunakan AWS RAM, ulangi dua langkah sebelumnya untuk mendapatkan ARN bagi sumber daya kedua `PoolShare2` dan hapus pembagian sumber daya kedua.

4. Jalankan perintah berikut untuk mendapatkan ID alokasi untuk CIDR BYOIP. Pastikan `--region` nilainya cocok dengan AWS Wilayah CIDR BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

   Output menunjukkan alokasi di 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. Lepaskan alamat IP terakhir di CIDR dari kolam IPv4 publik. Masukkan alamat IP dengan netmask /32. Anda harus menjalankan kembali perintah ini untuk setiap alamat IP dalam rentang CIDR. Jika CIDR Anda adalah a`/24`, Anda harus menjalankan perintah ini untuk menghentikan penyediaan masing-masing 256 alamat IP di CIDR. `/24` Ketika Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus cocok dengan Wilayah IPAM Anda.

   Langkah ini harus dilakukan oleh **`byoip-owner-account`** akun.

```
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
```

   Dalam output, Anda akan melihat CIDR yang telah di-deprovisioned.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
```

```
    "DeprovisionedAddresses": [

        "130.137.249.255"

    ]

}
```

6. Lihat CIDR BYOIP Anda lagi dan pastikan tidak ada lagi alamat yang disediakan. Ketika Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus cocok dengan Wilayah IPAM Anda.

   Langkah ini harus dilakukan oleh **`byoip-owner-account`** akun.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
```

   Dalam output, Anda akan melihat jumlah alamat IP di kolam IPv4 publik Anda.

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

7. Jalankan perintah berikut untuk menghapus kolam tingkat atas.

```
aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
id ipam-pool-0a03d430ca3f5c035
```

   Dalam output, Anda dapat melihat status hapus.

```
{
    "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: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet

Lengkapi tutorial ini untuk merencanakan ruang alamat IP VPC untuk mengalokasikan alamat IP ke subnet VPC dan memantau metrik terkait alamat IP di tingkat subnet dan VPC.

> **Note**
>
> Tutorial ini mencakup mengalokasikan ruang alamat IPv4 pribadi dalam lingkup IPAM pribadi untuk VPC dan subnet. Anda juga dapat menyelesaikan tutorial ini menggunakan ruang lingkup publik dan rentang IPv6 CIDR dengan membuat VPC dengan opsi blok IPv6 CIDR yang disediakan Amazon di konsol VPC.

Merencanakan ruang alamat IP VPC untuk subnet memungkinkan Anda melakukan hal berikut:

- Rencanakan dan atur alamat IP VPC Anda untuk alokasi ke subnet: Anda dapat membagi ruang alamat IP VPC menjadi blok CIDR yang lebih kecil dan menyediakan blok CIDR tersebut ke subnet dengan kebutuhan bisnis yang berbeda, seperti jika Anda menjalankan beban kerja dalam pengembangan atau produksi subnet.

- Sederhanakan alokasi alamat IP untuk subnet VPC: Setelah ruang alamat VPC Anda direncanakan dan diatur, Anda dapat memilih panjang netmask daripada memasukkan CIDR secara manual. Misalnya, jika pengembang membuat subnet untuk beban kerja pengembangan hosting, mereka harus memilih kumpulan dan panjang netmask untuk subnet dan IPAM akan secara otomatis mengalokasikan blok CIDR ke subnet Anda.

Contoh berikut menunjukkan hierarki struktur kolam dan sumber daya yang akan Anda buat dengan tutorial ini:

- Ruang lingkup pribadi
  - Kumpulan perencanaan sumber daya (10.0.0.0/20)
    - Kolam subnet Dev (10.0.0.0/24)
      - Subnet Dev (10.0.0.0/28)
    - Kolam subnet prod (10.0.0.1/24)
      - Subnet produk (10.0.0.16/28)

⚠ Important

- Kolam perencanaan sumber daya dapat digunakan untuk mengalokasikan CIDR ke subnet atau dapat digunakan sebagai kolam sumber di mana Anda dapat membuat kolam lainnya. Dalam tutorial ini, kita menggunakan resource planning pool sebagai source pool untuk subnet pool.
- Anda dapat membuat beberapa kumpulan perencanaan sumber daya menggunakan VPC yang sama jika VPC memiliki lebih dari satu CIDR yang disediakan untuknya; jika VPC memiliki dua CIDR yang ditetapkan padanya, misalnya, Anda dapat membuat dua kumpulan perencanaan sumber daya, satu dari setiap CIDR. Setiap CIDR dapat ditugaskan ke satu pool pada satu waktu.

Langkah 1: Buat VPC

Selesaikan langkah-langkah di bagian ini untuk membuat VPC yang akan digunakan untuk perencanaan alamat IP subnet. Untuk informasi selengkapnya tentang izin IAM yang diperlukan untuk membuat VPC, lihat contoh kebijakan Amazon VPC di Panduan Pengguna Amazon VPC.

> **Note**
>
> Anda dapat menggunakan VPC yang sudah ada daripada membuat yang baru, tetapi tutorial ini berfokus pada skenario di mana VPC dikonfigurasi dengan blok CIDR yang dialokasikan secara manual, bukan blok CIDR otomatis yang dialokasikan IPAM.

Untuk membuat VPC

1. Menggunakan akun admin IPAM, buka konsol VPC di https://console.aws.amazon.com/vpc/.
2. Pilih Buat VPC.
3. Masukkan nama untuk VPC, seperti tutorial-vpc.
4. Pilih input manual IPv4 CIDR dan masukkan blok CIDR IPv4. Dalam tutorial ini, kami menggunakan 10.0.0.0/20.
5. Lewati opsi untuk menambahkan blok CIDR IPv6.
6. Pilih Buat VPC.
7. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
8. Pilih Sumber Daya di panel navigasi kiri.
9. Tunggu hingga VPC yang Anda buat muncul. Ini membutuhkan waktu untuk terjadi dan Anda mungkin perlu menyegarkan jendela untuk melihatnya muncul. VPC harus ditemukan oleh IPAM sebelum Anda melanjutkan ke langkah berikutnya.

Langkah 2: Buat kolam perencanaan sumber daya

Selesaikan langkah-langkah di bagian ini untuk membuat kumpulan perencanaan sumber daya.

Untuk membuat kolam perencanaan sumber daya

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi.
4. Pilih Buat kolam.
5. Di bawah lingkup IPAM, biarkan ruang lingkup pribadi dipilih.
6. (Opsional) Tambahkan tag Nama untuk kumpulan, seperti “Resource-planning-pool”.

7. Di bawah Sumber, pilih cakupan IPAM.
8. Di bawah Perencanaan sumber daya, pilih Rencanakan ruang IP dalam VPC dan pilih VPC yang Anda buat di langkah sebelumnya. VPC adalah sumber daya yang digunakan untuk menyediakan CIDR ke kumpulan perencanaan sumber daya.
9. Di bawah CIDR untuk penyediaan, pilih CIDR VPC untuk disediakan untuk kumpulan sumber daya. CIDR yang Anda berikan ke kumpulan perencanaan sumber daya harus sesuai dengan CIDR yang disediakan ke VPC. Dalam tutorial ini, kami menggunakan 10.0.0.0/20.
10. Pilih Buat kolam.
11. Setelah pool dibuat, pilih tab CIDR untuk melihat status CIDR yang disediakan. Segarkan halaman dan tunggu status CIDR berubah dari Pending-provisioned ke Provisioned sebelum Anda melanjutkan ke langkah berikutnya.

Langkah 3: Buat subnet pool

Selesaikan langkah-langkah di bagian ini untuk membuat dua subnet pool yang akan digunakan untuk mengalokasikan ruang IP ke subnet.

Untuk membuat subnet pool

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi.
4. Pilih Buat kolam.
5. Di bawah lingkup IPAM, biarkan ruang lingkup pribadi dipilih.
6. (Opsional) Tambahkan tag Nama untuk kumpulan, seperti “dev-subnet-pool”.
7. Di bawah Sumber, pilih kolam IPAM dan pilih kumpulan perencanaan sumber daya yang Anda buat di Langkah 3. Keluarga alamat, konfigurasi perencanaan sumber daya, dan Lokal secara otomatis diwarisi dari kumpulan sumber.
8. Di bawah CIDR untuk penyediaan, pilih CIDR untuk menyediakan subnet pool. Dalam tutorial ini, kami menggunakan 10.0.0.0/24.
9. Pilih Buat kolam.
10. Setelah pool dibuat, pilih tab CIDR untuk melihat status CIDR yang disediakan. Segarkan halaman dan tunggu status CIDR berubah dari Pending-provisioned ke Provisioned sebelum Anda melanjutkan ke langkah berikutnya.

11. Ulangi proses ini untuk membuat subnet lain yang disebut “prod-subnet-pool”.

Pada titik ini, jika Anda ingin membuat subnet pool ini tersedia untuk AWS akun lain, Anda dapat berbagi subnet pool. Untuk petunjuk tentang cara melakukannya, lihatMembagikan kumpulan IPAM menggunakanAWS RAM. Kemudian kembali ke sini untuk menyelesaikan tutorial.

Langkah 4: Buat subnet

Selesaikan langkah-langkah ini untuk membuat dua subnet.

Untuk membuat subnet

1. Menggunakan akun yang sesuai, buka konsol VPC di https://console.aws.amazon.com/vpc/.
2. Pilih Subnet > Buat subnet.
3. Pilih VPC yang Anda buat di awal tutorial ini.
4. Masukkan nama untuk subnet, seperti “tutorial-subnet”.
5. (opsional) Pilih Availability Zone.
6. Di bawah blok IPv4 CIDR, pilih blok IPV4 CIDR yang dialokasikan IPAM dan pilih kumpulan subnet dev dan netmask /28.
7. Pilih Buat subnet.
8. Ulangi proses ini untuk membuat subnet lain. Kali ini pilih subnet pool prod dan netmask /28.
9. Kembali ke konsol IPAM dan pilih Resources di panel navigasi kiri.
10. Cari subnet pool yang Anda buat dan tunggu subnet yang Anda buat muncul di bawahnya. Ini membutuhkan waktu untuk terjadi dan Anda mungkin perlu menyegarkan jendela untuk melihatnya muncul.

Tutorialnya selesai. Anda dapat membuat subnet pool tambahan sesuai kebutuhan atau Anda dapat meluncurkan instans EC2 ke salah satu subnet.

IPAM menerbitkan metrik yang terkait dengan penggunaan alamat IP di subnet. Anda dapat menyetel CloudWatch alarm pada metrik SubnetIpuSage, sehingga memungkinkan Anda untuk mengambil tindakan ketika ambang batas pemanfaatan IP dilanggar. Jika, misalnya, Anda memiliki /24 CIDR (256 alamat IP) yang ditetapkan ke subnet dan Anda ingin diberi tahu ketika 80% IP telah digunakan, Anda dapat mengatur CloudWatch alarm untuk mengingatkan Anda ketika ambang batas ini tercapai. Untuk informasi selengkapnya tentang membuat alarm untuk penggunaan subnet IP, lihatKiat cepat untuk membuat alarm.

Langkah 5: Pembersihan

Selesaikan langkah-langkah ini untuk menghapus sumber daya yang Anda buat dengan tutorial ini.

Untuk membersihkan sumber daya

1. Menggunakan akun admin IPAM, buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi.
4. Pilih kumpulan perencanaan sumber daya dan pilih Tindakan > Hapus.
5. Pilih Cascade delete. Pool perencanaan sumber daya dan subnet pool akan dihapus. Ini tidak akan menghapus subnet itu sendiri. Mereka akan tetap dengan CIDR yang disediakan untuk mereka, meskipun CIDR tidak lagi berasal dari kolam IPAM.
6. Pilih Hapus.
7. Hapus subnet.
8. Hapus VPC.

Pembersihan selesai.

Identity and access management di IPAM

AWS menggunakan kredensial keamanan untuk mengidentifikasi dan memberi Anda akses menuju AWS sumber daya Anda. Anda dapat menggunakan fitur (IAM) AWS Identity and Access Management untuk mengizinkan pengguna, layanan, dan aplikasi lain untuk menggunakan sumber daya AWS sepenuhnya atau dengan cara yang terbatas, tanpa berbagi kredensial keamanan Anda.

Bagian ini menjelaskan peran AWS terkait layanan yang dibuat khusus untuk IPAM dan kebijakan terkelola yang melekat pada peran terkait layanan IPAM. Untuk informasi selengkapnya tentang peran dan kebijakan AWS IAM, lihat Istilah dan konsep peran dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang manajemen identitas dan akses untuk VPC, lihat Manajemen Identitas dan akses untuk Amazon VPC di Panduan Pengguna Amazon VPC.

Konten

- Peran tertaut layanan untuk IPAM
- AWSkebijakan terkelola untuk IPAM
- Contoh kebijakan

Peran tertaut layanan untuk IPAM

Peran terkait layanan diAWS Identity and Access Management (IAM) memungkinkanAWS layanan untuk memanggilAWS layanan lain atas nama Anda. Untuk informasi selengkapnya tentang peran tertaut layanan, lihat Menggunakan peran tertaut layanan dalam Panduan Pengguna IAM.

Saat ini hanya ada satu peran terkait layanan untuk IPAM: AWSServiceRoleForIPAM.

Izin yang diberikan kepada peran yang ditautkan dengan layanan

IPAM menggunakan peran AWSServiceRoleForIPAMterkait layanan untuk memanggil tindakan dalam kebijakan AWSIPAMServiceRolePolicyterkelola terlampir. Untuk informasi lebih lanjut tentang tindakan yang diizinkan dalam kebijakan itu, lihatAWSkebijakan terkelola untuk IPAM.

Juga melekat pada peran terkait layanan adalah kebijakan tepercaya IAM yang memungkinkan`ipam.amazonaws.com` layanan untuk mengambil peran terkait layanan.

Membuat peran tertaut layanan

IPAM memantau penggunaan alamat IP dalam satu atau lebih akun dengan mengasumsikan peran terkait layanan dalam akun, menemukan sumber daya dan CIDR mereka, dan mengintegrasikan sumber daya dengan IPAM.

Peran yang tertaut dengan layanan dibuat dengan salah satu dari dua cara yang terhubung dengan layanan ini:

- Saat Anda berintegrasi denganAWS Organizations

  Jika AndaIntegrasikan IPAM dengan akun di Organisasi AWS menggunakan konsol IPAM atau menggunakan`enable-ipam-organization-admin-account`AWS CLI perintah, peran AWSServiceRoleForIPAMterkait layanan secara otomatis dibuat di setiap akun anggotaAWS Organizations Anda. Akibatnya, sumber daya dalam semua akun anggota dapat ditemukan oleh IPAM.

  > **Important**
  >
  > Untuk IPAM untuk membuat peran tertaut layanan atas nama Anda:
  >
  > - Akun manajemenAWS Organizations yang memungkinkan integrasi IPAM denganAWS Organizations harus memiliki kebijakan IAM yang melekat padanya yang memungkinkan tindakan berikut:
  >   - `ec2:EnableIpamOrganizationAdminAccount`
  >   - `organizations:EnableAwsServiceAccess`
  >   - `organizations:RegisterDelegatedAdministrator`
  >   - `iam:CreateServiceLinkedRole`
  > - Akun IPAM harus memiliki kebijakan IAM yang memungkinkan tindakan tertaut`iam:CreateServiceLinkedRole` tindakan tersebut.

- Saat Anda membuat IPAM menggunakan satuAWS akun

  Jika AndaGunakan IPAM dengan satu akun, peran AWSServiceRoleForIPAMtertaut layanan secara otomatis dibuat saat Anda membuat IPAM sebagai akun tersebut.

> **Important**
>
> Jika Anda menggunakan IPAM dengan satuAWS akun, sebelum membuat IPAM, Anda harus memastikan bahwaAWS akun yang Anda gunakan memiliki kebijakan IAM yang melekat padanya yang memungkinkan`iam:CreateServiceLinkedRole` tindakan tersebut. Saat Anda membuat IPAM, Anda secara otomatis membuat peran AWSServiceRoleForIPAMterkait layanan. Untuk informasi selengkapnya tentang mengelola kebijakan IAM, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

Mengedit peran tertaut layanan

Anda tidak dapat mengedit peran yang terhubung dengan layanan AWSServiceRoleForIPAM.

Hapus peran tertaut layanan

Jika Anda tidak perlu lagi menggunakan IPAM, kami sarankan agar Anda menghapus peran AWSServiceRoleForIPAMtertaut layanan.

> **Note**
>
> Anda dapat menghapus peran tertaut layanan hanya setelah Anda menghapus semua sumber daya IPAM dalamAWS akun Anda. Hal ini memastikan bahwa Anda tidak dapat secara tidak sengaja menghapus kemampuan pemantauan IPAM.

Ikuti langkah-langkah berikut untuk menghapus peran terkait layanan melaluiAWS CLI:

1. Hapus sumber daya IPAM Anda menggunakan deprovision-ipam-pool-cidrdan menghapus-ipam. Untuk informasi selengkapnya, lihat Deprovision CIDR dari kolam dan Menghapus IPAM.
2. Nonaktifkan akun IPAM dengan disable-ipam-organization-admin-account.
3. Nonaktifkan layanan IPAM dengan disable-aws-service-accessmenggunakan`--service-principal ipam.amazonaws.com` opsi.
4. Hapus peran yang ditautkan dengan layanan delete-service-linked-role. Saat Anda menghapus peran tertaut layanan, kebijakan tertaut layanan, kebijakan tertaut layanan juga dihapus. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

AWSkebijakan terkelola untuk IPAM

Jika Anda menggunakan IPAM dengan satu AWS akun dan Anda membuat IPAM, kebijakan AWSIPAMServiceRolePolicyterkelola secara otomatis dibuat di akun IAM Anda dan dilampirkan ke peran terkait layanan. AWSServiceRoleForIPAM

Jika Anda mengaktifkan integrasi IPAM dengan AWS Organizations, kebijakan AWSIPAMServiceRolePolicyterkelola akan dibuat secara otomatis di akun IAM Anda dan di setiap akun anggota AWS Organizations Anda, dan kebijakan terkelola dilampirkan ke peran terkait AWSServiceRoleForIPAMlayanan.

Kebijakan terkelola ini memungkinkan IPAM melakukan hal berikut:

- Pantau CIDR yang terkait dengan sumber daya jaringan di semua anggota Organisasi AndaAWS.
- Simpan metrik yang terkait dengan IPAM di Amazon CloudWatch, seperti ruang alamat IP yang tersedia di kolam IPAM Anda dan jumlah CIDR sumber daya yang mematuhi aturan alokasi.

Contoh berikut menunjukkan detail kebijakan terkelola yang dibuat.

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

Pernyataan pertama dalam contoh sebelumnya memungkinkan IPAM untuk memantau CIDR yang digunakan oleh AWS akun tunggal Anda atau oleh anggota Organisasi Anda. AWS

Pernyataan kedua dalam contoh sebelumnya menggunakan kunci `cloudwatch:PutMetricData` kondisi untuk memungkinkan IPAM menyimpan metrik IPAM di namespace Amazon Anda. `AWS/IPAM` CloudWatch Metrik ini digunakan oleh AWS Management Console untuk menampilkan data tentang alokasi di pool dan cakupan IPAM Anda. Untuk informasi selengkapnya, lihat Memantau penggunaan CIDR dengan dasbor IPAM.

Pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk IPAM sejak layanan ini mulai melacak perubahan ini.

Perubahan	Deskripsi	Tanggal
AWSIPAMServiceRolePolicy	Tindakan ditambahkan ke kebijakan AWSIPAMSe rviceRolePolicy terkelola	November 13, 2023

Perubahan	Deskripsi	Tanggal
	(`ec2:GetIpamDiscoveredPublicAddresses`) untuk mengaktifkan IPAM mendapatkan alamat IP publik selama penemuan sumber daya.	
AWSIPAMServiceRolePolicy	Tindakan ditambahkan ke kebijakan AWSIPAMServiceRolePolicy terkelola (`ec2:DescribeAccountAttributes`, `ec2:DescribeNetworkInterfaces`, `ec2:DescribeSecurityGroups`, `ec2:DescribeSecurityGroupRules`, `ec2:DescribeVpnConnections`, `globalaccelerator:ListAccelerators`, dan `globalaccelerator:ListByoipCidrs`) untuk memungkinkan IPAM mendapatkan alamat IP publik selama penemuan sumber daya.	November 1, 2023

Perubahan	Deskripsi	Tanggal
AWSIPAMServiceRolePolicy	Dua tindakan ditambahkan ke kebijakan AWSIPAMServiceRolePolicy terkelola (`ec2:GetIpamDiscoveredAccounts` dan `ec2:GetIpamDiscoveredResourceCidrs`) untuk mengaktifkan IPAM agar AWS akun dan CIDR sumber daya dipantau selama penemuan sumber daya.	Januari 25, 2023
IPAM mulai melacak perubahan	IPAM mulai melacak perubahan untuk kebijakan yang AWS dikelola.	Desember 2, 2021

Contoh kebijakan

Contoh kebijakan di bagian ini berisi semua tindakan AWS Identity and Access Management (IAM) yang relevan untuk penggunaan IPAM penuh. Tergantung pada bagaimana Anda menggunakan IPAM, Anda mungkin tidak perlu menyertakan semua tindakan IAM. Untuk pengalaman penuh menggunakan konsol IPAM, Anda mungkin perlu menyertakan tindakan IAM tambahan untuk layanan seperti AWS Organizations, AWS Resource Access Manager (RAM), dan. 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"
                }
```

```
            }
        }
    ]
}
```

Kuota untuk IPAM Anda

Bagian ini mencantumkan kuota yang terkait dengan IPAM. Konsol Service Quotas juga menyediakan informasi tentang kuota IPAM. Anda dapat menggunakan konsol Service Quotas untuk melihat kuota default dan meminta peningkatan kuota untuk kuota yang dapat disesuaikan. Untuk informasi lebih lanjut, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Nama	Default	Dapat Disesuaikan
IPv6 CIDR yang disediakan Amazon panjang blok netmask	/52	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
Blok CIDR IPv6 yang disediakan Amazon per kolam Regional	1	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
Autonomous System Numbers (ASN) yang dapat Anda bawa ke IPAM	5	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
CIDR per kolam	50	Ya
Administrator IPAM per organisasi	1	Tidak
IPAM per Wilayah	1	Tidak

Nama	Default	Dapat Disesuaikan
Kedalaman kolam (jumlah kolam di dalam kolam)	10	Ya
Kolam per lingkup	50	Ya
Asosiasi penemuan sumber daya per IPAM	5	Ya
Penemuan sumber daya per Wilayah	1	Tidak
Metrik pemanfaatan sumber daya	50	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
Cakupan per IPAM	5	/Ya. Saat Anda membuat IPAM, cakupan default pribadi dan publik dibuat untuk Anda. Jika Anda ingin membuat cakupan tambahan, itu akan menjadi cakupan pribadi. Anda tidak dapat membuat cakupan publik tambahan.

Harga untuk IPAM

Bagian ini menjelaskan cara melihat informasi terkait harga dan biaya IPAM Anda saat ini.

Lihat informasi harga

IPAM ditawarkan dalam dua tingkatan: Tingkat Gratis dan Tingkat Lanjut. Untuk informasi selengkapnya tentang fitur yang tersedia di setiap tingkatan dan biaya yang terkait dengan tingkatan, lihat tab IPAM di halaman harga Amazon VPC.

Lihat biaya dan penggunaan Anda saat ini AWS Cost Explorer

Saat Anda menggunakan Tingkat Lanjut IPAM, Anda membayar harga per jam per alamat IP aktif yang dikelola oleh IPAM. Jika Anda ingin melihat dan menganalisis biaya dan penggunaan IPAM Anda, Anda dapat menggunakan. AWS Cost Explorer

1. Buka AWS Cost Management konsol di https://console.aws.amazon.com/cost-management/home.
2. Pilih Cost Explorer.
3. Filter untuk penggunaan IPAM dengan memilih jenis Penggunaan dan memasukkan**`IPAddressManager`**.
4. Pilih satu atau beberapa kotak centang. Masing-masing mewakili AWS Wilayah yang berbeda.
5. Klik Terapkan.

Jika, misalnya, Anda memilih USE1-IP AddressManager -IP-Hours (Jam) dan us-east-1 adalah Wilayah rumah IPAM Anda, Anda akan melihat jumlah jam IP aktif yang ditagih oleh IPAM di semua Wilayah dan biayanya. Jika, katakanlah, penggunaan dalam jam adalah 18, ini berarti bahwa Anda dapat memiliki 1 alamat IP aktif selama 18 jam, 3 alamat IP di 3 Wilayah berbeda masing-masing aktif selama 6 jam, atau kombinasi dari ini yang menambahkan hingga 18 jam.

Untuk informasi selengkapnya AWS Cost Explorer, lihat Menganalisis biaya Anda dengan AWS Cost Explorer di Panduan AWS Cost Management Pengguna.

Informasi terkait

Sumber daya terkait berikut dapat membantu Anda ketika bekerja dengan layanan ini.

- Praktik Terbaik Manajer Alamat IP Amazon VPC: SebuahAWSblog tentang praktik terbaik untuk merencanakan dan membuat skema alamat yang dapat diskalakan dengan Amazon VPC IP Address Manager.
- Manajemen Alamat Jaringan dan Audit dalam Skala Besar dengan Amazon VPC IP Address Manager: SebuahAWSblog yang memperkenalkan Amazon VPC IP Address Manager dan menunjukkan cara menggunakan layanan diAWSkonsol.
- Konfigurasikan akses berbutir halus ke sumber daya Anda yang dibagikan menggunakanAWS Resource Access Manager: SebuahAWSblog yang menjelaskan cara berbagi kolam IPAM dengan akun diAWSUnit organisasi organisasi.

Riwayat dokumen untuk IPAM

Tabel berikut menjelaskan rilis untuk IPAM.

Fitur	Deskripsi	Tanggal Rilis
IPAM Tingkatan Gratis dan Tingkat Lanjut	Anda sekarang dapat memilih antara Tingkat Gratis dan Tingkat Lanjut untuk IPAM Anda.	November 17, 2023
Wawasan IP publik	Sebelumnya, Anda hanya dapat melihat wawasan IP publik di satu Wilayah. Anda sekarang dapat melihat wawasan IP publik di seluruh Wilayah. Selain itu, Anda sekarang dapat melihat wawasan alamat IP publik di Amazon CloudWatch.	November 17, 2023
Rencanakan ruang alamat IP VPC untuk alokasi IP subnet	Anda sekarang dapat menggunakan IPAM untuk merencanakan ruang IP subnet dalam VPC dan memantau metrik terkait alamat IP di tingkat subnet dan VPC.	November 17, 2023
Bawa ASN Anda sendiri (BYOASN)	Anda sekarang dapat membawa nomor sistem otonom Anda sendiri (ASN) keAWS.	November 17, 2023
AWSpembaruan kebijakan terkelola - Pembaruan ke kebijakan yang ada	Ada AWSIPAMServiceRolePolicy diperbarui.	November 17, 2023
AWSpembaruan kebijakan terkelola - Pembaruan ke kebijakan yang ada	Ada AWSIPAMServiceRolePolicy diperbarui.	November 1, 2023

Fitur	Deskripsi	Tanggal Rilis
Metrik pemanfaatan sumber daya	IPAM sekarang menerbitkan metrik pemanfaatan IP untuk sumber daya yang dipantau IPAM ke Amazon. CloudWatch	Agustus 2, 2023
Wawasan IP publik	Wawasan IP publik menunjukkan kepada Anda semua alamat IPv4 publik yang digunakan oleh layanan di Wilayah ini di akun Anda. Anda dapat menggunakan wawasan ini untuk mengidentifikasi penggunaan alamat IPv4 publik dan melihat rekomendasi untuk merilis alamat IP Elastis yang tidak digunakan.	Juli 28, 2023
AWSpembaruan kebijakan terkelola - Pembaruan ke kebijakan yang ada	Ada AWSIPAMServiceRolePolicy diperbarui.	Januari 25, 2023
Integrasikan IPAM dengan akun di luar organisasi	Anda sekarang dapat mengelola alamat IP di luar organisasi Anda dari satu akun IPAM dan berbagi kumpulan IPAM dengan akun Organizations AWS lain.	Januari 25, 2023
Blok CIDR bersebelahan IPv6 yang disediakan Amazon untuk kolam IPAM	Saat Anda membuat kolam IPAM di ruang lingkup publik, Anda sekarang dapat menyediakan blok CIDR bersebelahan IPv6 yang disediakan Amazon ke kolam. Untuk informasi selengkapnya, lihat Buat kolam IPv6.	Januari 25, 2023
Rilis pertama	Rilis ini memperkenalkan Amazon VPC IP Address Manager.	Desember 2, 2021

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.