Manajer Alamat IP

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: Manajer Alamat IP

Table of Contents

Apa itu IPAM?

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

Anda dapat menggunakan IPAM untuk melakukan hal berikut:

- Mengatur ruang alamat IP ke dalam domain routing dan keamanan
- Memantau ruang alamat IP yang sedang digunakan dan memantau sumber daya yang menggunakan ruang terhadap aturan bisnis
- Melihat riwayat penetapan alamat IP di organisasi Anda
- Alokasikan secara otomatis CIDRs untuk VPCs menggunakan aturan bisnis tertentu
- Memecahkan masalah konektivitas jaringan
- Aktifkan berbagi lintas wilayah dan lintas akun dari alamat Bring Your Own IP (BYOIP) Anda
- Menyediakan IPv6 blok CIDR bersebelahan yang disediakan Amazon ke kumpulan untuk pembuatan VPC

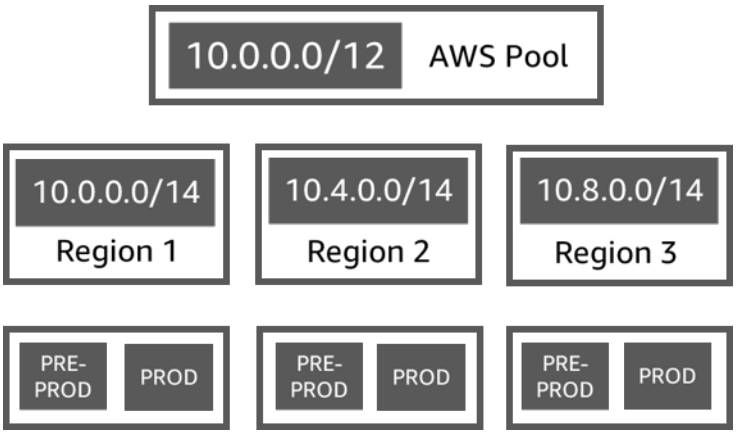
Panduan ini terdiri dari bagian-bagian berikut:

- Bagaimana IPAM bekerja: Konsep dan terminologi IPAM.
- Memulai dengan IPAM: Langkah-langkah untuk mengaktifkan manajemen alamat IP di seluruh perusahaan dengan AWS Organizations, membuat IPAM, dan merencanakan penggunaan alamat IP.
- Mengelola ruang alamat IP di IPAM: Langkah-langkah untuk mengelola IPAM, cakupan, kumpulan, 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 CIDRs VPC, dan membawa alamat IP publik Anda sendiri ke IPAM. CIDRs

Bagaimana IPAM bekerja

Topik ini menjelaskan beberapa konsep kunci untuk membantu Anda memulai dengan IPAM.

Diagram berikut menunjukkan hierarki kolam IPAM untuk beberapa AWS Wilayah dalam kolam IPAM tingkat atas. Setiap kolam AWS Regional memiliki dua kolam pengembangan IPAM di dalamnya, satu kolam untuk pra-produksi dan satu sumber daya produksi kolam. Untuk informasi lebih lanjut 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 memilih AWS Wilayah mana yang akan dibuat. Saat Anda membuat IPAM, AWS VPC IPAM secara otomatis membuat dua cakupan untuk IPAM. Cakupan, bersama dengan kumpulan dan alokasi, adalah komponen kunci dari IPAM Anda.

- Lingkup adalah wadah tingkat tertinggi dalam IPAM. Saat Anda membuat IPAM, cakupan publik default dan cakupan pribadi default dibuat secara otomatis untuk Anda. Setiap ruang lingkup mewakili ruang IP untuk satu jaringan. Ruang lingkup pribadi ditujukan untuk semua alamat IP yang tidak dapat diiklankan ke internet. Ruang lingkup publik umumnya ditujukan untuk semua alamat IP yang dapat diiklankan ke internet dari AWS. Perhatikan bahwa saat menyediakan BYOIPv6 alamat ke kolam IPAM, Anda dapat mengonfigurasi alamat agar tidak dapat diiklankan secara publik meskipun berada dalam lingkup publik. Cakupan memungkinkan Anda untuk menggunakan kembali alamat IP di beberapa jaringan yang tidak terhubung tanpa menyebabkan alamat IP tumpang tindih atau konflik. Dalam lingkup, Anda membuat kolam IPAM.
- Pool adalah kumpulan rentang alamat IP yang berdekatan (atau). CIDRs Kolam IPAM memungkinkan Anda untuk mengatur alamat IP Anda sesuai dengan kebutuhan routing dan keamanan Anda. Anda dapat memiliki beberapa kolam 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 aplikasi. Dalam kolam IPAM, Anda mengalokasikan CIDRs ke AWS sumber daya.

- Alokasi adalah tugas CIDR dari kolam IPAM ke sumber daya lain atau kolam IPAM. Saat Anda membuat VPC dan memilih kolam 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 IPv6 ruang publik dan pribadi. Untuk informasi selengkapnya tentang IPv6 alamat publik dan pribadi, lihat IPv6 alamat di Panduan Pengguna Amazon VPC.

Untuk memulai dan membuat IPAM, lihatMemulai dengan IPAM.

Memulai dengan IPAM

Ikuti langkah-langkah di bagian ini untuk memulai dengan IPAM. Bagian ini dimaksudkan untuk membantu Anda memulai dengan cepat dengan IPAM, tetapi Anda mungkin menemukan bahwa apa yang dapat Anda capai dengan langkah-langkah di bagian ini tidak sesuai dengan kebutuhan Anda. Untuk informasi tentang berbagai cara Anda dapat menggunakan IPAM, lihat Merencanakan penyediaan alamat IP danTutorial untuk Manajer Alamat IP VPC Amazon.

Di bagian ini, 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.

Tugas

- Akses IPAM
- Konfigurasikan opsi integrasi untuk IPAM Anda
- Buat IPAM
- Merencanakan penyediaan alamat IP
- Alokasikan CIDRs dari kolam IPAM

Akses IPAM

Seperti AWS layanan lainnya, Anda dapat membuat, mengakses, dan mengelola IPAM Anda menggunakan metode berikut:

- AWS Management Console: Menyediakan antarmuka web yang dapat Anda gunakan untuk membuat dan mengelola IPAM Anda. Lihat https://console.aws.amazon.com/ipam/.
- AWS Command Line Interface (AWS CLI): Menyediakan perintah untuk serangkaian AWS layanan yang luas, termasuk Amazon VPC. AWS CLI Ini didukung di Windows, macOS, dan Linux. Untuk mendapatkan AWS CLI, lihat AWS Command Line Interface.
- AWS SDKs: Menyediakan bahasa khusus APIs. AWS SDKsMengurus banyak detail koneksi, seperti menghitung tanda tangan, menangani percobaan ulang permintaan, dan menangani kesalahan. Untuk informasi selengkapnya, lihat AWS SDKs.
- Query API: Menyediakan tindakan API tingkat rendah yang Anda panggil menggunakan permintaan HTTPS. Menggunakan Query API adalah cara paling langsung untuk mengakses IPAM. Namun, aplikasi Anda harus menangani detail tingkat rendah seperti membuat hash untuk

menandatangani permintaan, dan menangani kesalahan. Untuk informasi selengkapnya, lihat tindakan Amazon IPAM di Referensi Amazon EC2 API.

Panduan ini terutama berfokus pada penggunaan Konsol AWS Manajemen untuk membuat, mengakses, dan mengelola IPAM Anda. Dalam setiap deskripsi tentang cara menyelesaikan proses di konsol, kami menyertakan tautan ke Referensi AWS CLI Perintah sehingga Anda dapat melakukan tugas yang sama dengan menggunakan AWS CLI.

Jika Anda adalah pengguna pertama kali IPAM, tinjau Bagaimana IPAM bekerja untuk mempelajari tentang peran IPAM di Amazon VPC dan kemudian lanjutkan dengan instruksi di. Konfigurasikan opsi integrasi untuk IPAM Anda

Konfigurasikan opsi integrasi untuk IPAM Anda

Bagian ini menjelaskan opsi Anda tentang cara mengintegrasikan IPAM dengan AWS Organizations, AWS akun lain, atau menggunakannya dengan satu AWS akun.

Sebelum Anda mulai menggunakan IPAM, Anda harus memilih salah satu opsi di bagian ini untuk mengaktifkan IPAM untuk memantau CIDRs terkait dengan sumber daya EC2 jaringan 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 mengintegrasikan dengan AWS Organizations, untuk mengintegrasikan IPAM dengan akun di luar organisasi Anda, lihatIntegrasikan IPAM dengan akun di luar organisasi Anda.
- 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

- 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 CIDRs dari kumpulan IPAM yang dibagikan menggunakan Resource Access Manager AWS (RAM). 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 CIDRs yang digunakan oleh yang ada VPCs 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.

> **Note**
>
> Saat berintegrasi dengan AWS Organizations:
>
> - 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.

- Akun IPAM harus berupa akun anggota AWS Organizations. Anda tidak dapat menggunakan akun manajemen AWS Organizations sebagai akun IPAM. Untuk memeriksa apakah IPAM Anda sudah terintegrasi dengan AWS Organizations, gunakan langkah-langkah di bawah ini dan lihat detail integrasi dalam pengaturan Organisasi.
- 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 menggunakan peran IAM yang memiliki kebijakan IAM yang melekat padanya yang memungkinkan tindakan tersebut. `iam:CreateServiceLinkedRole` Saat Anda membuat IPAM, Anda secara otomatis membuat peran terkait layanan AWSService RoleFor IPAM.
- Pengguna yang terkait dengan akun manajemen AWS Organizations harus menggunakan peran IAM yang memiliki tindakan kebijakan IAM berikut dilampirkan:
  - `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 Referensi AWS CLI Perintah. 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 mereka CIDRs, 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 Anda

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

Mengintegrasikan IPAM dengan AWS akun di luar organisasi memungkinkan Anda melakukan hal berikut:

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

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

Daftar Isi

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 dan. GetIpamDiscoveredResourceCidrsGetIpamDiscoveredAccounts APIs 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 adalah AWS akun layanan pihak ketiga yang membuat sumber daya untuk beberapa pelanggan mereka sendiri, sumber daya tersebut akan ditemukan oleh penemuan sumber daya. Jika akun AWS layanan pihak ketiga berbagi penemuan sumber daya dengan AWS akun pengguna akhir, pengguna akhir akan memiliki visibilitas ke

sumber daya pelanggan lain dari layanan pihak ketiga. AWS Untuk alasan itu, AWS layanan pihak ketiga harus berhati-hati dalam membuat dan berbagi penemuan sumber daya atau menggunakan AWS akun terpisah untuk setiap pelanggan.

Gambaran umum proses

Bagian ini menjelaskan cara mengintegrasikan IPAM Anda dengan AWS 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.

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

- Pemilik Org Utama - Akun AWS Organizations manajemen untuk organisasi 1.
- Akun IPAM Org Utama - Akun administrator yang didelegasikan IPAM untuk organisasi 1.
- Pemilik Org Sekunder - Akun AWS 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 Utama (lihatIntegrasikan IPAM dengan akun di Organisasi AWS).
2. Akun IPAM Org Utama 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 Utama menggunakan AWS RAM (lihat Buat penemuan sumber daya untuk diintegrasikan dengan IPAM lain danBagikan penemuan sumber daya dengan AWS akun lain). Penemuan sumber daya harus dibuat di Wilayah asal yang sama dengan IPAM Org Utama.
5. Akun IPAM Org Utama menerima undangan berbagi sumber daya menggunakan AWS RAM (lihat Menerima dan menolak undangan berbagi sumber daya di Panduan Pengguna).AWS RAM
6. Akun IPAM Org Utama mengaitkan penemuan sumber daya dengan IPAM mereka (lihat). Mengaitkan penemuan sumber daya dengan IPAM

7. Akun IPAM Org Utama sekarang dapat memantau and/or pengelolaan sumber daya IPAM yang dibuat oleh akun di Org Sekunder.
8. (Opsional) Akun IPAM Org Utama membagikan kumpulan IPAM dengan akun anggota di Org Sekunder (lihatBagikan kolam IPAM menggunakan AWS RAM).
9. (Opsional) Jika Akun IPAM Org Utama ingin berhenti menemukan sumber daya di Org Sekunder, itu dapat memisahkan penemuan sumber daya dari IPAM (lihat). Pisahkan penemuan sumber daya
10. (Opsional) Jika Akun Admin Org Sekunder ingin berhenti berpartisipasi dalam IPAM Org Utama, mereka dapat membatalkan pembagian penemuan sumber daya bersama (lihat Memperbarui bagian sumber daya AWS RAM di Panduan AWS RAM Pengguna) atau menghapus penemuan sumber daya (lihatHapus penemuan sumber daya).

Gunakan IPAM dengan satu akun

Jika Anda memilih untuk tidak Integrasikan IPAM dengan akun di Organisasi AWS melakukannya, Anda dapat menggunakan IPAM dengan satu AWS akun.

Saat Anda membuat IPAM di bagian berikutnya, peran terkait layanan secara otomatis dibuat untuk layanan Amazon VPC IPAM di (IAM). AWS Identity and Access Management

Peran terkait layanan adalah jenis peran IAM yang memungkinkan AWS layanan mengakses AWS layanan lain atas nama Anda. Mereka menyederhanakan proses manajemen izin dengan secara otomatis membuat dan mengelola izin yang diperlukan untuk AWS layanan tertentu untuk melakukan tindakan yang diperlukan, merampingkan pengaturan dan administrasi layanan ini.

IPAM menggunakan peran terkait layanan untuk memantau dan menyimpan metrik yang CIDRs terkait dengan sumber daya jaringan. EC2 Untuk informasi selengkapnya tentang peran terkait layanan dan cara IPAM menggunakannya, lihat. Peran terkait layanan untuk IPAM

> **Important**
>
> Jika Anda menggunakan IPAM dengan satu AWS akun, Anda harus memastikan bahwa AWS akun yang Anda gunakan untuk membuat IPAM menggunakan peran IAM dengan kebijakan yang dilampirkan padanya yang mengizinkan tindakan tersebut. `iam:CreateServiceLinkedRole` Saat Anda membuat IPAM, Anda secara otomatis membuat peran terkait layanan AWSService RoleFor IPAM. Untuk informasi selengkapnya tentang mengelola kebijakan IAM, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

Setelah AWS akun tunggal memiliki izin untuk membuat peran terkait layanan IPAM, buka. Buat 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 alamat IP. CIDRs AWS Wilayah 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 AWS Wilayah 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 Manajer 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. AWS Wilayah tempat Anda membuat IPAM 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 CIDRs untuk in`us-west-2`, pilih VPCs `us-west-2` di sini. 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 apakah Anda ingin mengaktifkan IPv6 GUA Pribadi CIDRs. Untuk informasi selengkapnya tentang metrik ini, lihat Aktifkan penyediaan GUA pribadi IPv6 CIDRs.
8. Pilih apakah Anda ingin mengaktifkan mode Pengukuran. Untuk informasi selengkapnya tentang metrik ini, lihat Aktifkan distribusi biaya.
9. Pilih Buat IPAM.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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 IPAMs 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, lihatBagaimana IPAM bekerja.

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). CIDRs 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 tingkat atas IPv4 dan kemudian lewati keAlokasikan CIDRs dari kolam IPAM.

Konten

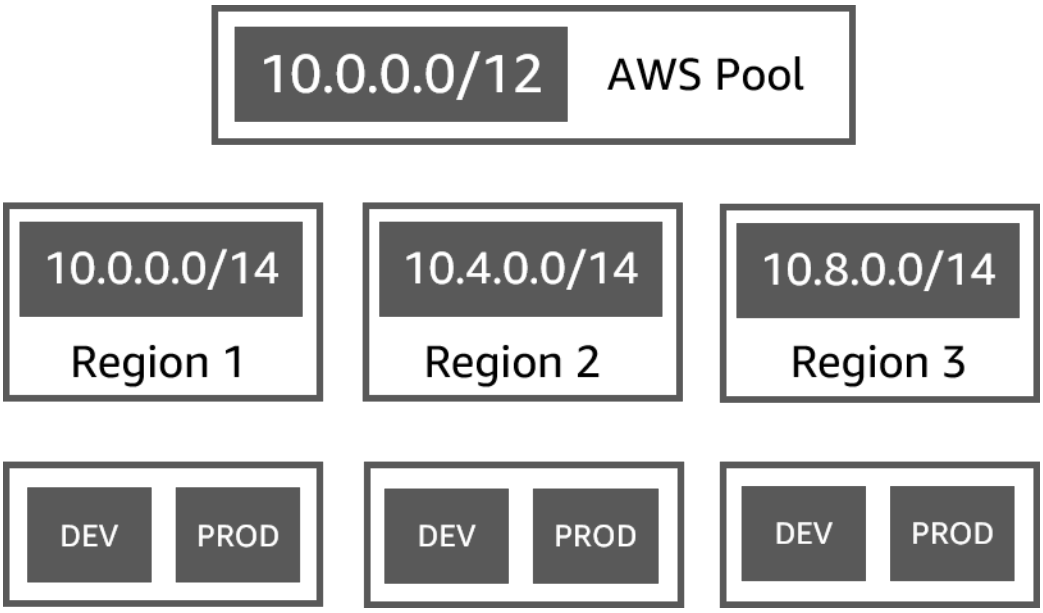
- Contoh rencana kolam IPAM
- Buat IPv4 kolam
- Buat kumpulan IPv6 alamat di IPAM Anda

Contoh rencana kolam IPAM

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

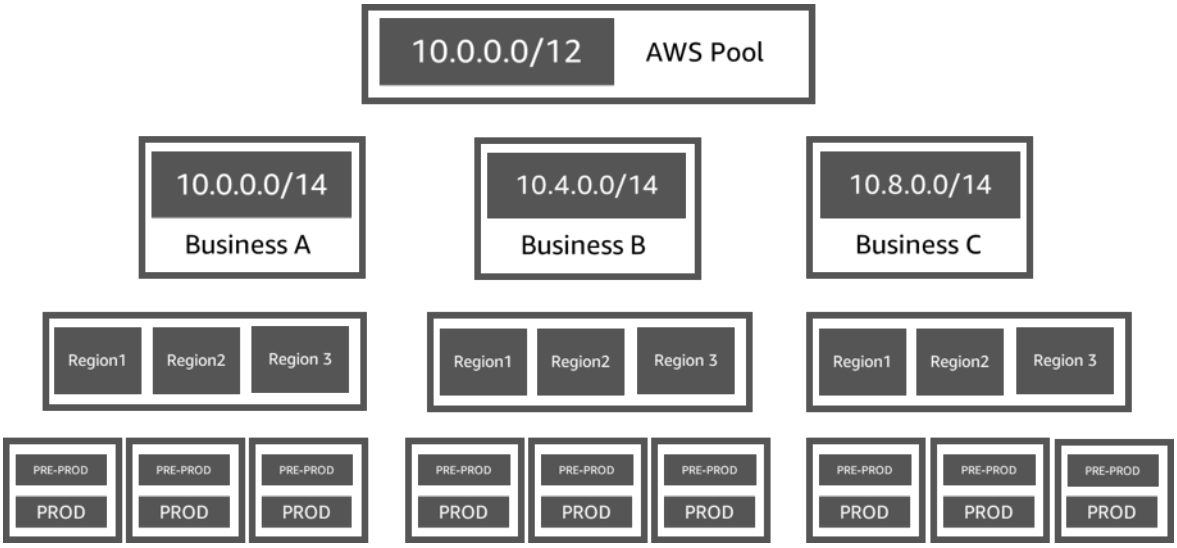
IPv4 kolam di beberapa AWS Wilayah

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.



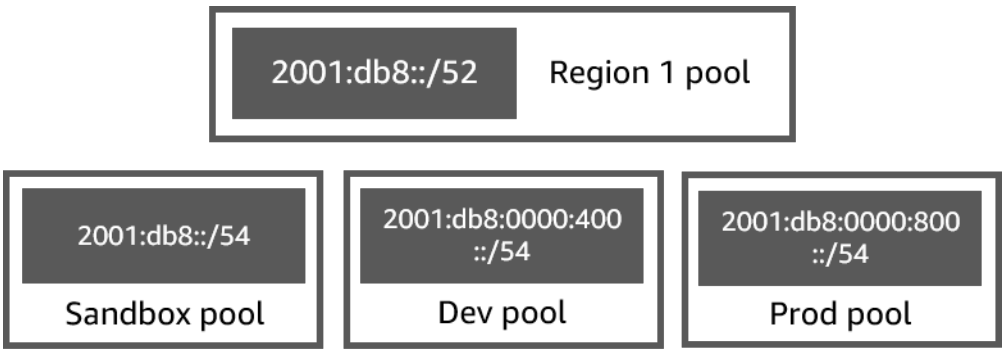
IPv4 kolam untuk berbagai lini bisnis

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.



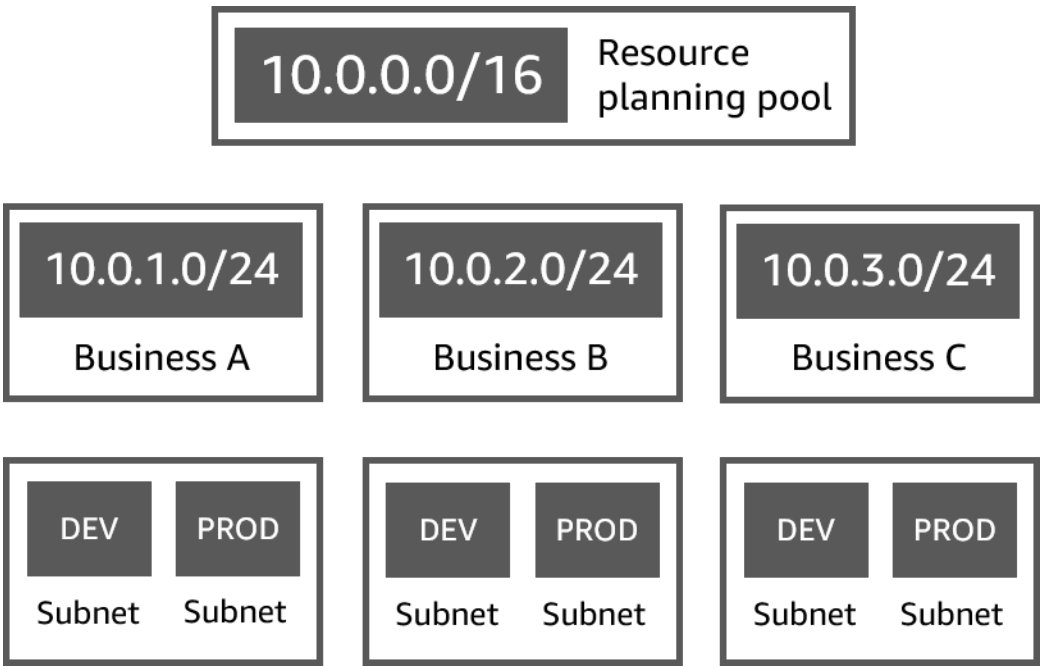
IPv6 kolam renang di suatu AWS Wilayah

Contoh berikut menunjukkan hierarki IPv6 kolam 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 IPv4 kolam

Ikuti langkah-langkah di bagian ini untuk membuat hierarki kolam IPv4 IPAM.

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

- 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 2 (10.0.0.0/16)
        - Kolam pengembangan (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.0.0/25)

Pada contoh sebelumnya, CIDRs yang digunakan hanyalah contoh saja. Mereka menggambarkan bahwa setiap kolam dalam kolam tingkat atas disediakan dengan sebagian CIDR tingkat atas.

Konten

Buat kolam tingkat atas IPv4

Ikuti langkah-langkah di bagian ini untuk membuat kolam IPAM IPv4 tingkat atas. Saat Anda membuat kolam, Anda menyediakan CIDR untuk digunakan kolam. 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 non-produksi VPCs (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.0.0/25)

Pada contoh sebelumnya, CIDRs yang digunakan hanyalah 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 CIDRs 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, lihatMemantau 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, lihatBagikan kolam IPAM menggunakan AWS 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 VPCs dengan tag prod yang dapat diperoleh CIDRs dari kumpulan IPAM. Anda juga dapat menetapkan aturan yang menyatakan bahwa CIDRs dialokasikan dari kumpulan ini tidak boleh lebih besar dari /24. Dalam hal ini, membuat sumber daya menggunakan CIDR yang lebih besar dari /24 dari kumpulan ini melanggar aturan alokasi pada kumpulan dan pembuatan gagal. Sumber daya yang ada dengan CIDR yang lebih besar dari /24 ditandai sebagai tidak sesuai.

> **Important**
>
> Topik ini mencakup cara membuat IPv4 kumpulan tingkat atas dengan rentang alamat IP yang disediakan oleh AWS. Jika Anda ingin membawa rentang IPv4 alamat 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, lihatBagaimana IPAM bekerja.

   Secara default, saat Anda membuat pool, cakupan pribadi default dipilih. Kolam dalam lingkup pribadi harus berupa IPv4 kolam renang. Kolam di ruang lingkup publik bisa IPv4 atau IPv6 kolam renang. 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 Alamat keluarga, 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 pool IPAM dengan tempat yang sama dengan Wilayah VPC tersebut. Harap diingat bahwa setelah Anda memilih tempat untuk sebuah pool, Anda tidak dapat memodifikasinya. Jika Wilayah asal IPAM tidak tersedia karena pemadaman dan pool memiliki tempat yang berbeda dari Wilayah asal IPAM, pool 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 sendiri IPv4 atau rentang alamat IPv6 IP 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-hal berikut:
      - CIDRs 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 CIDRs yang tumpang tindih, IPAM akan mengimpor CIDR terbesar saja.
- Jika IPAM menemukan beberapa CIDRs dengan pencocokan CIDRs, 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.
> - Butuh beberapa waktu agar alokasi CIDR VPC yang ada 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 IPv4 alamat adalah 0 - 32. Kemungkinan panjang netmask untuk IPv6 alamat 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 digunakan CIDRs 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.

> **Note**
>
> Aturan alokasi hanya berlaku untuk sumber daya terkelola dalam kumpulan itu. Aturan tidak berlaku untuk sumber daya di kolam dalam kolam renang.

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

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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 IPv4 kolam 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 CIDRs dari kolam IPAM

> **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 non-produksi VPCs (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.0.0/25)

Pada contoh sebelumnya, CIDRs yang digunakan hanyalah 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, lihatBagaimana IPAM bekerja.
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. Jika Anda membuat kumpulan ini di ruang lingkup publik, Anda akan melihat opsi untuk 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. 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 pool IPAM dengan locale yang sama dengan Wilayah VPC tersebut. Harap diingat bahwa setelah Anda memilih locale untuk sebuah pool, Anda tidak dapat memodifikasinya. Jika Wilayah asal IPAM tidak tersedia karena pemadaman dan pool memiliki locale yang berbeda dari Wilayah asal IPAM, pool masih dapat digunakan untuk mengalokasikan alamat IP.

   > **Note**
   >
   > Jika Anda membuat pool di Tingkat Gratis, Anda hanya dapat memilih wilayah lokal yang sesuai dengan Wilayah asal IPAM Anda. Untuk menggunakan semua fitur IPAM di seluruh wilayah lokal, tingkatkan ke Tingkat Lanjutan.

10. Jika Anda membuat kumpulan ini di ruang lingkup publik, Anda akan melihat opsi untuk Layanan. Pilih EC2(EIP/VPC). Layanan yang Anda pilih akan menentukan layanan AWS tempat CIDR akan dapat diiklankan. Saat ini, satu-satunya pilihan adalah EC2 (EIP/VPC), yang berarti bahwa CIDRs dialokasikan dari kumpulan ini akan dapat diiklankan untuk layanan EC2 Amazon (untuk alamat IP Elastis) dan layanan Amazon VPC (untuk terkait dengan). CIDRs VPCs
11. (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 CIDRs ke kolam kapan saja dengan mengedit kolam.
12. Anda memiliki opsi aturan alokasi yang sama di sini seperti yang Anda lakukan saat membuat kumpulan tingkat atas. Lihat Buat kolam tingkat atas IPv4 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.
13. (Opsional) Pilih Tag untuk kolam.

14. Setelah selesai mengonfigurasi pool, pilih Create pool.
15. Lihat Buat IPv4 kolam pengembangan.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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 IPv4 kolam 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 CIDRs dari kolam IPAM

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 non-produksi VPCs (10.0.0.0/24)
          - Alokasi untuk VPC (10.0.1.0/25)

Pada contoh sebelumnya, CIDRs yang digunakan hanyalah 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, lihatBagaimana IPAM bekerja.
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 CIDRs 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 tingkat atas IPv4 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 CIDRs dari kolam IPAM.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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 kumpulan IPv6 alamat di IPAM Anda

AWS menawarkan IPv6 konektivitas di banyak layanannya, termasuk EC2, VPC, dan S3, memungkinkan Anda untuk menggunakan ruang alamat yang ditingkatkan dan fitur keamanan yang ditingkatkan. IPv6 IPv6dirancang untuk mengatasi keterbatasan mendasar ini IPv4. Dengan pindah ke ruang alamat 128-bit, IPv6 menawarkan sejumlah besar alamat IP unik. Perluasan alamat besar-besaran ini memungkinkan proliferasi berkelanjutan dari teknologi yang terhubung, dari smartphone dan perangkat IoT hingga infrastruktur cloud.

Selain itu, Anda dapat menggunakan IPAM untuk memastikan bahwa Anda menggunakan berdekatan IPv6 CIDRs untuk pembuatan VPC. Dialokasikan secara bersebelahan adalah yang dialokasikan secara CIDRs berurutan. CIDRs Mereka memungkinkan Anda untuk menyederhanakan aturan keamanan dan jaringan Anda; IPv6 CIDRs dapat digabungkan dalam satu entri di seluruh jaringan dan konstruksi keamanan seperti daftar kontrol akses, tabel rute, grup keamanan, dan firewall.

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

> **Note**
>
> IPv6 Pengalamatan publik dan pribadi tersedia di AWS. AWS mempertimbangkan alamat IP publik yang diiklankan di internet dari AWS, sedangkan alamat IP pribadi tidak dan tidak dapat diiklankan di internet dari. AWS Jika Anda ingin jaringan pribadi Anda mendukung IPv6 dan tidak berniat merutekan lalu lintas dari alamat ini ke internet, buat IPv6 kolam Anda dalam lingkup pribadi. Untuk informasi selengkapnya tentang IPv6 alamat publik dan pribadi, lihat IPv6alamat di Panduan Pengguna Amazon VPC.

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

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

Pada contoh sebelumnya, CIDRs yang digunakan hanyalah contoh saja. Mereka menggambarkan bahwa kolam Pengembangan di dalam kolam Regional disediakan dengan sebagian dari kumpulan Regional CIDR.

Konten

Buat kumpulan IPv6 alamat Regional di IPAM Anda

Ikuti langkah-langkah di bagian ini untuk membuat kolam IPAM IPv6 regional. 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 IPv6 regional:

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

Pada contoh sebelumnya, CIDRs yang digunakan hanyalah contoh saja. Mereka menggambarkan bahwa setiap kolam dalam kolam IPv6 regional 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, lihatMemantau penggunaan CIDR berdasarkan sumber daya.

> **Note**
>
> 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, lihatBagikan kolam IPAM menggunakan AWS 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 VPCs dengan tag prod yang dapat diperoleh CIDRs dari kumpulan IPAM.

Note

- Topik ini mencakup cara membuat kolam IPv6 regional dengan rentang IPv6 alamat yang disediakan oleh AWS atau dengan IPv6 jangkauan pribadi. Jika Anda ingin membawa rentang alamat publik IPv4 atau IPv6 IP Anda sendiri ke AWS (BYOIP), ada prasyarat. Untuk informasi selengkapnya, lihat Tutorial: Bawa alamat IP Anda ke IPAM.
- Jika Anda membuat IPv6 kolam dalam lingkup pribadi, Anda dapat menggunakan rentang IPv6 GUA atau ULA pribadi. Untuk menggunakan rentang GUA pribadi, Anda harus terlebih dahulu mengaktifkan opsi pada IPAM Anda (lihatAktifkan penyediaan GUA pribadi IPv6 CIDRs).

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 pribadi atau publik. Jika Anda ingin jaringan pribadi Anda mendukung IPv6 dan tidak berniat merutekan lalu lintas dari alamat ini ke internet, pilih ruang lingkup pribadi. Untuk informasi lebih lanjut tentang cakupan, lihatBagaimana IPAM bekerja.

   Secara default, saat Anda membuat pool, cakupan pribadi default dipilih.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.
6. Di bawah Sumber, pilih cakupan IPAM.
7. Untuk keluarga Alamat, pilih IPv6. Jika Anda membuat kumpulan ini di ruang lingkup publik, semua yang ada CIDRs di kolam ini akan dapat diiklankan secara publik.
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. Jika Anda ingin menyediakan blok IPv6 CIDR yang disediakan Amazon ke kolam, itu 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 pool IPAM dengan tempat yang sama dengan Wilayah VPC tersebut. Harap diingat bahwa setelah Anda memilih tempat untuk sebuah pool, Anda tidak dapat memodifikasinya. Jika Wilayah asal IPAM tidak tersedia karena pemadaman dan pool memiliki tempat yang berbeda dari Wilayah asal IPAM, pool masih dapat digunakan untuk mengalokasikan alamat IP.

> **Note**
>
> Jika Anda membuat pool di Tingkat Gratis, Anda hanya dapat memilih tempat yang sesuai dengan Wilayah asal IPAM Anda. Untuk menggunakan semua fitur IPAM di seluruh tempat, tingkatkan ke Tingkat Lanjutan.

10. (Opsional) Jika Anda membuat IPv6 pool di ruang lingkup publik, di bawah Layanan, pilih EC2 (EIP/VPC). Layanan yang Anda pilih akan menentukan layanan AWS tempat 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 terkait dengan). CIDRs VPCs
11. (Opsional) Jika Anda membuat IPv6 kumpulan dalam lingkup publik, di bawah opsi sumber IP Publik, pilih Amazon yang dimiliki untuk AWS menyediakan rentang IPv6 alamat untuk kumpulan ini. Sebagaimana dicatat di bagian atas halaman ini, topik ini mencakup cara membuat kumpulan IPv6 regional dengan rentang alamat IP yang disediakan oleh AWS. Jika Anda ingin membawa sendiri IPv4 atau rentang IPv6 alamat ke AWS (BYOIP), ada prasyarat. Untuk informasi selengkapnya, lihat Tutorial: Bawa alamat IP Anda ke IPAM.
12. (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, lakukan salah satu hal berikut:

    - Jika Anda membuat IPv6 kumpulan di ruang lingkup publik dengan sumber IP Publik milik Amazon, untuk menyediakan CIDR, di bawah ketentuan, pilih Tambahkan CIDR milik Amazon dan pilih ukuran netmask antara/40 dan /52 CIDRs untuk CIDR. Ketika Anda memilih panjang netmask di menu dropdown, Anda melihat panjang netmask serta jumlah /56 CIDRs yang diwakili netmask. Secara default, Anda dapat menambahkan satu

blok IPv6 CIDR yang disediakan Amazon ke kolam Regional. Untuk informasi tentang meningkatkan batas default, lihatKuota untuk IPAM Anda.

- Jika Anda membuat IPv6 kolam dalam lingkup pribadi, Anda dapat menggunakan rentang IPv6 GUA atau ULA pribadi:
  - Untuk detail penting tentang IPv6 pengalamatan pribadi, lihat IPv6 Alamat pribadi di Panduan Pengguna Amazon VPC.
  - Untuk menggunakan rentang IPv6 ULA pribadi, di bawah CIDRsketentuan, pilih Tambahkan ULA CIDR oleh netmask dan pilih ukuran netmask atau pilih Input IPv6 CIDR pribadi dan masukkan rentang ULA. Ruang IPv6 ULA yang valid adalah apa pun di bawah fd00: :/8 yang tidak tumpang tindih dengan rentang cadangan Amazon fd00: :/16.
  - Untuk menggunakan rentang IPv6 GUA pribadi, Anda harus terlebih dahulu mengaktifkan opsi pada IPAM Anda (lihatAktifkan penyediaan GUA pribadi IPv6 CIDRs). Setelah Anda mengaktifkan IPv6 GUA pribadi CIDRs, masukkan IPv6 GUA di Input IPv6 CIDR pribadi.

13. 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 IPv6 alamat 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 CIDRs 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 digunakan CIDRs 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.

14. (Opsional) Pilih Tag untuk kolam.
15. Pilih Buat kolam.
16. Lihat Buat kumpulan IPv6 alamat pengembangan di IPAM Anda.

Command line

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

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

1. Jika Anda ingin mengaktifkan penyediaan IPv6 GUA pribadi CIDRs, ubah IPAM dengan modify-ipam dan sertakan opsi untuk. `enable-private-gua` Untuk informasi selengkapnya, lihat Aktifkan penyediaan GUA pribadi IPv6 CIDRs.
2. Buat kolam dengan create-ipam-pool.
3. Menyediakan CIDR ke kolam: provision-ipam-pool-cidr.
4. Edit kumpulan setelah Anda membuatnya untuk mengubah aturan alokasi: modify-ipam-pool.

Buat kumpulan IPv6 alamat pengembangan di IPAM Anda

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

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
  - Cakupan
    - Kolam regional di AWS Wilayah 1 (2001:db8: :/52)
      - Kolam pengembangan (2001:db8: :/54)
        - Alokasi untuk VPC (2001:db8: :/56)

Pada contoh sebelumnya, CIDRs yang digunakan hanyalah 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 IPv6 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 lingkup IPAM, pilih ruang lingkup. Untuk informasi lebih lanjut tentang cakupan, lihatBagaimana IPAM bekerja.
5. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool.
6. Di bawah Sumber, pilih kolam IPAM. Kemudian, di bawah kolam Sumber, pilih kolam IPv6 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 CIDRs ke kolam kapan saja dengan mengedit kolam.
9. Anda memiliki opsi aturan alokasi yang sama di sini seperti yang Anda lakukan saat membuat kumpulan IPv6 Regional. Lihat Buat kumpulan IPv6 alamat Regional di IPAM Anda 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 kolam renang.
11. Setelah selesai mengonfigurasi pool, pilih Create pool.
12. Lihat Alokasikan CIDRs dari kolam IPAM.

Command line

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

Gunakan AWS CLI perintah berikut untuk membuat kumpulan IPv6 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 kumpulan pengembangan tambahan di dalam kolam IPv6 Regional, sesuai kebutuhan.

Alokasikan CIDRs dari kolam IPAM

Salah satu fitur penting dari IPAM adalah kemampuan untuk mengalokasikan dan mengelola ruang alamat IP. Saat membuat VPC, Anda harus menentukan blok CIDR alamat IP, yang menentukan rentang alamat IP yang tersedia untuk VPC tersebut. IPAM menyederhanakan proses ini dengan memberikan tampilan global dari seluruh inventaris alamat IP Anda, membantu Anda menetapkan dan menggunakan kembali awalan IP secara strategis di beberapa. VPCs

Alokasi ruang alamat ini sangat penting untuk memastikan tidak ada rentang IP yang tumpang tindih, yang dapat menyebabkan konflik perutean dan masalah konektivitas. IPAM juga memungkinkan Anda untuk memesan ruang alamat IP untuk ekspansi VPC future, menghindari kebutuhan untuk penomoran ulang yang rumit nanti.

Ikuti langkah-langkah di bagian ini untuk mengalokasikan CIDR dari kolam IPAM ke 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. Alokasikan digunakan saat Anda mengaitkan CIDR dari kolam IPAM dengan sumber daya.

Anda dapat mengalokasikan CIDRs dari kolam IPAM dengan cara berikut:

- Gunakan AWS layanan yang terintegrasi dengan IPAM, seperti Amazon VPC, dan pilih opsi untuk menggunakan kolam IPAM untuk CIDR. IPAM secara otomatis membuat alokasi di kolam untuk Anda.

- Alokasikan CIDR secara manual dalam kolam IPAM untuk memesannya untuk digunakan nanti dengan AWS layanan yang terintegrasi dengan IPAM, seperti Amazon VPC.

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

Daftar Isi

Buat VPC yang menggunakan CIDR kolam IPAM

Dengan Amazon Virtual Private Cloud (Amazon VPC), Anda dapat meluncurkan AWS sumber daya di jaringan virtual yang terisolasi secara logis yang telah Anda tentukan. Jaringan virtual ini sangat mirip dengan jaringan konvensional yang akan Anda operasikan di pusat data Anda sendiri dengan manfaatnya, yaitu menggunakan infrastruktur AWS yang dapat diskalakan.

Virtual Private Cloud (VPC) adalah jaringan virtual yang didedikasikan untuk akun Anda AWS . VPC diisolasi secara logis dari jaringan virtual lain di Cloud AWS . Anda dapat menentukan rentang alamat IP untuk VPC, menambahkan subnet, menambahkan gateway, dan mengaitkan grup keamanan.

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 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 petunjuk lengkap menggunakan AWS CLI, termasuk membuat VPC, lihat bagian. Tutorial untuk Manajer Alamat IP VPC Amazon

Alokasikan CIDR secara manual ke kolam untuk memesan ruang alamat IP

Ikuti langkah-langkah di bagian ini untuk mengalokasikan CIDR secara manual ke kolam. Anda dapat melakukan ini untuk memesan CIDR dalam kolam IPAM untuk digunakan nanti. Anda juga dapat memesan ruang di kolam IPAM untuk mewakili jaringan lokal. IPAM akan mengelola reservasi tersebut untuk Anda dan menunjukkan jika ada CIDRs 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, 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, lihatBagaimana IPAM bekerja.
4. Di panel konten, pilih kolam renang.
5. Pilih Tindakan > Buat alokasi kustom.
6. Pilih apakah akan menambahkan CIDR tertentu untuk dialokasikan (misalnya, `10.0.0.0/24` untuk IPv4 atau `2001:db8::/52` untuk IPv6) atau tambahkan CIDR berdasarkan ukuran dengan memilih panjang netmask saja (misalnya, untuk atau `/24` untuk IPv4). `/52` IPv6
7. Pilih Alokasikan.
8. Anda dapat melihat alokasi di IPAM dengan memilih Pools di panel navigasi, memilih kolam, dan melihat tab Alokasi untuk kolam.

Command line

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

Gunakan AWS CLI perintah berikut untuk mengalokasikan CIDR secara manual ke kolam:

1. Dapatkan ID 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 merilis CIDR yang dialokasikan secara manual, lihat. Lepaskan alokasi

Mengelola ruang alamat IP di IPAM

Tugas di bagian ini adalah opsional. Perhatikan bahwa bagian ini adalah pengelompokan prosedur yang semuanya terkait dengan bekerja dengan IPAM. Prosedurnya diurutkan menurut abjad.

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

Otomatiskan pembaruan daftar prefiks dengan IPAM

Daftar awalan terkelola adalah sekumpulan blok CIDR yang dapat Anda referensikan dalam aturan grup keamanan dan tabel rute alih-alih menentukan alamat IP individual. Misalnya, alih-alih membuat aturan grup keamanan terpisah untuk`10.1.0.0/16`,, dan `10.2.0.0/1610.3.0.0/16`, Anda dapat membuat satu daftar awalan yang berisi ketiganya CIDRs dan mereferensikannya dalam satu aturan.

Ada dua jenis:

- Daftar awalan yang dikelola pelanggan: Rentang IP yang Anda tentukan dan kelola
- AWS-daftar awalan terkelola: rentang IP untuk AWS layanan (seperti S3 atau) CloudFront

Fitur IPAM ini mengotomatiskan pengelolaan daftar awalan yang dikelola pelanggan dengan menjaga entri CIDR Anda disinkronkan dengan perubahan jaringan Anda.

Masalah ini memecahkan

Tanpa otomatisasi, tim jaringan menghabiskan waktu yang signifikan untuk memperbarui daftar awalan secara manual saat infrastruktur berubah dan mempertahankan daftar awalan yang konsisten di seluruh lingkungan dan Wilayah.

IPAM memecahkan ini dengan membiarkan Anda membuat aturan yang secara otomatis mengisi daftar awalan. Anda dapat menggunakan dua pendekatan: referensi CIDRs dari kolam IPAM Anda, atau membuat aturan berdasarkan AWS sumber daya Anda yang sebenarnya — seperti 'sertakan semua yang VPCs ditandai dengan env=prod', 'sertakan semua subnet di us-east-1', atau 'sertakan semua alamat IP Elastis yang dimiliki oleh akun 123456789'. Ketika Anda menambahkan atau menghapus sumber daya ini, IPAM secara otomatis memperbarui daftar awalan dengan mereka. CIDRs

Cara kerjanya

Anda membuat aturan yang memberi tahu IPAM alamat IP mana yang akan disertakan dalam daftar awalan. Misalnya, “sertakan semua VPC yang CIDRs ditandai dengan env=prod”. Saat Anda menambah atau menghapus produksi VPCs, IPAM secara otomatis memperbarui daftar awalan.

Kapan menggunakannya

- Grup keamanan: Buat aturan “sertakan semua env = prod yang VPCs ditandai” sehingga saat Anda menambahkan produksi baru VPCs, aturan tersebut secara otomatis diizinkan dalam aturan grup keamanan Anda
- Multi-wilayah: Terapkan aturan IPAM yang sama di beberapa wilayah untuk menyimpan daftar awalan yang identik tanpa menyalin entri CIDR secara manual
- Infrastruktur dinamis: Ketika Anda create/delete VPCs atau subnet, mereka CIDRs secara otomatis added/removed dari daftar awalan tanpa pembaruan manual

Prasyarat

Sebelum Anda mulai, pastikan Anda memiliki:

- IPAM dengan Tingkat Lanjut diaktifkan
- Daftar awalan yang dikelola pelanggan (atau buat satu selama penyiapan)
- Izin IAM untuk operasi daftar awalan IPAM dan EC2

Langkah-langkah penyiapan

Langkah 1: Buat resolver daftar awalan IPAM

Tentukan mana CIDRs yang akan disertakan dalam daftar awalan Anda dengan membuat resolver daftar awalan IPAM.

AWS Management Console

Untuk membuat resolver daftar awalan IPAM

1. Buka konsol IPAM.
2. Di panel navigasi, pilih Penyelesai daftar awalan.
3. Pilih Buat resolver daftar awalan.
4. Pada Langkah 1: Konfigurasikan detail resolver, pilih yang berikut ini:
   - IPAM: Sebuah contoh IPAM
   - Alamat keluarga: IPv4 atau IPv6

- Tag nama - opsional: Nama deskriptif
- Deskripsi - opsional: Deskripsi
- Tags: Tag sumber daya

5. Pilih Berikutnya.
6. Pada Langkah 2: Konfigurasikan aturan, pilih Tambahkan aturan. Anda dapat menambahkan hingga 99 aturan.

> **Important**
>
> Anda dapat membuat resolver daftar awalan tanpa aturan pemilihan CIDR apa pun, tetapi itu akan menghasilkan versi kosong (tidak mengandung CIDRs) hingga Anda menambahkan aturan.

7. Pilih salah satu jenis aturan:

- CIDR statis: Daftar tetap CIDRs yang tidak berubah (seperti daftar manual yang direplikasi di seluruh Wilayah)
- CIDR kolam IPAM: CIDRs dari kolam IPAM tertentu (seperti semua CIDRs dari kolam produksi IPAM Anda)

  Jika Anda memilih opsi ini, pilih salah satu hal berikut:

  - Cakupan IPAM: Pilih cakupan IPAM untuk mencari sumber daya
  - Kondisi:
    - Properti
      - ID kolam IPAM: Pilih pool IPAM yang berisi sumber daya
      - CIDR (seperti 10.24.34.0/23)
    - Operasi: Equals/Not sama
    - Nilai: Nilai yang akan dicocokkan dengan kondisi
- Cakupan sumber daya CIDR: CIDRs dari AWS sumber daya seperti VPCs, subnet, EIPs dalam lingkup IPAM

  Jika Anda memilih opsi ini, pilih salah satu hal berikut:

  - Cakupan IPAM: Pilih cakupan IPAM untuk mencari sumber daya
  - Tipe sumber daya: Pilih sumber daya, seperti VPC atau subnet.
  - Kondisi:

- Properti:
  - ID sumber daya: ID unik sumber daya (seperti vpc-1234567890abcdef0)
  - Pemilik sumber daya (seperti 111122223333)
  - Wilayah sumber daya (seperti us-east-1)
  - Tanda sumber daya (seperti kunci: nama, nilai: dev-vpc-1)
  - CIDR (seperti 10.24.34.0/23)
- Operasi: Equals/Not sama
- Nilai: Nilai yang akan dicocokkan dengan kondisi

8. Pilih Berikutnya.
9. Pilih Validasi dan buat.

Command line

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

Gunakan AWS CLI perintah berikut untuk membuat resolver daftar awalan IPAM:

- Gunakan perintah create-ipam-prefix-list-resolver dan simpan ID resolver yang dikembalikan untuk langkah 2.

Langkah 2: Buat target resolver untuk terhubung ke daftar awalan

Tautkan resolver Anda ke daftar awalan yang ada dengan membuat target resolver. Gunakan ID resolver yang dikembalikan dari Langkah 1.

AWS Management Console

Untuk membuat target penyelesai daftar awalan IPAM

1. Di konsol IPAM, pilih Penyelesai daftar awalan.
2. Pilih resolver yang Anda buat di Langkah 1.
3. Pada halaman detail resolver, pilih tab Target.
4. Pilih Buat target.
5. Konfigurasikan target:

- Wilayah: Pilih Wilayah tempat daftar awalan terkelola yang ada atau tempat Anda akan membuatnya.
- Daftar awalan: Pilih daftar awalan terkelola yang ada atau buat yang baru

6. Di bawah Versi yang diinginkan, pilih salah satu dari berikut ini:
   - Selalu lacak versi terbaru: Pilih ini untuk pembaruan otomatis ketika Anda ingin daftar prefiks Anda tetap terkini seiring dengan perubahan infrastruktur tanpa intervensi manual.
   - Lacak versi tertentu: Pilih ini untuk stabilitas saat Anda membutuhkan pembaruan yang dapat diprediksi dan terkontrol, dan jika Anda ingin menyetujui perubahan pada daftar prefiks Anda secara manual.
7. Pilih Buat target.

Command line

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

Gunakan AWS CLI perintah berikut untuk membuat target penyelesai daftar awalan IPAM:

- Gunakan perintah create-ipam-prefix-list-resolver-target dengan ID resolver dari langkah 1 dan ID daftar awalan yang ada.

IPAM sekarang secara otomatis memperbarui daftar awalan Anda berdasarkan aturan Anda. Daftar awalan akan diisi dengan CIDRs pencocokan kriteria Anda.

Langkah 3: Memantau versi dan sinkronisasi

Sebagai hasil dari pembuatan resolver daftar awalan dan target, penyelesai daftar awalan menghasilkan versi CIDR berdasarkan aturan Anda dan kemudian target menyinkronkannya CIDRs dari resolver ke daftar awalan terkelola tertentu. Setiap versi adalah snapshot dari apa yang CIDRs cocok dengan aturan Anda pada saat itu. Nomor versi bertambah setiap kali daftar CIDR berubah karena perubahan infrastruktur.

Contoh versi:

Keadaan Awal (Versi 1)

Lingkungan produksi:

- vpc-prod-web (10.1.0.0/16) - ditandai env=prod
- vpc-prod-db (10.2.0.0/16) - ditandai env=prod

Aturan penyelesai: Sertakan semua VPCs env = prod yang ditandai

Versi 1 CIDRs: 10.1.0.0/16, 10.2.0.0/16

Perubahan Infrastruktur (Versi 2)

VPC baru ditambahkan:

- vpc-prod-api (10.3.0.0/16) - ditandai env=prod

IPAM secara otomatis mendeteksi perubahan dan membuat versi baru.

Versi 2 CIDRs: 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16

Bagian ini menjelaskan bagaimana Anda dapat memantau pembuatan versi dengan AWS konsol atau AWS CLI dan keberhasilan sinkronisasi dengan CLI. AWS

Selain itu, kami mendorong Anda untuk menyetel CloudWatch alarm pada metrik kegagalan karena Anda mungkin perlu menilai kembali dan menyesuaikan aturan pemilihan CIDR agar tetap berada dalam batas untuk versi dan ukuran daftar awalan. Untuk daftar CloudWatch metrik yang terkait dengan daftar awalan IPAM, lihat. Metrik penyelesai daftar awalan IPAM

AWS Management Console

Untuk melihat versi yang dibuat dan memantau sinkronisasi target

1. Di konsol IPAM, pilih Penyelesai daftar awalan.
2. Pilih resolver yang Anda buat di Langkah 1.
3. Pada halaman detail resolver, pilih tab Versi. Di sini Anda akan melihat versi apa pun yang telah dibuat oleh resolver bersama dengan versi apa pun CIDRs .
4. Pada halaman detail resolver, pilih tab Monitoring. Dalam tampilan ini, Metrik penyelesai daftar awalan IPAM disajikan dalam bentuk grafik:
   - Keberhasilan pembuatan versi penyelesai daftar awalan
   - Kegagalan pembuatan versi penyelesai daftar awalan

5. Dari tab Pemantauan, Anda juga dapat mengonfigurasi CloudWatch alarm dengan memilih Buat alarm untuk pembuatan versi penyelesai daftar awalan. Anda dibawa ke CloudWatch konsol dengan alarm yang dikonfigurasi sebagian untuk metrik. Untuk informasi selengkapnya tentang cara menyelesaikan pembuatan alarm, lihat Membuat CloudWatch alarm berdasarkan ambang batas statis di Panduan CloudWatch Pengguna Amazon.

Command line

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

Gunakan AWS CLI perintah berikut untuk memantau versi dan sinkronisasi:

1. Gunakan resolver-version-entries perintah get-ipam-prefix-list- untuk melihat versi terbaru yang dibuat oleh resolver.
2. Gunakan perintah describe-ipam-prefix-list-resolver-target untuk memantau status sinkronisasi target resolver.

Perintah monitor menunjukkan:

- state - status sinkronisasi saat ini (create-complete, modify-complete, dan banyak lagi)
- lastSyncedVersion - Versi terakhir berhasil disinkronkan
- DesiredVersion - versi target untuk disinkronkan
- StateMessage - detail kesalahan jika sinkronisasi gagal

> **Important**
>
> Untuk mendukung alur kerja rollback, IPAM akan menyimpan salinan dari 10 versi resolver daftar awalan sebelumnya untuk masing-masing targetnya; Selain itu, IPAM akan menghapus versi yang lebih lama dari ambang ini jika tetap tidak direferensikan selama 7 hari tambahan.

Langkah 4: (Opsional) Aktifkan dan nonaktifkan sinkronisasi daftar awalan IPAM

Jika daftar awalan terkelola telah dikonfigurasi sebagai target daftar awalan IPAM dan Anda ingin membuat perubahan pada daftar awalan tanpa memerlukan izin untuk mengakses target penyelesai

daftar awalan IPAM, Anda dapat mengubah daftar awalan terkelola dan menonaktifkan sinkronisasi dengan penyelesai daftar awalan IPAM. Ketika dinonaktifkan, daftar CIDRs awalan tidak diperbarui secara otomatis dan Anda dapat membuat perubahan pada mereka. Saat diaktifkan, daftar awalan diperbarui CIDRs secara otomatis berdasarkan aturan pemilihan CIDR resolver terkait.

Ubah status pemantauan VPC CIDRs

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 VPC CIDRs 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: CIDR VPC telah terdeteksi oleh IPAM dan sedang dipantau untuk tumpang tindih dengan kepatuhan aturan alokasi lainnya. CIDRs
- Diabaikan: CIDR VPC telah dipilih untuk dibebaskan dari pemantauan. VPC yang diabaikan tidak CIDRs dievaluasi untuk tumpang tindih dengan kepatuhan aturan lain CIDRs atau 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 di https://console.aws.amazon.com/ipam/.

2. Pada panel navigasi, silakan 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 bawah VPC CIDRs, pilih salah satu yang CIDRs dialokasikan ke VPC dan pilih Tindakan > Tandai sebagai diabaikan atau Hapus tanda sebagai diabaikan.
6. Pilih Tandai sebagai diabaikan atau Hapus tanda sebagai diabaikan.

Command line

Gunakan AWS CLI perintah berikut untuk mengubah status pemantauan CIDR VPC:

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

Buat cakupan tambahan

Ikuti langkah-langkah di bagian ini untuk membuat ruang lingkup tambahan.

Cakupan adalah kontainer dengan tingkat tertinggi di dalam IPAM. Ketika Anda membuat IPAM, IPAM menciptakan 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 alamat IP tumpang tindih 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 Anda 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 pribadi IPv4 atau pribadi IPv6 CIDRs, sumber daya CIDRs diimpor ke ruang lingkup pribadi default dan tidak muncul dalam cakupan pribadi tambahan apa pun yang Anda buat. Anda dapat berpindah CIDRs dari cakupan pribadi default ke ruang lingkup pribadi lainnya. Untuk informasi, lihat Pindahkan VPC antar cakupan CIDRs.

AWS Management Console

Untuk membuat ruang lingkup pribadi tambahan

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

Command line

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

Gunakan AWS CLI perintah berikut untuk membuat ruang lingkup pribadi tambahan:

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

Hapus IPAM

Anda mungkin ingin menghapus IPAM jika tidak lagi diperlukan, jika Anda perlu merestrukturisasi manajemen alamat IP Anda, atau jika Anda ingin memulai baru dengan konfigurasi IPAM

baru. Menghapus IPAM dapat membantu menyederhanakan manajemen alamat IP Anda dan menyelaraskan dengan perubahan persyaratan bisnis atau operasional.

Ikuti langkah-langkah di bagian ini untuk menghapus IPAM. Untuk informasi tentang meningkatkan jumlah default yang dapat IPAMs Anda miliki daripada menghapus IPAM yang ada, lihat. Kuota untuk IPAM Anda

> **Note**
>
> Menghapus IPAM menghapus semua data yang dipantau yang terkait dengan IPAM termasuk data historis untuk. CIDRs

AWS Management Console

Untuk menghapus 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 > Hapus IPAM.
5. Lakukan salah satu tindakan berikut:

   - Pilih Hapus Cascade untuk menghapus IPAM, cakupan pribadi, kumpulan dalam cakupan pribadi, dan alokasi apa pun di kolam dalam lingkup pribadi. Anda tidak dapat menghapus IPAM dengan opsi ini jika ada kumpulan di ruang lingkup publik Anda. Jika Anda menggunakan opsi ini, IPAM melakukan hal berikut:
     - Menyalokasikan semua yang CIDRs dialokasikan ke sumber daya VPC (seperti VPCs) di kolam dalam lingkup pribadi.

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

     - Pembatalan semua IPv4 CIDRs disediakan untuk kolam IPAM dalam lingkup pribadi.
     - Menghapus semua kolam IPAM dalam cakupan 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:
    - Alokasi rilis dalam kolam IPAM. Untuk informasi selengkapnya, lihat Lepaskan alokasi.
    - CIDRs Deprovision disediakan untuk pool dalam IPAM. Untuk informasi selengkapnya, lihat Pembuangan CIDRs dari kolam.
    - Hapus cakupan non-default tambahan. Untuk informasi selengkapnya, lihat Hapus ruang lingkup.
    - Hapus kolam IPAM Anda. Untuk informasi selengkapnya, lihat Hapus kolam.
6. Masuk **`delete`** dan kemudian pilih Hapus.

Command line

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

Gunakan AWS CLI perintah berikut untuk menghapus IPAM:

1. Lihat saat ini IPAMs: deskripsikan ipams
2. Hapus IPAM: hapus-ipam
3. Lihat update Anda IPAMs: describe-ipams

Untuk membuat IPAM baru, lihatBuat IPAM.

Hapus kolam

Kumpulan IPAM di AWS mewakili rentang alamat IP yang ditentukan yang dapat dialokasikan dan dikelola dalam AWS lingkungan atau organisasi tertentu. Pool digunakan untuk mengatur ruang alamat IP, mengaktifkan manajemen alamat IP otomatis, dan menerapkan kebijakan tata kelola alamat IP di seluruh infrastruktur cloud Anda.

Anda mungkin ingin menghapus kolam IPAM untuk menghapus ruang alamat IP yang tidak terpakai atau tidak perlu dan merebutnya kembali untuk tujuan lain. Anda tidak dapat menghapus kumpulan alamat IP jika ada alokasi di dalamnya. Anda harus terlebih dahulu melepaskan alokasi dan Pembuangan CIDRs dari kolam sebelum Anda dapat menghapus kumpulan.

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

AWS Management Console

Untuk menghapus kolam

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

Command line

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

Gunakan AWS CLI perintah berikut untuk menghapus pool:

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

Untuk membuat kolam baru, lihatBuat kolam tingkat atas IPv4.

Hapus ruang lingkup

Anda mungkin ingin menghapus cakupan IPAM jika tidak lagi memenuhi tujuan yang dimaksudkan, seperti ketika Anda merestrukturisasi jaringan Anda, mengkonsolidasikan wilayah, atau menyesuaikan alokasi alamat IP Anda. Menghapus cakupan yang tidak digunakan dapat membantu merampingkan konfigurasi IPAM Anda dan mengoptimalkan manajemen alamat IP Anda di dalamnya. AWS

> **Note**
>
> Anda tidak dapat menghapus cakupan jika salah satu dari 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 cakupan adalah cakupan default, lihat jenis Lingkup dalam detail cakupan.
> - Ada satu atau lebih kolam dalam ruang lingkup. Anda harus terlebih dahulu Hapus kolam sebelum Anda dapat menghapus ruang lingkup.

AWS Management Console

Untuk menghapus ruang lingkup

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Lingkup.
3. Di panel konten, pilih cakupan yang ingin Anda hapus.
4. Pilih Tindakan > Hapus cakupan.
5. Masuk **`delete`** dan kemudian pilih Hapus.

Command line

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

Gunakan AWS CLI perintah berikut untuk menghapus ruang lingkup:

1. Lihat cakupan: describe-ipam-scopes
2. Hapus ruang lingkup: delete-ipam-scope
3. Lihat cakupan yang diperbarui: describe-ipam-scopes

Untuk membuat ruang lingkup baru, lihatBuat cakupan tambahan. Untuk menghapus IPAM, lihatHapus IPAM.

Pembuangan CIDRs dari kolam

Anda mungkin ingin menghentikan penyediaan CIDR kumpulan untuk membebaskan ruang alamat IP, menyederhanakan manajemen alamat IP, mempersiapkan perubahan jaringan, atau memenuhi persyaratan kepatuhan. Mendeprovisioning kumpulan CIDR memungkinkan kontrol dan optimalisasi alokasi alamat IP Anda yang lebih baik dalam IPAM, sambil memastikan ruang IP yang tidak digunakan direklamasi dan tersedia untuk penggunaan di masa mendatang. Anda tidak dapat menghentikan penyediaan CIDR jika ada alokasi di kolam. Untuk menghapus alokasi, lihatthe section called “Lepaskan alokasi”.

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

AWS Management Console

Untuk menghentikan penyediaan kolam CIDR

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatBagaimana IPAM bekerja.
4. Di panel konten, pilih kumpulan yang ingin CIDRs Anda hentikan penyediaannya.
5. Pilih CIDRstab.
6. Pilih satu atau lebih CIDRs dan pilih Deprovision CIDRs.
7. Pilih Deprovision CIDR.

Command line

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

Gunakan AWS CLI perintah berikut untuk menghentikan penyediaan CIDR kumpulan:

1. Dapatkan ID kolam IPAM: describe-ipam-pools
2. Lihat arus Anda CIDRs untuk kolam renang: get-ipam-pool-cidrs

3. Penundaan: CIDRs deprovision-ipam-pool-cidr
4. Lihat pembaruan Anda CIDRs: get-ipam-pool-cidrs

Untuk menyediakan CIDR baru ke kolam renang, lihatPembuangan CIDRs dari kolam. Jika Anda ingin menghapus kolam, lihatHapus kolam.

Mengedit kolam IPAM

Anda mungkin ingin mengedit kolam untuk melakukan salah satu hal berikut:

- Ubah aturan alokasi untuk kolam renang. Untuk informasi selengkapnya tentang aturan alokasi, lihatBuat kolam tingkat atas IPv4.
- Ubah nama pool, deskripsi, atau metadata lainnya untuk meningkatkan organisasi dan visibilitas dalam IPAM.
- Ubah opsi kumpulan seperti sumber daya yang ditemukan impor otomatis untuk mengoptimalkan manajemen alamat IP otomatis IPAM.

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

AWS Management Console

Untuk mengedit kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, 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 selengkapnya tentang cakupan, lihat Bagaimana IPAM bekerja
4. Di panel konten, pilih kumpulan CIDR-nya yang ingin Anda edit.
5. Pilih Tindakan > Edit.
6. Buat perubahan apa pun yang Anda butuhkan pada kolam renang. Untuk informasi tentang opsi konfigurasi kolam, lihatBuat kolam tingkat atas IPv4.
7. Pilih Perbarui.

Command line

Gunakan AWS CLI perintah berikut untuk mengedit pool:

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

Aktifkan distribusi biaya

Ketika Anda mengaktifkan distribusi biaya, Anda mendistribusikan biaya untuk alamat IP aktif ke akun menggunakan alamat IP daripada ke pemilik IPAM. Ini berguna untuk organisasi besar di mana admin IPAM yang didelegasikan mengelola alamat IP secara terpusat menggunakan IPAM dan setiap akun bertanggung jawab atas penggunaannya sendiri, menghilangkan kebutuhan untuk perhitungan penagihan manual.

Opsi distribusi biaya tersedia saat Anda membuat IPAM atau memodifikasi IPAM dalam mode Pengukuran, di mana:

- Pemilik IPAM (default): AWS Akun yang memiliki IPAM dikenakan biaya untuk semua alamat IP aktif yang dikelola di IPAM.
- Pemilik sumber daya: AWS Akun yang memiliki alamat IP dibebankan untuk alamat IP aktif.

Persyaratan

- IPAM Anda harus terintegrasi dengan AWS Organizations.
- IPAM harus dibuat oleh admin IPAM yang didelegasikan di Organisasi Anda. AWS
- Wilayah asal IPAM harus berupa Wilayah yang diaktifkan secara default. Ini tidak bisa menjadi wilayah opt-in.

Cara kerja pengisian daya

- Meskipun Anda dapat mendistribusikan biaya alamat IP dalam suatu organisasi, semua biaya IPAM dikonsolidasikan ke akun pembayar organisasi melalui penagihan konsolidasi AWS Organisasi.
- Ketika distribusi biaya diaktifkan, akun anggota organisasi masih dapat melihat penggunaan dan biaya IPAM individu mereka dalam tagihan akun mereka.

- IPAM ARN akan muncul pada tagihan akun individu ketika distribusi biaya diaktifkan, yang memungkinkan pemilik sumber daya untuk melacak penggunaan IP aktif IPAM mereka. Jika Anda menggunakan Ekspor Data AWS, biaya IPAM muncul dengan IPAM ARN terkait dalam tagihan akun konsolidasi dan individu.
- Hanya akun dalam organisasi administrator yang didelegasikan yang dapat menerima biaya untuk sumber daya yang mereka miliki. Biaya alamat IP di luar organisasi dibebankan kepada pemilik IPAM.

Batasan waktu

- Anda memiliki waktu 24 jam untuk memilih keluar setelah memungkinkan distribusi biaya. Setelah 24 jam, Anda tidak dapat mengubah pengaturan selama 7 hari. Setelah 7 hari, Anda dapat menonaktifkan distribusi biaya.

Integrasikan VPC IPAM dengan infrastruktur Infoblox

Integrasi Amazon VPC IPAM dan Infoblox menghubungkan AWS VPC IP Address Manager (IPAM) Anda dengan Infoblox, memungkinkan Anda mengelola AWS alamat IP melalui alur kerja Infoblox yang ada sambil mendapatkan kemampuan cloud-native. AWS

Integrasi ini memecahkan tantangan perusahaan umum: menghindari sistem manajemen IP duplikat. Alih-alih mempelajari alat baru dan memelihara proses terpisah untuk AWS dan jaringan lokal, Anda dapat menunjuk Infoblox sebagai otoritas manajemen untuk cakupan IPAM VPC dan terus menggunakan antarmuka Infoblox yang Anda kenal untuk semua operasi alamat IP.

Ikhtisar proses integrasi

Langkah-langkah berikut memberikan gambaran umum tentang proses integrasi lengkap:

1. Konfigurasikan cakupan IPAM (dijelaskan dalam dokumen ini): Admin yang didelegasikan Amazon VPC IPAM membuat cakupan baru atau memodifikasi ruang lingkup yang ada untuk menggunakan Infoblox sebagai otoritas eksternalnya.
2. Konfigurasi Infoblox (dijelaskan di luar dokumen ini): Lihat. Langkah selanjutnya
3. Buat kumpulan tingkat atas: Admin yang didelegasikan Amazon VPC IPAM membuat kumpulan dalam cakupan yang ditautkan ke Infoblox. Kolam dimulai tanpa CIDR yang ditugaskan.
4. Penyediaan CIDR dari otoritas eksternal: Admin yang didelegasikan Amazon VPC IPAM memberikan CIDR untuk kumpulan. Anda dapat meminta CIDR yang tersedia (Infoblox memilih

dari rentang yang diizinkan) atau meminta CIDR tertentu (Infoblox menerima atau menolak berdasarkan ketersediaan). IPAM secara otomatis berkoordinasi dengan Infoblox untuk mendapatkan dan menyediakan CIDR yang disetujui.

5. Lanjutkan dengan operasi IPAM standar: Buat kumpulan anak dan VPCs dari CIDR yang dialokasikan menggunakan prosedur IPAM Amazon VPC standar.

Kapan menggunakan integrasi ini

Gunakan integrasi ini jika Anda sudah menggunakan atau berencana menggunakan Infoblox untuk manajemen jaringan lokal dan ingin memperluas praktik manajemen IP yang ada AWS tanpa mempertahankan sistem terpisah.

Prasyarat

Sebelum mengonfigurasi integrasi ini, pastikan Anda memiliki:

- VPC IPAM Tingkat Lanjut: diaktifkan di akun Anda. AWS Untuk informasi selengkapnya, lihat VPC IPAM Tingkat Lanjut.
- Izin IAM yang diperlukan: tercantum di bawah ini
- Pengidentifikasi sumber daya Infoblox: dari administrator Infoblox Anda

Peran IAM untuk Infoblox

Buat peran IAM untuk diasumsikan oleh prinsipal Infoblox, atau gunakan peran yang ada. Peran tersebut membutuhkan izin ini:

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

Untuk petunjuk tentang cara menambahkan izin ini ke peran atau kebijakan IAM, lihat Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna IAM.

> **Note**
>
> Infoblox mungkin memerlukan izin untuk penemuan VPC IPAM selain izin yang diperlukan untuk mengaktifkan integrasi ini.

Konfigurasikan integrasi Infoblox di VPC IPAM

Anda dapat mengaktifkan integrasi Infoblox saat Anda membuat atau memodifikasi cakupan di konsol AWS VPC IPAM atau. AWS CLI

> **Important**
>
> Integrasi Infoblox hanya tersedia untuk cakupan pribadi, bukan cakupan publik.

Membuat ruang lingkup baru dengan integrasi Infoblox

1. Buka konsol VPC Amazon di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, pilih IPAM, lalu pilih Scopes.
3. Pilih Buat ruang lingkup.
4. Untuk pengaturan Lingkup, lakukan hal berikut:
   - ID IPAM diisi secara otomatis.
   - (Opsional) Untuk tag Nama, masukkan nama untuk ruang lingkup.
   - (Opsional) Untuk Deskripsi, masukkan deskripsi untuk ruang lingkup.
5. Untuk Scope Authority, pilih Infoblox IPAM.
6. Untuk pengidentifikasi sumber daya Infoblox, masukkan pengidentifikasi sumber daya Infoblox dalam format. `<version>.identity.account.<entity_realm>.<entity_id>`
7. Verifikasi bahwa Anda memiliki izin IAM yang diperlukan seperti yang ditampilkan di kotak informasi.
8. Pilih Buat ruang lingkup.

AWS CLI Perintah terkait untuk ini adalah create-ipam-scope.

Memodifikasi cakupan yang ada

Untuk mengubah otoritas cakupan dari Amazon VPC IPAM ke Infoblox IPAM untuk cakupan yang ada, edit pengaturan cakupan dan ikuti langkah-langkah konfigurasi yang sama di prosedur sebelumnya.

AWS CLI Perintah terkait untuk ini adalah modify-ipam-scope.

Langkah selanjutnya

Ini melengkapi konfigurasi Amazon VPC IPAM yang diperlukan untuk integrasi. Setelah mengonfigurasi otoritas lingkup, Anda dapat membuat kumpulan IPAM tingkat atas dalam cakupan. Untuk informasi selengkapnya, lihat Buat kolam tingkat atas IPv4.

Integrasi ini juga memerlukan konfigurasi kumpulan sumber Infoblox, memverifikasi status pekerjaan penemuan, menyiapkan ruang lingkup pribadi untuk dikelola oleh Infoblox, memungkinkan manajemen Infoblox untuk Amazon VPC IPAM, dan membuat kumpulan baik dari integrasi Infoblox atau langsung dari portal Infoblox.

Untuk informasi tentang sisi integrasi Infoblox, lihat Panduan Pengguna Integrasi AWS IPAM di dokumentasi Infoblox.

Aktifkan penyediaan GUA pribadi IPv6 CIDRs

Jika Anda ingin jaringan pribadi Anda mendukung IPv6 dan tidak berniat merutekan lalu lintas dari alamat ini ke internet, Anda dapat menyediakan rentang IPv6 ULA atau GUA pribadi ke kolam IPAM dalam lingkup pribadi.

Untuk detail penting tentang IPv6 pengalamatan pribadi, lihat IPv6 Alamat pribadi di Panduan Pengguna Amazon VPC.

Ada dua jenis IPv6 alamat pribadi:

- IPv6 Rentang ULA: IPv6 alamat seperti yang didefinisikan dalam RFC4193. Rentang alamat ini akan selalu dimulai dengan “fc” atau “fd”, yang membuatnya mudah diidentifikasi. Ruang IPv6 ULA yang valid adalah apa pun di bawah fd00: :/8 yang tidak tumpang tindih dengan rentang cadangan Amazon fd00: :/16.
- IPv6 Rentang GUA: IPv6 alamat seperti yang didefinisikan dalam RFC3587. Opsi untuk menggunakan rentang IPv6 GUA sebagai IPv6 alamat pribadi dinonaktifkan secara default dan harus diaktifkan sebelum Anda dapat menggunakannya.

Untuk menggunakan rentang alamat IPv6 ULA, Anda memilih IPv6 opsi saat Anda menyediakan CIDR ke kolam IPAM dan masukkan rentang IPv6 ULA. Namun, untuk menggunakan rentang IPv6 GUA Anda sendiri sebagai IPv6 alamat pribadi, Anda harus terlebih dahulu menyelesaikan langkah-langkah di bagian ini. Opsi ini dinonaktifkan secara default.

Note

- Saat Anda menggunakan rentang IPv6 GUA pribadi, kami mengharuskan Anda menggunakan rentang IPv6 GUA yang dimiliki oleh Anda.
- IPAM menemukan sumber daya dengan alamat IPv6 ULA dan GUA dan memantau kumpulan untuk ruang alamat IPv6 ULA dan GUA yang tumpang tindih.
- Jika Anda ingin terhubung ke internet dari sumber daya yang memiliki IPv6 alamat pribadi, Anda dapat melakukannya, tetapi Anda harus merutekan lalu lintas melalui sumber daya di subnet lain dengan IPv6 alamat publik untuk mencapainya.
- Jika Anda memiliki jangkauan IPv6 GUA pribadi yang dialokasikan ke VPC, Anda tidak dapat menggunakan ruang GUA IPv6 publik yang tumpang tindih dengan ruang GUA IPv6 pribadi di VPC yang sama.
- Komunikasi antara sumber daya dengan rentang alamat IPv6 ULA dan GUA pribadi didukung (seperti di Direct Connect. Pengintip VPC, gateway transit, atau koneksi VPN).
- IPv6 Rentang GUA pribadi tidak dapat dikonversi ke rentang GUA yang diiklankan secara publik IPv6 .

AWS Management Console

Untuk mengaktifkan penyediaan GUA pribadi IPv6 CIDRs

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih IPAMs.
3. Pilih IPAM Anda dan pilih Tindakan > Edit.
4. Di bawah Private IPv6 GUA CIDRs, pilih Aktifkan penyediaan ruang GUA CIDR ke kolam IPAM pribadi IPv6 .
5. Pilih Simpan perubahan.

Command line

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

Gunakan AWS CLI perintah berikut untuk mengaktifkan penyediaan GUA pribadi IPv6 : CIDRs

1. Lihat saat ini IPAMs dengan deskripsi-ipams
2. Ubah IPAM dengan modify-ipam dan sertakan opsi untuk. `enable-private-gua`

Setelah Anda mengaktifkan opsi untuk menyediakan IPv6 GUA pribadi CIDRs, Anda dapat menyediakan IPv6 GUA CIDR pribadi ke kolam renang. Lihat informasi yang lebih lengkap di Penyediaan CIDRs ke kolam.

Menegakkan penggunaan IPAM untuk pembuatan VPC dengan SCPs

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

Bagian ini menjelaskan cara membuat kebijakan kontrol layanan AWS Organizations yang mengharuskan anggota di organisasi Anda untuk menggunakan IPAM saat mereka membuat VPC. Kebijakan kontrol layanan (SCPs) adalah jenis kebijakan organisasi yang memungkinkan Anda mengelola izin di organisasi Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .

Menegakkan IPAM saat membuat VPCs

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

Untuk membuat SCP dan membatasi pembuatan VPC ke IPAM

1. Ikuti langkah-langkah dalam Membuat kebijakan kontrol layanan di Panduan AWS Organizations Pengguna dan masukkan teks berikut di editor JSON:

   JSON

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

2. Lampirkan kebijakan ke satu atau lebih unit organisasi di organisasi Anda. Untuk informasi selengkapnya, lihat Melampirkan kebijakan dan Melepaskan kebijakan di Panduan AWS Organizations Pengguna.

Menegakkan kolam IPAM saat membuat VPCs

Ikuti langkah-langkah di bagian ini untuk meminta anggota di organisasi Anda menggunakan kumpulan IPAM tertentu saat membuat VPCs.

Untuk membuat SCP dan membatasi pembuatan VPC ke kolam IPAM

1. Ikuti langkah-langkah dalam Membuat kebijakan kontrol layanan di Panduan AWS Organizations Pengguna dan masukkan teks berikut di editor JSON:

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
```

```
        "Effect": "Deny",
        "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
        "Resource": "arn:aws:ec2:*:*:vpc/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Ipv4IpamPoolId": "ipam-pool-0123456789abcdefg"
            }
          }
    }]
}
```

2. Ubah nilai `ipam-pool-0123456789abcdefg` contoh ke ID IPv4 kumpulan yang ingin Anda batasi pengguna.
3. Lampirkan kebijakan ke satu atau lebih unit organisasi di organisasi Anda. Untuk informasi selengkapnya, lihat Melampirkan kebijakan dan Melepaskan kebijakan di Panduan AWS Organizations Pengguna.

Menegakkan IPAM untuk semua kecuali daftar yang diberikan OUs

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

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

1. Ikuti langkah-langkah dalam Membuat kebijakan kontrol layanan di Panduan AWS Organizations Pengguna dan masukkan teks berikut di editor JSON:

   JSON

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

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

2. Hapus nilai contoh (sepertio-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/) dan tambahkan jalur entitas AWS Organizations dari opsi OUs yang ingin Anda miliki (tetapi tidak memerlukan) untuk menggunakan IPAM. Untuk informasi selengkapnya tentang jalur entitas, lihat Memahami jalur entitas AWS Organizations dan aws:PrincipalOrgPaths di Panduan Pengguna IAM.
3. Lampirkan kebijakan ke root organisasi Anda. Untuk informasi selengkapnya, lihat Melampirkan kebijakan dan Melepaskan kebijakan di Panduan AWS Organizations Pengguna.

Kecualikan unit organisasi dari IPAM

Jika IPAM Anda terintegrasi dengan AWS Organizations, Anda dapat mengecualikan unit organisasi (OU) agar tidak dikelola oleh IPAM. Ketika Anda mengecualikan OU, IPAM tidak akan mengelola alamat IP di akun di OU itu. Fitur ini memberi Anda lebih banyak fleksibilitas dalam cara Anda menggunakan IPAM.

Anda dapat menggunakan pengecualian OU dengan cara berikut:

- Aktifkan IPAM untuk bagian-bagian tertentu dari bisnis Anda: Jika Anda memiliki beberapa unit bisnis atau anak perusahaan di AWS Organizations, Anda sekarang dapat menggunakan IPAM hanya untuk yang membutuhkannya.
- Pisahkan akun kotak pasir Anda: Anda dapat mengecualikan akun kotak pasir Anda dari IPAM, hanya berfokus pada akun yang benar-benar penting bagi manajemen IP Anda.

Cara kerja pengecualian OU

Diagram di bagian ini menunjukkan dua kasus penggunaan untuk menambahkan pengecualian OU di IPAM.

Diagram pertama menunjukkan dampak penambahan pengecualian unit organisasi (OU) pada OU induk saja. Akibatnya, IPAM tidak akan mengelola alamat IP di akun di OU induk. IPAM akan mengelola alamat IP di akun di sisi lain di OUs luar pengecualian.

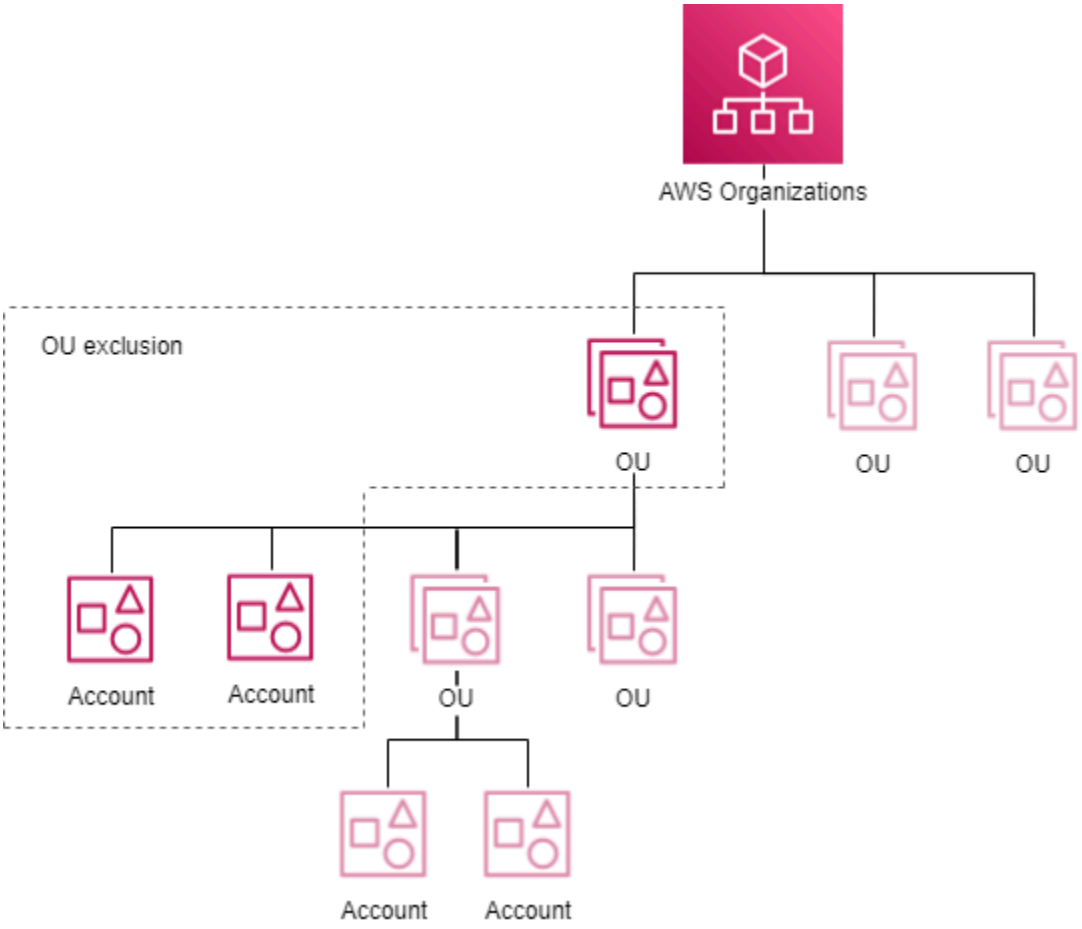
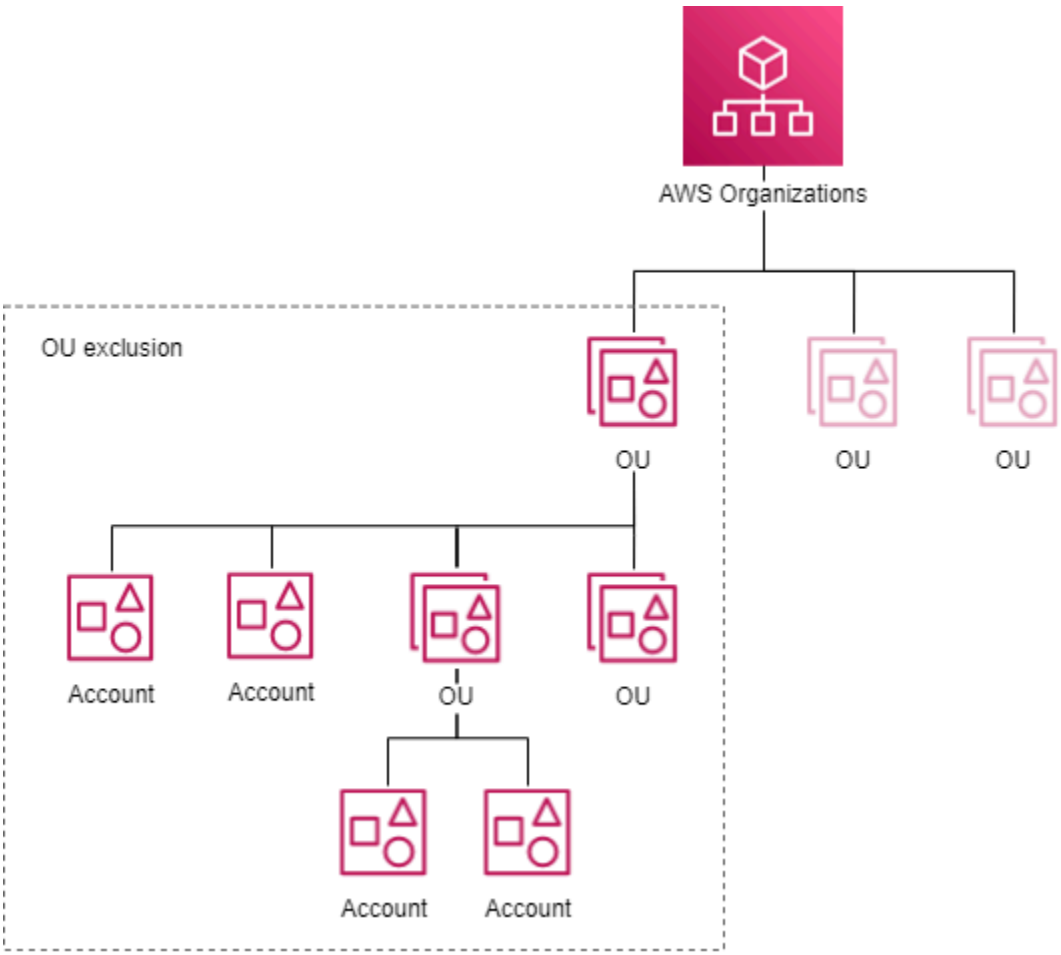


Diagram kedua menunjukkan dampak penambahan pengecualian unit organisasi (OU) pada OU orang tua dan semua anak OUs. Akibatnya, IPAM tidak akan mengelola alamat IP di akun di OU induk atau di akun pada anak OUs mana pun. IPAM akan mengelola alamat IP di akun di OUs luar pengecualian.



Menambahkan atau menghapus pengecualian OU

Selesaikan langkah-langkah di bagian ini untuk menambah atau menghapus pengecualian OU.

> **Note**
>
> - Akun admin IPAM yang didelegasikan tidak dikecualikan meskipun berada dalam OU yang dikecualikan.
> - IPAM Anda harus terintegrasi dengan AWS Organizations untuk menambahkan pengecualian OU. Organisasi harus ada OUs di dalamnya.
> - Anda harus menjadi admin IPAM yang didelegasikan untuk melihat, menambah, atau menghapus pengecualian OU.
> - Butuh waktu bagi IPAM untuk menemukan unit organisasi yang baru dibuat.

- Ada kuota default untuk jumlah pengecualian yang dapat Anda tambahkan per penemuan sumber daya. Untuk informasi selengkapnya, lihat Pengecualian unit organisasi per penemuan sumber daya diKuota untuk IPAM Anda.
- Jika Anda membagikan penemuan sumber daya dengan akun lain, akun tersebut dapat melihat pengecualian OU di dalamnya, yang berisi informasi seperti ID Org, ID Root, dan unit organisasi IDs dari Organisasi pemilik penemuan sumber daya.

AWS Management Console

Untuk menambah atau menghapus pengecualian OU

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Penemuan sumber daya.
3. Pilih penemuan sumber daya default Anda.
4. Pilih Edit.
5. Di bawah pengecualian unit Organisasi, lakukan hal berikut:
   - Untuk menambahkan pengecualian OU:
     - Jika Anda ingin mengecualikan OU dan semua anaknya OUs:
       - Temukan OU di tabel dan pilih kotak centang. Semua anak OUs dipilih secara otomatis.
     - Jika Anda ingin mengecualikan hanya akun OU induk:
       - Temukan OU di tabel dan pilih kotak centang. Semua anak OUs dipilih secara otomatis. Hapus pilihan semua anak OUs.
     - Atau, Anda dapat menggunakan kolom Tindakan untuk memilih hanya OU induk atau orang tua dan anak OUs:
       - Pilih semua anak OUs: Sertakan anak mana pun OUs dalam pengecualian. Sebagai hasil dari memilih OU, OU ditambahkan di layar. Setiap OU berisi ID dan jalur entitas dari pengecualian OU.
       - Pilih hanya OU ini: Sertakan hanya OU ini dalam pengecualian. Sebagai hasil dari memilih OU, OU ditambahkan di layar. Setiap OU berisi ID dan jalur entitas dari pengecualian OU.
       - Salin jalur entitas OU: Salin jalur entitas organisasi untuk digunakan sesuai kebutuhan.

- Jika Anda sudah mengetahui jalur entitas AWS Organizations atau Anda ingin membangunnya:
  - Pilih Masukan pengecualian unit organisasi dan masukkan jalur entitas pengecualian OU. Bangun jalur untuk OU (s) menggunakan AWS Organizations IDs dipisahkan oleh a/. Sertakan semua anak OUs dengan mengakhiri jalan dengan/*.
    - Contoh 1
      - Jalan menuju anak OU: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
      - Dalam contoh ini, `o-a1b2c3d4e5` adalah ID organisasi, `r-f6g7h8i9j0example` adalah ID root, `ou-ghi0-awsccccc` adalah ID OU, dan `ou-jkl0-awsddddd` merupakan ID OU anak.
      - IPAM tidak akan mengelola alamat IP di akun di OU anak.
    - Contoh 2
      - Jalur di mana semua anak OUs akan menjadi bagian dari pengecualian: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
      - Dalam contoh ini, IPAM tidak akan mengelola alamat IP di akun di OU (`ou-ghi0-awsccccc`) atau di akun di mana pun OUs yang merupakan anak-anak dari OU.
- Untuk menghapus pengecualian OU:
  - Pilih X di sebelah OU yang sudah ditambahkan. /*Setelah ID OU menunjukkan bahwa itu adalah OU orang tua dan anak itu OUs adalah bagian dari pengecualian OU.

6. Pilih Simpan perubahan.

Command line

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

1. Lihat detail penemuan sumber daya untuk mendapatkan ID penemuan sumber daya default untuk langkah berikutnya describe-ipam-resource-discoveries.

   Masukan:

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

   Output:

```
{

    "IpamResourceDiscoveries": [

        {

            "OwnerId": "111122223333",

            "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",

            "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-
resource-discovery/ipam-res-disco-1234567890abcdef0",
            "IpamResourceDiscoveryRegion": "us-east-1",

            "OperatingRegions": [

                {

                    "RegionName": "us-east-1"

                },

                {

                    "RegionName": "us-west-1"

                },

                {

                    "RegionName": "us-west-2"

                }

            ],

            "IsDefault": true,

            "State": "modify-complete",

            "Tags": []
```

```
        }

    ]

}
```

2. Menambahkan atau menghapus pengecualian unit organisasi dari penemuan sumber daya dengan modify-ipam-resource-discoverydan `--add-organizational-unit-exclusions` atau `--remove-organizational-unit-exclusions` opsi. Anda harus memasukkan jalur entitas AWS Organizations. Bangun jalur untuk OU (s) menggunakan AWS Organizations IDs dipisahkan oleh a/. Sertakan semua anak OUs dengan mengakhiri jalan dengan/*. Anda tidak dapat menyertakan jalur entitas yang sama lebih dari sekali dalam menambah atau menghapus parameter.

   - Contoh 1
     - Jalan menuju anak OU: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
     - Dalam contoh ini, `o-a1b2c3d4e5` adalah ID organisasi, `r-f6g7h8i9j0example` adalah ID root, `ou-ghi0-awsccccc` adalah ID OU, dan `ou-jkl0-awsddddd` merupakan ID OU anak.
     - IPAM tidak akan mengelola alamat IP di akun di OU anak.
   - Contoh 2
     - Jalur di mana semua anak OUs akan menjadi bagian dari pengecualian: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
     - Dalam contoh ini, IPAM tidak akan mengelola alamat IP di akun di OU (`ou-ghi0-awsccccc`) atau di akun di mana pun OUs yang merupakan anak-anak dari OU.

   > **Note**
   >
   > Kumpulan pengecualian yang dihasilkan tidak boleh “tumpang tindih”, yang berarti dua atau lebih pengecualian OU tidak boleh mengecualikan OU yang sama. Contoh jalur entitas yang tidak tumpang tindih:
   >
   > - Jalur 1 ="o-1/r-1/ou-1/”
   > - Jalur 2 ="o-1/r-1/ou-1/ou-2/”

Jalur ini tidak tumpang tindih karena Path 1 hanya mengecualikan akun di bawah ou-1 dan Path 2 hanya mengecualikan akun di bawah ou-2.
Contoh jalur entitas yang tumpang tindih:

- Jalur 1 ="o-1/r-1/ou-1/*”
- Jalur 2 ="o-1/r-1/ou-1/ou-2/”

Jalur ini tumpang tindih karena Jalur 1 mewakili “o-1/r-1/ou-1/” dan “o-1/r-1/ou-1/ou-2/”, dan “o-1/r-1/ou-1/ou-2/” tumpang tindih dengan Path 2.

Masukan:

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

Output:

```
{
    "IpamResourceDiscovery": {
        "OwnerId": "111122223333",
        "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-resource-
discovery/ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryRegion": "us-east-1",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "IsDefault": false,
        "State": "modify-in-progress",
        "OrganizationalUnitExclusions": [
            {
```

```
                "OrganizationsEntityPath": "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-
ghi0-awsccccc/*"
            }
        ]
    }
}
```

Ubah tingkat IPAM

IPAM menawarkan dua tingkatan: Tingkat Gratis dan Tingkat Lanjut. Beralih ke Tingkat Lanjut Manajer Alamat IP VPC Amazon memberikan kontrol yang lebih terperinci atas manajemen alamat IP Anda. Ini dapat bermanfaat karena kompleksitas jaringan Anda tumbuh, memungkinkan Anda untuk mengoptimalkan dan mengelola ruang alamat IP Anda dengan lebih baik. 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.

> **Note**
>
> 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.

> **Note**
>
> Jika Anda berada di Tingkat Gratis, Anda akan melihat perkiraan jumlah IP aktif IPAM Anda adalah... .
> Total jumlah IP aktif adalah jumlah alamat IP aktif di IPAM Anda yang akan dikenakan biaya jika Anda beralih dari Tingkat Gratis ke Tingkat Lanjut. Alamat IP aktif didefinisikan sebagai alamat IP atau awalan yang terkait dengan Antarmuka Jaringan Elastis (ENI) yang dilampirkan ke sumber daya seperti Instans EC2.
>
> - Metrik ini hanya tersedia untuk pelanggan di Tingkat Gratis.
> - Jika IPAM Anda terintegrasi dengan AWS Organizations, jumlah IP aktif mencakup semua akun Organisasi.
> - Anda tidak dapat melihat rincian jumlah IP aktif berdasarkan jenis IP (public/private) or class (IPv4/IPv6).
> - IPAM hanya dihitung IPs dari yang ENIs dimiliki oleh akun yang dipantau. Hitungannya mungkin tidak akurat untuk subnet bersama. Alamat IP dikecualikan jika pemilik subnet atau pemilik ENI tidak dicakup oleh IPAM.

5. Pilih tingkat IPAM yang ingin Anda gunakan untuk IPAM.
6. Pilih Simpan perubahan.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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 saat ini IPAMs: deskripsikan-ipams
2. Ubah tingkat IPAM: modify-ipam
3. Lihat update Anda IPAMs: describe-ipams

Ubah Wilayah operasi IPAM

Wilayah Operasi adalah AWS Wilayah di mana IPAM diizinkan untuk mengelola alamat CIDRs IP. IPAM hanya menemukan dan memantau sumber daya di AWS Wilayah yang Anda pilih sebagai Wilayah operasi.

Menambahkan wilayah operasi ke IPAM memungkinkan Anda mengelola ruang alamat IP di beberapa AWS Wilayah. Ini dapat meningkatkan pemanfaatan alamat IP, memungkinkan segmentasi regional, dan mendukung infrastruktur yang didistribusikan secara geografis. Memperluas cakupan Regional IPAM memberikan fleksibilitas dan kontrol yang lebih besar atas manajemen alamat IP Anda secara keseluruhan.

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 Simpan perubahan.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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 saat ini IPAMs: deskripsikan-ipams
2. Menambah atau menghapus Kawasan operasi IPAM: modify-ipam
3. Lihat update Anda IPAMs: describe-ipams

Penyediaan CIDRs ke kolam

Ikuti langkah-langkah di bagian ini untuk menyediakan CIDRs ke kolam. Jika Anda sudah menyediakan CIDR saat membuat pool, Anda mungkin perlu menyediakan tambahan CIDRs jika pool mendekati alokasi penuh. Untuk memantau penggunaan kolam renang, lihatPantau 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 VPC atau alamat IP Elastis.

AWS Management Console

Untuk penyediaan CIDRs ke kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, 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, lihatBagaimana IPAM bekerja.
4. Di panel konten, pilih kumpulan tempat Anda ingin menambahkan CIDR.
5. Pilih Tindakan > Ketentuan CIDRs.
6. Lakukan salah satu tindakan berikut:
   - Jika Anda menyediakan CIDR ke kolam di ruang lingkup publik, masukkan Netmask.
   - Jika Anda menyediakan CIDR ke IPv4 kolam dalam lingkup pribadi, masukkan CIDR.
   - Jika Anda menyediakan CIDR ke IPv6 kolam dalam lingkup pribadi, perhatikan hal berikut:
     - Untuk detail penting tentang IPv6 pengalamatan pribadi, lihat IPv6 Alamat pribadi di Panduan Pengguna Amazon VPC.
     - Untuk menggunakan rentang IPv6 ULA pribadi, di bawah CIDRsketentuan, pilih Tambahkan ULA CIDR oleh netmask dan pilih ukuran netmask atau pilih Input IPv6 CIDR pribadi dan masukkan rentang ULA. Rentang yang valid untuk IPv6 ULA pribadi adalah /9 hingga /60 dimulai dengan fd80: :/9.

- Untuk menggunakan rentang IPv6 GUA pribadi, Anda harus terlebih dahulu mengaktifkan opsi pada IPAM Anda (lihatAktifkan penyediaan GUA pribadi IPv6 CIDRs). Setelah Anda mengaktifkan IPv6 GUA pribadi CIDRs, masukkan IPv6 GUA di Input IPv6 CIDR pribadi.

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

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

Command line

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

Gunakan AWS CLI perintah berikut untuk menyediakan CIDRs ke kolam:

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

Pindahkan VPC antar cakupan CIDRs

Bergerak CIDRs antar cakupan memungkinkan Anda mengoptimalkan alokasi alamat IP, mengatur berdasarkan Wilayah, memisahkan masalah, menegakkan kepatuhan, dan beradaptasi dengan

perubahan infrastruktur. Fleksibilitas ini membantu mengelola ruang alamat IP Anda secara efisien seiring dengan berkembangnya beban kerja Anda.

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

Important

- Anda hanya dapat memindahkan VPC CIDRs. Saat Anda memindahkan CIDR VPC, subnet CIDRs VPC juga dipindahkan secara otomatis.
- Anda hanya dapat memindahkan VPC CIDRs dari satu ruang lingkup pribadi ke ruang lingkup pribadi lainnya. Anda tidak dapat memindahkan VPC CIDRs dari ruang lingkup publik ke ruang lingkup pribadi atau dari ruang lingkup pribadi ke ruang lingkup publik.
- AWS Akun yang sama harus memiliki kedua cakupan.
- Jika CIDR VPC saat ini dialokasikan dari kumpulan dalam lingkup pribadi, permintaan pemindahan berhasil, tetapi CIDR VPC tidak akan dipindahkan sampai Anda merilis alokasi CIDR VPC dari kumpulan saat ini. Untuk informasi tentang merilis alokasi, lihat Melepaskan alokasi.

AWS Management Console

Untuk memindahkan CIDR yang dialokasikan ke VPC

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

Command line

Gunakan AWS CLI perintah berikut untuk memindahkan CIDR VPC:

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

Tentukan strategi IPv4 alokasi publik dengan kebijakan IPAM

Kebijakan IPAM adalah seperangkat aturan yang menentukan bagaimana IPv4 alamat publik dari kolam IPAM dialokasikan ke sumber daya. AWS Setiap aturan memetakan AWS layanan ke kolam IPAM yang akan digunakan layanan untuk mendapatkan alamat IP. Satu kebijakan dapat memiliki beberapa aturan dan diterapkan ke beberapa AWS Wilayah. Jika pool IPAM kehabisan alamat, maka layanan akan kembali ke alamat IP yang disediakan Amazon. Kebijakan dapat diterapkan ke AWS akun individu atau entitas dalam AWS Organizations. Jika Anda membawa IP Anda sendiri (BYOIP), ini membantu mengurangi biaya AWS publik IPv4 Anda.

Kapan menggunakan kebijakan IPAM

Gunakan kebijakan IPAM untuk:

- Mengurangi IPv4 biaya publik dengan menggunakan alamat BYOIP
- Kontrol secara terpusat IP mana yang digunakan AWS sumber daya Anda
- Pastikan alokasi IP yang konsisten di seluruh organisasi Anda

Cara kerjanya

Saat Anda membuat AWS sumber daya yang memerlukan alamat IP publik di akun dengan kebijakan IPAM diberlakukan:

- IPAM memeriksa aturan kebijakan Anda secara berurutan.
- Jika aturan cocok dengan jenis sumber daya, IPAM mengalokasikan IP dari kumpulan yang ditentukan.
- Jika pool kosong dan overflow diaktifkan, Amazon memberikan alamat IP.
- Jika tidak ada aturan yang cocok, perilaku default berlaku.

Layanan dan sumber daya yang didukung

Anda dapat membuat kebijakan IPAM untuk menentukan bagaimana IPv4 alamat publik dari kumpulan IPAM dialokasikan ke AWS layanan dan sumber daya berikut:

- Alamat IP elastis (EIPs)
- Aplikasi Load Balancer () ALBs
- Amazon Relational Database Service (RDS)
- Gerbang NAT regional

> **Important**
>
> Jika Anda memilih kumpulan IPAM atau ID alokasi EIP tertentu saat membuat AWS sumber daya, itu akan menggantikan kebijakan IPAM.

Prasyarat

- IPAM di akun administrator yang didelegasikan dengan tingkat lanjutan diaktifkan
- Kolam IPAM publik dengan alamat IPv4
- Izin IAM untuk operasi IPAM dan EC2

Terminologi

Kebijakan IPAM

Kebijakan IPAM adalah seperangkat aturan yang menentukan bagaimana IPv4 alamat publik dari kolam IPAM dialokasikan ke sumber daya. AWS Setiap aturan memetakan AWS layanan ke kolam IPAM yang akan digunakan layanan untuk mendapatkan alamat IP. Satu kebijakan dapat memiliki beberapa aturan dan diterapkan ke beberapa AWS Wilayah. Jika pool IPAM kehabisan alamat, maka layanan akan kembali ke alamat IP yang disediakan Amazon. Kebijakan dapat diterapkan ke AWS akun individu atau entitas dalam AWS Organizations. Kebijakan dapat diterapkan ke AWS akun individu atau entitas dalam AWS Organizations.

Aturan Alokasi

Konfigurasi opsional dalam kebijakan IPAM yang memetakan jenis AWS sumber daya ke kolam IPAM tertentu. Jika tidak ada aturan yang ditentukan, jenis sumber daya akan kembali ke penggunaan alamat IP yang disediakan Amazon.

Target

AWS Akun individu atau entitas dalam AWS Organisasi tempat kebijakan IPAM dapat diterapkan.

Langkah 1: Buat kebijakan IPAM

Menggunakan AWS Konsol:

Ikuti langkah-langkah berikut untuk membuat kebijakan IPAM menggunakan AWS Konsol:

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi di sebelah kiri, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Masukkan Nama untuk kebijakan Anda (opsional).
5. Pilih IPAM untuk dikaitkan dengan kebijakan ini.
6. (Opsional) Tambahkan tanda.
7. Pilih Buat kebijakan.

Menggunakan AWS CLI:

Gunakan perintah create-ipam-policy.

Langkah 2: Tambahkan aturan alokasi

Setelah membuat kebijakan, Anda perlu menambahkan aturan alokasi yang menentukan bagaimana alamat IP dialokasikan:

Menggunakan AWS Konsol:

Ikuti langkah-langkah berikut untuk menambahkan aturan alokasi menggunakan AWS Konsol:

1. Di panel navigasi di sebelah kiri, pilih Kebijakan.
2. Pilih kebijakan yang Anda buat di langkah sebelumnya.
3. Di halaman detail kebijakan, pilih tab Aturan alokasi.
4. Pilih Buat aturan alokasi.
5. Konfigurasikan konfigurasi Layanan:

    - Lokal: Pilih AWS Wilayah (us-east-1) atau Zona Lokal tempat Anda ingin kebijakan ini berlaku.
    - Jenis sumber daya: Pilih jenis AWS layanan atau sumber daya untuk kebijakan ini (Alamat IP elastis, instans database RDS, Application Load Balancers, atau gateway NAT dalam mode ketersediaan regional).

6. Konfigurasikan konfigurasi Aturan:
    - Kolam IPAM: Pilih kolam IPAM yang akan memberikan alamat IP.
    - Tinjau detail kumpulan (lokal, sumber IP publik, ruang yang tersedia, dan rentang CIDR tersedia).
7. (Opsional) Pilih Tambahkan aturan baru untuk membuat aturan tambahan.
8. Pilih Buat aturan alokasi.

Menggunakan AWS CLI:

Gunakan perintah modify-ipam-policy-allocation-rules.

Langkah 3: Aktifkan kebijakan

Tentukan akun mana yang harus menggunakan kebijakan ini.

Menggunakan AWS Konsol:

Ikuti langkah-langkah berikut untuk mengaktifkan kebijakan menggunakan AWS Konsol:

1. Di halaman detail kebijakan, pilih tab Target.
2. Pilih Kelola target kebijakan.
3. Lakukan salah satu tindakan berikut:
    - Untuk penggunaan akun tunggal (IPAM tidak terintegrasi dengan AWS Organizations), pilih Aktifkan untuk akun Anda.
    - Untuk IPAM yang terintegrasi dengan AWS Organizations (ketika Anda adalah admin yang didelegasikan):
        - Di bagian Struktur organisasi, pilih akun atau unit organisasi tempat Anda ingin menerapkan kebijakan ini.
        - Centang kotak Diaktifkan untuk setiap target.
        - Pilih Simpan Perubahan.
        - Penting: Mengaktifkan kebijakan ini akan menggantikan kebijakan IPAM aktif apa pun pada akun atau unit organisasi yang dipilih.

Menggunakan AWS CLI:

Gunakan enable-ipam-policyperintah berdasarkan pengaturan Anda:

Untuk penggunaan akun tunggal (IPAM tidak terintegrasi dengan AWS Organizations):

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

Untuk IPAM yang terintegrasi dengan AWS Organizations (ketika Anda adalah admin yang didelegasikan), tetapkan kebijakan untuk menargetkan akun di AWS Organisasi:

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

Untuk IPAM yang terintegrasi dengan AWS Organizations (ketika Anda adalah admin yang didelegasikan), tetapkan kebijakan untuk menargetkan unit organisasi:

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

Important

Mengaktifkan kebijakan ini akan menggantikan kebijakan IPAM aktif pada akun atau unit organisasi yang dipilih.

Langkah 4: Uji kebijakan Anda

Buat sumber daya baru dari jenis yang Anda konfigurasikan (seperti EIP) di salah satu akun target. Sumber daya akan secara otomatis menggunakan alamat IP dari kolam IPAM Anda.

Important

Jika Anda memilih kumpulan IPAM atau ID alokasi EIP tertentu saat membuat AWS sumber daya, itu akan menggantikan kebijakan IPAM.

Langkah 5: Pantau penggunaan

Periksa kolam IPAM Anda di konsol untuk melihat alamat IP dialokasikan ke sumber daya Anda.

Lepaskan alokasi

Jika Anda berencana untuk menghapus pool, Anda mungkin perlu merilis alokasi pool. Alokasi adalah tugas CIDR dari kolam IPAM ke sumber daya lain atau kolam IPAM.

Anda tidak dapat menghapus pool jika pool telah CIDRs disediakan, dan Anda tidak dapat membatalkan penyediaan CIDRs jika dialokasikan ke sumber CIDRs daya.

Note

- Untuk merilis alokasi manual, gunakan langkah-langkah di bagian ini atau hubungi ReleaseIpamPoolAllocation API.
- Untuk merilis alokasi dalam lingkup pribadi, Anda harus mengabaikan atau menghapus CIDR sumber daya. Untuk informasi selengkapnya, lihat Ubah status pemantauan VPC CIDRs. 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 kolam IPAM.
- Untuk merilis alokasi dalam lingkup publik, Anda harus menghapus CIDR sumber daya. Anda tidak dapat mengabaikan sumber daya publik CIDRs. Untuk informasi selengkapnya, lihat Pembersihan di Bawa IPv4 CIDR publik Anda sendiri ke IPAM hanya menggunakan CLI AWS atau Pembersihan di. Bawa 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 baik untuk penggunaan satu akun atau penggunaan multi-akun.

Saat Anda merilis CIDR yang dikelola oleh IPAM Anda, Amazon VPC IPAM mendaur ulang CIDR kembali ke kolam IPAM. Jika Anda menggunakan IPAM di Tingkat Lanjut, dibutuhkan beberapa menit agar CIDR tersedia untuk alokasi masa depan. Jika Anda menggunakan IPAM di Tingkat Gratis, CIDR akan memakan waktu hingga 48 jam agar CIDR tersedia untuk alokasi masa depan. Untuk informasi selengkapnya tentang kumpulan dan alokasi, lihatBagaimana IPAM bekerja.

AWS Management Console

Untuk merilis alokasi kolam

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Dari menu tarik-turun di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatBagaimana IPAM bekerja.
4. Di panel konten, pilih kumpulan tempat alokasi berada.
5. Pilih tab Alokasi.
6. Pilih satu atau lebih alokasi. Anda dapat mengidentifikasi alokasi berdasarkan jenis Sumber Daya mereka:
   - kustom: Sebuah alokasi kustom.
   - vpc: Alokasi VPC.
   - ipam-pool: Alokasi kolam IPAM.
   - ec2-public-ipv4-pool: Alokasi kolam renang umum. IPv4
   - subnet: Alokasi subnet.
7. Pilih Tindakan > Lepaskan alokasi kustom.
8. Pilih Deallocate CIDR.

Command line

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

Gunakan AWS CLI perintah berikut untuk melepaskan alokasi pool:

1. Dapatkan ID kolam IPAM: describe-ipam-pools
2. Lihat alokasi Anda saat ini di kolam: 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 CIDRs dari kolam IPAM. Untuk menghapus pool setelah merilis alokasi, Anda harus terlebih dahulu. Pembuangan CIDRs dari kolam

Bagikan kolam IPAM menggunakan AWS RAM

Ikuti langkah-langkah di bagian ini untuk berbagi kolam IPAM menggunakan AWS Resource Access Manager (RAM). Ketika Anda berbagi kolam IPAM dengan RAM, “prinsipal” dapat mengalokasikan CIDRs dari kolam ke AWS sumber daya, seperti VPCs, dari akun masing-masing. Principal adalah konsep dalam RAM yang berarti setiap AWS akun, peran IAM atau unit AWS organisasi dalam Organizations. Untuk informasi selengkapnya, lihat Berbagi AWS sumber daya Anda di Panduan Pengguna AWS RAM.

> **Note**
>
> - Anda hanya dapat berbagi kolam IPAM dengan AWS RAM jika Anda telah mengintegrasikan IPAM dengan Organizations AWS . Untuk informasi selengkapnya, lihat Integrasikan IPAM dengan akun di Organisasi AWS. Anda tidak dapat berbagi kolam IPAM dengan AWS RAM jika Anda adalah pengguna IPAM akun tunggal.
> - Anda harus mengaktifkan berbagi sumber daya dengan AWS Organizations dalam AWS RAM. Untuk informasi selengkapnya, lihat Mengaktifkan berbagi sumber daya dalam AWS Organizations dalam Panduan Pengguna AWS RAM.
> - Berbagi RAM hanya tersedia di AWS wilayah asal IPAM Anda. Anda harus membuat bagian di AWS Wilayah tempat IPAM berada, bukan di Wilayah kolam IPAM.
> - Akun yang membuat dan menghapus saham sumber daya kumpulan IPAM harus memiliki izin berikut dalam kebijakan IAM yang dilampirkan pada peran IAM mereka:
>   - `ec2:PutResourcePolicy`
>   - `ec2:DeleteResourcePolicy`
> - Anda dapat menambahkan beberapa kolam IPAM ke berbagi RAM.
> - Meskipun Anda dapat berbagi kumpulan IPAM dengan AWS akun apa pun di luar AWS Organisasi, IPAM hanya akan memantau alamat IP di akun di luar Organisasi jika pemilik akun telah melalui proses berbagi penemuan sumber daya mereka dengan admin IPAM

yang didelegasikan seperti yang dijelaskan dalam. Integrasikan IPAM dengan akun di luar organisasi Anda

AWS Management Console

Untuk berbagi kolam IPAM menggunakan RAM

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools.
3. Secara default, 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, lihatBagaimana IPAM bekerja.
4. Di panel konten, pilih kumpulan yang ingin Anda bagikan dan pilih Tindakan > Lihat detail.
5. Di bawah Berbagi sumber daya, pilih Buat berbagi sumber daya. Akibatnya, konsol AWS RAM terbuka. Anda akan membuat kolam bersama di AWS RAM.
6. Pilih Buat berbagi sumber daya.
7. Tambahkan Nama untuk sumber daya bersama.
8. Di bawah Pilih jenis sumber daya, pilih kolam IPAM dan pilih satu atau beberapa kolam IPAM.
9. Pilih Berikutnya.
10. Pilih salah satu izin untuk berbagi sumber daya:
    - AWSRAMDefaultPermissionsIpamPool: Pilih izin ini untuk mengizinkan prinsipal melihat CIDRs dan alokasi di kolam IPAM bersama dan di kolam renang. allocate/release CIDRs
    - AWSRAMPermissionIpamPoolByoipCidrImport: Pilih izin ini untuk mengizinkan prinsipal mengimpor BYOIP CIDRs ke kolam IPAM bersama. Anda akan memerlukan izin ini hanya jika Anda memiliki BYOIP yang ada CIDRs dan Anda ingin mengimpornya ke IPAM dan membagikannya dengan kepala sekolah. Untuk informasi tambahan tentang BYOIP CIDRs ke IPAM, lihat. Tutorial: Transfer IPv4 CIDR BYOIP ke IPAM
11. Pilih prinsipal yang diizinkan untuk mengakses sumber daya ini. Jika prinsipal akan mengimpor BYOIP yang ada CIDRs ke kolam IPAM bersama ini, tambahkan akun pemilik CIDR BYOIP 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 Referensi AWS CLI Perintah. Di sana Anda akan menemukan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

Gunakan AWS CLI perintah berikut untuk berbagi kolam IPAM menggunakan RAM:

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

Sebagai hasil dari menciptakan pembagian sumber daya dalam RAM, prinsipal lain sekarang dapat mengalokasikan CIDRs ke sumber daya menggunakan kolam IPAM. Untuk informasi tentang pemantauan sumber daya yang dibuat oleh kepala sekolah, lihat. Memantau 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.

Bekerja dengan penemuan sumber daya

Penemuan sumber daya adalah komponen IPAM yang memungkinkan IPAM untuk mengelola dan memantau sumber daya milik akun yang memiliki penemuan sumber daya. Ini memungkinkan IPAM untuk mempertahankan up-to-date inventaris penggunaan alamat IP di seluruh beban kerja Anda, memfasilitasi manajemen dan perencanaan alamat IP.

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 Anda Jika Anda tidak membuat IPAM dan mengintegrasikannya dengan akun di luar organisasi Anda, Anda tidak perlu membuat, berbagi, atau mengaitkan penemuan sumber daya.

Perhatikan bahwa bagian ini adalah pengelompokan prosedur yang semuanya terkait dengan bekerja dengan penemuan sumber daya.

Daftar Isi

Buat penemuan sumber daya untuk diintegrasikan dengan IPAM lain

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 Anda 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 Manajer 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. Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag 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 Buat.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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

Melihat detail penemuan sumber daya di AWS IPAM dapat memberikan wawasan berharga, seperti:

- Mengidentifikasi AWS sumber daya spesifik yang telah diimpor dan alokasi alamat IP terkait.

- Memantau status dan kemajuan proses penemuan sumber daya.
- Memecahkan masalah atau perbedaan apa pun antara IPAM dan sumber daya yang ditemukan.
- Menganalisis penggunaan dan tren alamat IP.

Informasi ini dapat membantu Anda mengoptimalkan manajemen alamat IP Anda dan memastikan keselarasan antara IPAM dan penerapan sumber daya Anda yang sebenarnya.

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 CIDRs dari jenis sumber daya berikut, IPv4 kolam Publik VPCs, subnet VPC, dan alamat IP Elastis.
     - Nama (ID Sumber Daya) — ID penemuan sumber daya.
     - IPs dialokasikan — Persentase ruang alamat IP yang digunakan. Untuk mengubah desimal menjadi persentase, kalikan desimal dengan 100. Perhatikan hal berikut:
       - Untuk sumber daya yang ada VPCs, ini adalah persentase ruang alamat IP di VPC yang diambil oleh subnet. CIDRs
       - Untuk sumber daya yang merupakan subnet, jika subnet memiliki IPv4 CIDR yang disediakan untuk itu, ini adalah persentase ruang IPv4 alamat di subnet yang digunakan. Jika subnet memiliki IPv6 CIDR yang disediakan untuk itu, persentase ruang IPv6 alamat yang digunakan tidak diwakili. Persentase ruang IPv6 alamat yang digunakan saat ini tidak dapat dihitung.
       - Untuk sumber daya yang merupakan IPv4 kolam publik, ini adalah persentase ruang alamat IP di kolam yang telah dialokasikan ke alamat IP Elastic (EIPs).

    - 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 pembagian sumber daya terdaftar.
    - Pembagian sumber daya ARN — Pembagian sumber daya ARN.
    - Status — Status saat ini dari pembagian sumber daya. Kemungkinan nilainya 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 tag 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 Referensi AWS CLI Perintah. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

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

Bagikan penemuan sumber daya dengan AWS akun lain

Ikuti langkah-langkah di bagian ini untuk membagikan penemuan sumber daya menggunakan AWS Resource Access Manager. Untuk informasi selengkapnya AWS 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 Anda 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 membagikan penemuan sumber daya dengan akun lain, akun tersebut dapat melihat pengecualian OU apa pun di dalamnya, yang berisi informasi seperti ID Org, ID Root, dan unit organisasi IDs dari Organisasi pemilik 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.

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 RAM Konsol 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 Berikutnya.
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 Berikutnya.
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 Mengaitkan penemuan sumber daya dengan IPAM.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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

Mengaitkan 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 sumber daya CIDRs 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 Anda 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 Referensi AWS CLI Perintah. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

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

Pisahkan 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 sumber daya CIDRs 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 Referensi AWS CLI Perintah. 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 Referensi AWS CLI Perintah. Dokumentasi memberikan deskripsi rinci tentang opsi yang dapat Anda gunakan saat menjalankan perintah.

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

Melacak penggunaan alamat IP di IPAM

Amazon VPC IP Address Manager menawarkan fitur pelacakan penggunaan alamat IP yang dapat bermanfaat bagi siapa saja yang mengelola lingkungan jaringan yang kompleks. IPAM memberikan visibilitas ke alokasi alamat IP, pemanfaatan, dan tren konsumsi di seluruh. AWS Ini membantu Anda mengidentifikasi alamat IP yang tidak digunakan atau tidak efisien digunakan, optimalisasi ruang alamat dan mencegah potensi kelelahan alamat IP.

IPAM melacak penggunaan alamat IP di tingkat CIDR, ruang lingkup, dan IPAM, memberikan pelaporan dan analitik terperinci. Ini berharga untuk penerapan skala besar, pengaturan multi-akun, dan persyaratan jaringan yang berkembang.

Dengan memanfaatkan pelacakan penggunaan IPAM, Anda dapat membuat keputusan berdasarkan informasi, meningkatkan manajemen alamat IP, dan memastikan pemanfaatan sumber daya IP yang efisien.

> **Note**
>
> Tugas yang dijelaskan dalam bagian ini adalah opsional. Jika Anda ingin menyelesaikan tugas di bagian ini, dan Anda telah mendelegasikan akun IPAM, tugas harus diselesaikan oleh akun IPAM.

Konten

Pantau penggunaan CIDR dengan dasbor IPAM

Dasbor IPAM di Amazon VPC IP Address Manager memungkinkan Anda memantau penggunaan CIDR untuk beberapa skenario utama:

- Identifikasi ruang alamat IP yang tidak digunakan atau kurang dimanfaatkan: Dasbor menyediakan visibilitas ke dalam pemanfaatan CIDR, memungkinkan Anda mengidentifikasi CIDRs dengan kapasitas yang tersedia yang dapat direklamasi atau dialokasikan kembali.
- Optimalkan manajemen alamat IP: Dengan melacak penggunaan CIDR dengan cermat, Anda dapat membuat keputusan berdasarkan informasi tentang memperluas, mengontrak, atau menetapkan kembali blok alamat IP untuk memenuhi persyaratan bisnis dan infrastruktur yang berubah.
- Mencegah kelelahan alamat IP: Memantau penggunaan CIDR membantu Anda mengantisipasi kapan Anda mungkin perlu memperoleh ruang alamat IP tambahan, memungkinkan Anda untuk secara proaktif merencanakan dan menghindari gangguan layanan karena penipisan alamat IP.
- Pastikan kepatuhan dan tata kelola: Dasbor IPAM dapat membantu Anda mendemonstrasikan pola penggunaan alamat IP untuk memenuhi persyaratan peraturan atau kebijakan internal seputar manajemen alamat IP.
- Memecahkan masalah jaringan: Data penggunaan CIDR terperinci dapat membantu mengidentifikasi akar penyebab masalah konektivitas jaringan atau konflik sumber daya.

Dengan memantau penggunaan CIDR secara ketat melalui dasbor IPAM, Anda dapat meningkatkan efisiensi, ketahanan, dan kepatuhan manajemen alamat IP Anda di dalamnya. AWS

AWS Management Console

Untuk memantau penggunaan CIDR menggunakan dasbor IPAM

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Dasbor.
3. Secara default, saat Anda melihat dasbor, 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, lihatBagaimana IPAM bekerja.
4. Dasbor menyajikan ikhtisar kolam IPAM Anda dan CIDRs dalam ruang lingkup. Anda dapat menambahkan, menghapus, mengubah ukuran, dan memindahkan widget untuk menyesuaikan dasbor.

    - Lingkup: Detail untuk ruang lingkup ini. 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 Lingkup: ID untuk lingkup ini.
- Jenis lingkup: Jenis ruang lingkup.
- ID IPAM: ID IPAM tempat cakupannya berada.
- Kolam IPAM dalam lingkup ini: ID IPAM tempat cakupannya berada.
- Lihat sumber daya jaringan dalam lingkup ini: Membawa Anda ke bagian Sumber Daya pada konsol IPAM.
- Cari riwayat alamat IP dalam lingkup ini: Membawa Anda ke bagian Riwayat IP Pencarian dari konsol IPAM.

- Jenis sumber daya CIDR: Jenis sumber daya CIDRs dalam ruang lingkup.
  - Subnet: Jumlah CIDRs untuk subnet.
  - VPC: Jumlah untuk. CIDRs VPCs
  - EIPs: Jumlah CIDRs untuk alamat IP Elastis.
  - IPv4 Kolam renang umum: Jumlah CIDRs untuk IPv4 kolam renang umum.
- Status manajemen: Keadaan manajemen CIDRs.
  - Tidak dikelola CIDRs: Jumlah sumber daya CIDRs untuk sumber daya yang tidak dikelola dalam lingkup ini.
  - Diabaikan CIDRs: Jumlah sumber daya CIDRs yang telah Anda pilih untuk dibebaskan dari pemantauan dengan IPAM dalam ruang lingkup. IPAM tidak mengevaluasi sumber daya yang diabaikan untuk tumpang tindih atau kepatuhan dalam suatu ruang lingkup. Ketika sumber daya dipilih untuk diabaikan, ruang apa pun 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 kumpulan).
  - Dikelola CIDRs: Jumlah sumber daya CIDRs untuk sumber daya yang dapat dikelola (VPCsatau IPv4 kolam umum) yang dialokasikan dari kolam IPAM dalam ruang lingkup.
- Sumber daya yang tumpang tindih CIDRs: Jumlah tumpang tindih dan tidak tumpang tindih. CIDRs Tumpang tindih CIDRs dapat menyebabkan perutean yang salah di Anda. VPCs
  - Tumpang tindih CIDRs: Jumlah CIDRs yang saat ini tumpang tindih dalam kolam IPAM dalam lingkup ini. Tumpang tindih CIDRs dapat menyebabkan perutean yang salah di Anda. VPCs
  - Nonoverlapping CIDRs: Jumlah sumber daya CIDRs yang tidak tumpang tindih dalam kolam IPAM dalam lingkup ini.

- Sumber daya yang sesuai CIDRs: Jumlah sumber daya yang sesuai. CIDRs
  - Sesuai CIDRs: Jumlah sumber daya CIDRs yang mematuhi aturan alokasi untuk kolam IPAM dalam ruang lingkup.
  - Noncompliant CIDRs: Jumlah sumber daya CIDRs yang tidak sesuai dengan aturan alokasi untuk kolam IPAM dalam lingkup.
- Status tumpang tindih: Jumlah tumpang CIDRs tindih dari waktu ke waktu.
  - OverlappingResourceCidrs: Jumlah tumpang CIDRs tindih dalam kolam IPAM dalam lingkup ini. Tumpang tindih CIDRs dapat menyebabkan perutean yang salah di Anda. VPCs
- Status kepatuhan: Jumlah CIDRs yang mematuhi versus tidak mematuhi aturan alokasi untuk kumpulan IPAM dalam ruang lingkup dari waktu ke waktu.
  - CompliantResourceCidrs: Jumlah sumber daya CIDRs yang mematuhi aturan alokasi.
  - NoncompliantResourceCidrs: Jumlah sumber daya CIDRs yang tidak mematuhi aturan alokasi.
- Pemanfaatan VPC: VPCs (IPv4 dan IPv6) dengan pemanfaatan IP tertinggi atau terendah. Anda dapat menggunakan informasi ini untuk mengonfigurasi CloudWatch alarm Amazon agar diperingatkan jika ambang batas penggunaan IP dilanggar. Untuk informasi selengkapnya, lihat Metrik pemanfaatan sumber daya IPAM.
- Pemanfaatan subnet: Subnet (IPv4 hanya) 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 IPAM.
- VPCs dengan IPs alokasi tertinggi: VPCs 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 file VPCs.
- Subnet dengan IPs alokasi tertinggi: Subnet yang memiliki persentase tertinggi dari ruang alamat IP dialokasikan untuk sumber daya. Ini berguna untuk menunjukkan kepada Anda jika Anda perlu menyediakan ruang alamat IP tambahan ke subnet.
- Penugasan kumpulan: 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 kolam lain dalam lingkup dari waktu ke waktu.

Command line

Informasi yang ditampilkan di dasbor berasal dari metrik yang disimpan di Amazon CloudWatch. Untuk informasi selengkapnya tentang metrik yang disimpan di Amazon CloudWatch, lihatPantau IPAM dengan Amazon CloudWatch. Gunakan CloudWatch opsi Amazon di Referensi AWS CLI untuk melihat metrik alokasi di kolam dan cakupan IPAM Anda.

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

Memantau penggunaan CIDR berdasarkan sumber daya

Tampilan Sumber Daya di Amazon VPC IP Address Manager memberikan ikhtisar terpusat pemanfaatan alamat IP di seluruh sumber daya Anda. AWS Ini memungkinkan Anda untuk dengan cepat mengidentifikasi sumber daya mana yang menggunakan alamat IP, melacak tren alokasi alamat, dan mengoptimalkan manajemen alamat IP Anda agar selaras dengan infrastruktur dan kebutuhan bisnis Anda yang terus berkembang.

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 lain, jadi penting untuk memahami perbedaan antara keduanya:

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

    > **Note**
    >
    > IPv4 Kolam renang umum dan kolam IPAM dikelola oleh sumber daya yang berbeda di AWS. Public IPv4 pool adalah sumber daya akun tunggal yang memungkinkan Anda mengonversi alamat IP milik publik CIDRs ke alamat IP Elastic. Kolam IPAM dapat digunakan untuk mengalokasikan ruang publik Anda ke kolam renang umum IPv4 .

  - VPCs

- 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:
  - Alamat IP elastis
  - IPv4 Kolam renang umum
  - VPCs
  - Subnet VPC

AWS Management Console

Untuk memantau penggunaan CIDR berdasarkan sumber daya

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Pada panel navigasi, silakan pilih Sumber Daya.
3. Dari menu tarik-turun IP di bagian atas panel konten, pilih protokol alamat IP yang ingin Anda gunakan: atau. IPv4 IPv6
4. Dari menu tarik-turun cakupan di bagian atas panel konten, pilih cakupan yang ingin Anda gunakan. Untuk informasi lebih lanjut tentang cakupan, lihatBagaimana IPAM bekerja.
5. Gunakan peta CIDR sumber daya untuk melihat ruang alamat IP yang tersedia, dialokasikan, dan tumpang-tindih dalam sebuah cakupan:
   - Tersedia: Rentang alamat IP tersedia untuk alokasi.
   - Sesuai dan tidak tumpang tindih: Rentang alamat IP dialokasikan ke sumber daya yang dikelola oleh IPAM.
   - Diisi: Rentang alamat IP dialokasikan ke sumber daya.
   - Tumpang-tindih: Rentang alamat IP telah dialokasikan ke beberapa sumber daya dan juga tumpang-tindih.
   - Tidak patuh: Rentang alamat IP tidak patuh. Ada sumber daya yang menggunakan rentang alamat IP yang tidak mematuhi aturan alokasi yang diatur untuk pool.

   Di peta CIDR, pilih blok alamat IP di bagian bawah peta untuk melihat sumber daya dalam blok CIDR yang lebih kecil. Pilih blok alamat IP di bagian atas peta untuk melihat sumber daya dalam blok CIDR yang lebih besar.

6. Dalam tabel, Anda dapat melihat detail berikut tentang sumber daya dalam cakupan:

   - Nama (ID Sumber Daya): Nama dan ID sumber daya sumber daya.
   - CIDR: CIDR yang berkaitan dengan sumber daya.
   - Status manajemen: Status sumber daya.
     - Dikelola: Sumber daya memiliki CIDR yang dialokasikan dari sebuah pool IPAM dan dipantau oleh IPAM untuk mendeteksi potensi tumpang tindih CIDR dan kepatuhan terhadap aturan alokasi pool.
     - Tidak dikelola: Sumber daya tidak memiliki CIDR yang dialokasikan dari pool IPAM dan tidak dipantau oleh IPAM untuk mendeteksi potensi kepatuhan CIDR terhadap aturan alokasi pool. CIDR dipantau untuk mendeteksi tumpang tindih.
     - Diabaikan: Sumber daya yang dipilih untuk tidak disertakan dalam pemantauan. Sumber daya yang diabaikan tidak dievaluasi terkait tumpang tindih atau kepatuhan aturan 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.
     - Patuh: Sumber daya yang dikelola mematuhi aturan alokasi pool IPAM.
     - Tidak patuh: Sumber daya CIDR tidak mematuhi satu atau beberapa aturan alokasi pool 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 pool IPAM dan tidak dipantau oleh IPAM untuk mendeteksi potensi kepatuhan CIDR terhadap aturan alokasi pool. CIDR dipantau untuk mendeteksi tumpang tindih.
     - Diabaikan: Sumber daya yang dipilih untuk tidak disertakan dalam pemantauan. Sumber daya yang diabaikan tidak dievaluasi terkait tumpang tindih atau kepatuhan aturan 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: Sumber daya CIDR tidak tumpang tindih dengan CIDR lain dalam cakupan yang sama.
    - Tumpang tindih: Sumber daya CIDR tumpang tindih dengan CIDR lain dalam cakupan yang sama. Harap diingat bahwa jika ada sumber daya CIDR yang tumpang tindih, bisa jadi sumber daya tersebut tumpang tindih dengan alokasi manual.
    - Diabaikan: Sumber daya yang dipilih untuk tidak disertakan dalam 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.
  - IPs dialokasikan: Untuk sumber daya yang ada VPCs, ini adalah persentase ruang alamat IP di VPC yang diambil oleh subnet. CIDRs Untuk sumber daya yang merupakan subnet, jika subnet memiliki IPv4 CIDR yang disediakan untuk itu, ini adalah persentase ruang IPv4 alamat di subnet yang digunakan. Jika subnet memiliki IPv6 CIDR yang disediakan untuk itu, persentase ruang IPv6 alamat yang digunakan tidak diwakili. Persentase ruang IPv6 alamat yang digunakan saat ini tidak dapat dihitung. Untuk sumber daya yang merupakan IPv4 kolam publik, ini adalah persentase ruang alamat IP di kolam yang telah dialokasikan ke alamat IP Elastic (EIPs).
  - 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 umum. IPv4
  - ID Pool: ID pool IPAM tempat sumber daya berada.
7. 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 Referensi AWS CLI Perintah. 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 sumber daya CIDRs yang mematuhi aturan alokasi) dan pemanfaatan sumber daya di namespace `AWS/IPAM` CloudWatch Amazon di Wilayah asal IPAM Anda.

Mengintegrasikan IPAM dengan CloudWatch meningkatkan kemampuan Anda untuk memantau, menganalisis, dan mengoptimalkan manajemen alamat IP Anda di dalamnya. AWS

Kasus penggunaan meliputi:

- Melacak tren pemanfaatan alamat IP: CloudWatch dapat memantau penggunaan kumpulan CIDR, alokasi ruang lingkup, dan metrik IPAM lainnya, membantu Anda secara proaktif mengidentifikasi potensi risiko kelelahan alamat IP.
- Menyetel peringatan berbasis pemanfaatan: Anda dapat mengonfigurasi CloudWatch alarm untuk memberi tahu Anda saat pemanfaatan CIDR mencapai ambang batas yang telah ditentukan, memungkinkan intervensi dan pengoptimalan tepat waktu.
- Memantau peristiwa IPAM: CloudWatch dapat menangkap dan menganalisis peristiwa terkait IPAM, seperti alokasi CIDR, deallokasi, dan modifikasi ruang lingkup, memberikan visibilitas ke dalam aktivitas manajemen alamat IP.
- Menghasilkan dasbor khusus: Dengan menggabungkan data IPAM dengan AWS metrik lain, Anda dapat membuat dasbor komprehensif untuk memvisualisasikan dan menganalisis lanskap alamat IP Anda bersama infrastruktur dan indikator kinerja terkait.

Daftar Isi

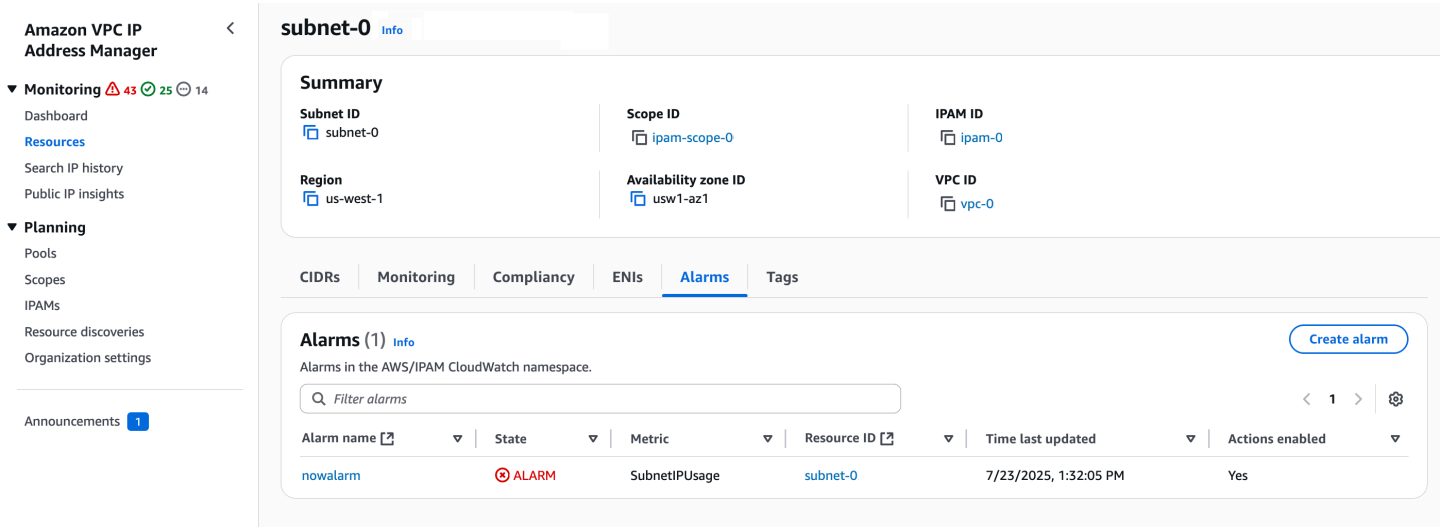
Mengelola alarm dari konsol IPAM

Anda dapat membuat dan mengelola CloudWatch alarm Amazon langsung dari konsol IPAM. Alarm untuk Metrik IPAM atau Metrik pemanfaatan sumber daya IPAM yang berada dalam status INSUFFICIENT_DATA atau ALARM akan muncul sebagai bilah peringatan di bagian atas konsol dan sebagai indikator visual di navigasi kiri di sebelah Pemantauan.

Untuk mengelola alarm untuk sumber daya tertentu, pilih Sumber Daya, lalu pilih VPC, subnet, atau kumpulan. Saat halaman detail sumber daya terbuka, pilih tab Alarm.

Tab Alarm menampilkan semua CloudWatch alarm yang terkait dengan sumber daya yang dipilih. Dari tab ini, Anda dapat melihat detail alarm, memantau status saat ini, dan mengakses opsi konfigurasi alarm. Tab menampilkan alarm dari `AWS/IPAM` namespace yang relevan dengan sumber daya yang Anda lihat.

Tangkapan layar berikut menunjukkan antarmuka manajemen alarm di konsol IPAM:



Tab Alarm memberikan ringkasan terperinci tentang CloudWatch alarm di CloudWatch namespace `AWS/IPAM` Amazon di Wilayah rumah IPAM Anda:

- Nama alarm: Nama alarm yang ditentukan pengguna. CloudWatch
- Status: Keadaan CloudWatch alarm saat ini:
  - ALARM: Metrik berada di luar ambang batas yang ditentukan.
  - OK: Metrik berada dalam ambang batas yang ditentukan.
  - INSUFFICIENT_DATA: Tidak cukup data untuk menentukan status alarm.
- Metrik: CloudWatch Metrik spesifik yang dipantau oleh alarm.

- ID Sumber Daya: Pengidentifikasi unik AWS sumber daya yang dipantau alarm.
- Waktu terakhir diperbarui: Tanggal dan waktu ketika status alarm terakhir diubah atau dievaluasi.
- Tindakan diaktifkan: Menunjukkan apakah CloudWatch tindakan diaktifkan untuk alarm:
  - Ya: Alarm dapat memicu tindakan yang dikonfigurasi ketika kondisi terpenuhi.
  - Tidak: Alarm memantau tetapi tidak menjalankan tindakan.

Selain itu, jika Anda melihat grafik pemanfaatan pada tab Monitoring untuk VPC, subnet, atau pool, Anda dapat memilih opsi untuk membuat alarm untuk pemanfaatan sumber daya. Anda kemudian diarahkan ke CloudWatch konsol dengan sumber daya dan detail metrik yang telah diisi sebelumnya. Dari sana, Anda dapat mengonfigurasi ambang alarm untuk, misalnya, diberi tahu saat pemanfaatan mencapai persentase tertentu.

Metrik IPAM

IPAM menerbitkan data tentang IPAM, kumpulan, dan cakupan 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 IPAM

`AWS/IPAM`Namespace mencakup metrik IPAM berikut.

Nama metrik	Deskripsi
TotalActiveIpCount	Total jumlah IP aktif adalah jumlah alamat IP aktif di IPAM Anda yang akan dikenakan biaya jika Anda beralih dari Tingkat Gratis ke Tingkat Lanjut. Alamat IP aktif didefinisikan sebagai alamat IP atau awalan yang terkait dengan Antarmuka Jaringan Elastis (ENI) yang dilampirkan ke sumber daya seperti EC2 Instance. • Metrik ini hanya tersedia untuk pelanggan di Tingkat Gratis.

Nama metrik	Deskripsi
	• Jika IPAM Anda terintegrasi dengan AWS Organizations, jumlah IP aktif mencakup semua akun Organisasi. • Anda tidak dapat melihat rincian jumlah IP aktif berdasarkan jenis IP (public/private) or class (IPv4/IPv6). • IPAM hanya dihitung IPs dari yang ENIs dimiliki oleh akun yang dipantau. Hitungannya mungkin tidak akurat untuk subnet bersama. Alamat IP dikecualikan jika pemilik subnet atau pemilik ENI tidak dicakup oleh IPAM.

Metrik kolam IPAM

`AWS/IPAM`Namespace menyertakan metrik kumpulan berikut untuk IPAM.

Nama metrik	Deskripsi
CompliantResourceCidrs	Jumlah sumber daya CIDRs yang dikelola yang mematuhi aturan alokasi kolam IPAM. Untuk informasi selengkapnya tentang aturan alokasi, lihatBuat kolam tingkat atas IPv4.
NoncompliantResourceCidrs	Jumlah sumber daya CIDRs yang dikelola yang tidak mematuhi aturan alokasi kolam IPAM. Untuk informasi selengkapnya tentang aturan alokasi, lihatBuat kolam tingkat atas IPv4.
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.
PercentAvailable	Persentase ruang IP pool yang belum dialokasikan ke kolam atau sumber daya lain.

Metrik cakupan IPAM

`AWS/IPAM`Namespace menyertakan metrik cakupan berikut untuk IPAM.

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

Metrik IP publik IPAM

`AWS/IPAM`Namespace mencakup metrik IP publik berikut untuk IPAM.

Nama metrik	Deskripsi
AmazonOwnedContigIPs	Jumlah alamat IP di dalamnya disediakan untuk CIDRs kolam umum bersebelahan yang disediakan Amazon yang dimiliki oleh IPAM. IPv4
AllocatedAmazonOwnedContigIPs	Jumlah alamat IP yang telah dialokasikan dari blok CIDR kolam renang publik bersebelahan yang disediakan Amazon. IPv4
UnallocatedAmazonOwnedContigIPs	Jumlah alamat IP dalam blok CIDR IPv4 kolam renang publik yang disediakan Amazon yang dimiliki oleh IPAM.
AssociatedAmazonOwnedContigIPs	Jumlah alamat IP Elastis yang telah dialokasikan dari blok CIDR IPv4 kolam publik bersebelahan yang disediakan Amazon yang terkait dengan antarmuka jaringan elastis.

Nama metrik	Deskripsi
UnassociatedAmazonOwnedContigIPs	Jumlah alamat IP Elastic yang telah dialokasikan dari blok CIDR IPv4 kolam publik bersebelahan yang disediakan Amazon yang tidak terkait dengan antarmuka jaringan elastis.

Metrik penyelesai daftar awalan IPAM

Kami mendorong Anda untuk menyetel CloudWatch alarm pada metrik kegagalan karena Anda mungkin perlu menilai kembali dan menyesuaikan aturan penyelesai daftar awalan IPAM agar tetap berada dalam batas untuk versi dan ukuran daftar awalan.

Nama metrik	Deskripsi
IpamPrefixListResolverSyncFailure	Penyelesai daftar awalan gagal disinkronkan dengan target. Ini dapat terjadi jika kuota seperti 'entri CIDR per versi penyelesai daftar awalan' terlampaui, daftar awalan target tidak ditemukan, atau sinkronisasi dinonaktifkan pada daftar awalan terkelola target.
IpamPrefixListResolverSyncSuccess	Penyelesai daftar awalan berhasil disinkronkan dengan target.
IpamPrefixListResolverVersionCreationSuccess	Pembuatan versi berhasil.
IpamPrefixListResolverVersionCreationFailure	Pembuatan versi gagal. Ini mungkin terjadi jika Anda telah mencapai kuota 'entri CIDR per versi penyelesai daftar awalan'.

Dimensi metrik

Untuk memfilter metrik IPAM, gunakan dimensi berikut.

Dimensi	Deskripsi
AddressFamily	Keluarga alamat IP untuk sumber daya CIDRs (IPv4 atau IPv6).

Dimensi	Deskripsi
Locale	AWS Wilayah di mana kolam IPAM tersedia untuk alokasi.
PooLid	ID dari sebuah kolam.
ScopeID	ID ruang lingkup.

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

Metrik pemanfaatan sumber daya IPAM

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

- VPCs (IPv4 dan IPv6)
- Subnet () IPv4
- IPv4 Kolam renang umum

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

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

- 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 VPCs 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 IPv4 kolam umum 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 AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS

Example Contoh

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

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

Metrik VPC

Nama dan deskripsi metrik VPC tercantum di bawah ini.

Nama metrik	Deskripsi
Vpc IPUsage	Total yang IPs tercakup CIDRs dalam subnet VPC dibagi dengan total yang IPs dicakup oleh CIDRs dalam VPC. Ini dihitung di semua VPC CIDRs dalam Lingkup IPAM yang sama dan secara terpisah untuk dan. IPv4 IPv6 CIDRs

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

Dimensi	Deskripsi
AddressFamily	Keluarga alamat IP untuk sumber daya CIDRs (IPv4 atau IPv6).
OwnerID	ID pemilik VPC.
Region	AWS Wilayah 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
Subnet IPUsage	Jumlah aktif IPs dibagi dengan total IPs dalam IPv4 CIDR subnet.

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

Dimensi	Deskripsi
AddressFamily	Keluarga alamat IP untuk sumber daya CIDRs (IPv4 hanya).
OwnerID	ID pemilik subnet.
Region	AWS Wilayah tempat subnet berada.
ScopeID	ID lingkup IPAM yang dimiliki subnet.
SubnetID	ID subnet.
VPCid	ID VPC yang dimiliki subnet.

Metrik IPv4 kolam renang umum

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

Nama metrik	Deskripsi
Kolam IPv4 Renang Umum IPUsage	Jumlah EIPs dari IPv4 kolam umum dibagi dengan total IPs di kolam renang.

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

Dimensi	Deskripsi
OwnerID	ID pemilik kolam IPv4 renang umum.
IPv4PooLid Publik	ID IPv4 kolam renang umum.
Region	AWS Wilayah tempat kolam IPv4 renang umum berada.
ScopeID	ID lingkup IPAM yang dimiliki IPv4 kolam umum.

Metrik wawasan IP publik

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

Nama metrik	Deskripsi
AmazonOwnedElasticIPs	Jumlah alamat IP Elastic milik Amazon yang telah Anda sediakan atau tetapkan ke sumber daya di akun Anda. AWS
AssociatedAmazonOwnedElasticIPs	Jumlah alamat IP Elastic milik Amazon yang telah Anda kaitkan dengan sumber daya di akun Anda AWS .
AssociatedBringYourOwnIPs	Jumlah IPv4 alamat publik yang Anda bawa AWS menggunakan Bawa alamat IP Anda sendiri (BYOIP) dan telah dikaitkan dengan sumber daya di akun Anda AWS .
BringYourOwnIPs	Jumlah IPv4 alamat publik yang Anda bawa AWS menggunakan Bring your own IP address (BYOIP).
EC2Publik IPs	Jumlah IPv4 alamat publik yang ditetapkan ke EC2 instance ketika instance diluncurkan ke subnet default atau ke subnet yang dikonfigurasi untuk secara otomatis menetapkan alamat publik. IPv4
ServiceManagedBringYourOwnIPs	Jumlah IPv4 alamat publik yang Anda bawa AWS menggunakan Bring your own IP address (BYOIP) yang disediakan dan dikelola oleh suatu layanan. AWS
ServiceManagedIPs	Jumlah IPv4 alamat publik yang disediakan dan dikelola oleh suatu AWS layanan.
UnassociatedAmazonOwnedElasticIPs	Jumlah alamat IP Elastic milik Amazon yang belum Anda kaitkan dengan sumber daya di akun Anda AWS .
UnassociatedBringYourOwnIPs	Jumlah IPv4 alamat 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.
Region	AWS Wilayah 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 CIDRs untuk jenis sumber daya berikut:

- VPCs
- 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 antarmuka jaringan. CIDRs

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 Pindahkan VPC antar cakupan CIDRs.
- 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 Anda, pemilik IPAM dapat melihat riwayat alamat IP dari semua sumber daya yang CIDRs 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 IPv4 atau IPv6 IP atau CIDR. Ini harus menjadi CIDR khusus untuk sumber daya.
4. Pilih ID cakupan IPAM.
5. Pilih date/time rentang.
6. Jika Anda ingin memfilter hasil berdasarkan VPC, masukkan ID VPC. Gunakan opsi ini jika CIDR muncul dalam beberapa VPCs.
7. Pilih Cari.

Command line

Perintah di bagian ini menautkan ke Referensi AWS CLI Perintah. 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 resource-to-CIDR asosiasi dalam lingkup IPAM. Perubahan diambil dalam snapshot periodik, sehingga waktu akhir mungkin telah terjadi sebelum waktu tertentu ini.
- Contoh waktu mulai: Contoh waktu mulai resource-to-CIDR asosiasi 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 apa pun yang termasuk dalam kisaran alamat IP 10.0.0.0/8. CIDRs Karena IPAM mengambil perubahan CIDRs pada snapshot periodik, 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.
  - Patuh: Sumber daya yang dikelola mematuhi aturan alokasi pool IPAM.
  - Tidak patuh: Sumber daya CIDR tidak mematuhi satu atau beberapa aturan alokasi pool 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 pool IPAM dan tidak dipantau oleh IPAM untuk mendeteksi potensi kepatuhan CIDR terhadap aturan alokasi pool. CIDR dipantau untuk mendeteksi tumpang tindih.
  - Diabaikan: Sumber daya yang dikelola telah dipilih untuk dibebaskan dari pemantauan. Sumber daya yang diabaikan tidak dievaluasi terkait tumpang tindih atau kepatuhan aturan 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: Sumber daya CIDR tidak tumpang tindih dengan CIDR lain dalam cakupan yang sama.
  - Tumpang tindih: Sumber daya CIDR tumpang tindih dengan CIDR lain dalam cakupan yang sama. Harap diingat bahwa jika ada sumber daya CIDR yang tumpang tindih, bisa jadi sumber daya tersebut 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.
- Tipe 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

Anda dapat menggunakan wawasan IP Publik untuk melihat hal berikut:

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

IPv4 Alamat publik adalah IPv4 alamat yang dapat dirutekan dari internet. IPv4Alamat publik diperlukan agar sumber daya dapat dijangkau secara langsung dari internet melalui. IPv4

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

Anda dapat melihat wawasan tentang jenis IPv4 alamat publik berikut:

- Alamat IP elastis (EIPs): Alamat IPv4 publik statis yang disediakan oleh Amazon yang dapat Anda kaitkan dengan instans EC2, elastic network interface, atau sumber daya. AWS
- IPv4 Alamat 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 menetapkan alamat publik secara otomatis). IPv4

- BYOIPv4 alamat: IPv4 Alamat publik dalam rentang IPv4 alamat yang Anda bawa AWS menggunakan Bring your own IP address (BYOIP).
- Alamat yang dikelola layanan: IPv4 IPv4 Alamat publik secara otomatis disediakan pada AWS sumber daya dan dikelola oleh layanan. AWS Misalnya, IPv4 alamat publik di Amazon ECS, Amazon RDS, atau Amazon. WorkSpaces

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

- Jenis IP Publik: Jumlah IPv4 alamat publik yang diatur berdasarkan jenis.
  - Milik Amazon EIPs: Alamat IP elastis yang telah Anda sediakan atau tetapkan ke sumber daya di akun Anda. AWS
  - EC2 publik IPs: Alamat IPv4 publik yang ditetapkan ke instans EC2 saat instance diluncurkan ke subnet default atau ke subnet yang telah dikonfigurasi untuk menetapkan alamat publik secara otomatis. IPv4
  - BYOIP: IPv4 Alamat publik yang telah Anda bawa AWS menggunakan Bring your own IP address (BYOIP).
  - Layanan dikelola IPs: IPv4 Alamat publik disediakan dan dikelola oleh layanan. AWS
  - Layanan dikelola BYOIP: IPv4 Alamat publik dibawa ke AWS dan dikelola oleh layanan. AWS
  - Bersebelahan milik Amazon EIPs: Alamat IP elastis yang dialokasikan dari kolam IPAM publik bersebelahan yang disediakan Amazon. IPv4
- Penggunaan EIP: Jumlah alamat IP Elastis yang diatur berdasarkan cara penggunaannya.
  - Terkait milik Amazon EIPs: 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: IPv4 Alamat publik yang Anda bawa AWS menggunakan BYOIP yang telah Anda kaitkan dengan antarmuka jaringan.
  - Tidak terkait milik Amazon EIPs: Alamat IP elastis yang telah Anda sediakan di AWS akun Anda tetapi Anda belum terkait dengan antarmuka jaringan.
  - BYOIP Tidak Terkait: IPv4 Alamat publik yang Anda bawa AWS menggunakan BYOIP tetapi Anda belum terkait dengan antarmuka jaringan.
  - Terkait milik Amazon yang berdekatan EIPs: Alamat IP elastis yang dialokasikan dari kolam IPAM publik bersebelahan yang disediakan Amazon dan terkait dengan sumber daya. IPv4

  - Bersebelahan milik Amazon yang tidak terkait EIPs: Alamat IP elastis yang dialokasikan dari kolam IPAM publik bersebelahan yang disediakan Amazon dan tidak terkait dengan sumber daya. IPv4
- Penggunaan IPv4 bersebelahan milik Amazon: Tabel yang menunjukkan IPs penggunaan IPv4 alamat publik yang berdekatan dari waktu ke waktu dan kolam IPAM milik Amazon terkait. IPv4
- Alamat IP Publik: Tabel IPv4 alamat publik dan atributnya.
  - Alamat IP: IPv4 Alamat 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: IPv4 Alamat publik tidak terkait dengan sumber daya apa pun dan tidak digunakan di akun Anda AWS .
  - Jenis alamat: Jenis alamat IP.
    - EIP milik Amazon: IPv4 Alamat publik adalah alamat IP Elastis.
    - BYOIP: IPv4 Alamat publik dibawa AWS menggunakan BYOIP.
    - IP publik EC2: Alamat IPv4 publik ditetapkan secara otomatis ke instans EC2.
    - Layanan BYOIP yang dikelola: IPv4 Alamat publik dibawa AWS menggunakan Bring Your Own IP (BYOIP).
    - IP yang dikelola layanan: IPv4 Alamat publik disediakan dan dikelola oleh layanan. AWS
  - Layanan: Layanan yang dikaitkan dengan alamat IP.
    - AGA: Sebuah AWS Global Accelerator. Jika akselerator perutean kustom digunakan, publiknya tidak IPs terdaftar. Untuk melihat publik ini IPs, 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 AWS Site-to-Site VPN virtual.
    - Lainnya: Layanan lain yang saat ini tidak dapat diidentifikasi.

- Nama (ID EIP): Jika IPv4 alamat publik ini adalah alokasi alamat IP Elastis, ini adalah nama dan ID dari alokasi EIP.
- ID antarmuka jaringan: Jika IPv4 alamat 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.
- Public IPv4 pool: 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 IPv4 kolam 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 IPv4 alamat 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 tidak terkait EIPs 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 mendapatkan AWS CLI, lihatAkses IPAM. Untuk informasi lebih lanjut tentang konsep IPAM yang disebutkan dalam tutorial ini, lihatBagaimana IPAM bekerja.

Konten

Memulai dengan IPAM menggunakan CLI AWS

Tutorial ini memandu Anda melalui proses pengaturan dan menggunakan Amazon VPC IP Address Manager (IPAM) dengan AWS CLI menggunakan satu akun. AWS Pada akhir tutorial ini, Anda akan membuat IPAM, membuat hierarki kumpulan alamat IP, dan mengalokasikan CIDR ke VPC.

Prasyarat

Sebelum Anda memulai tutorial ini, pastikan Anda memiliki:

- AWS Akun dengan izin untuk membuat dan mengelola sumber daya IPAM.
- AWS CLI diinstal dan dikonfigurasi dengan kredensil yang sesuai. Untuk informasi tentang menginstal AWS CLI, lihat Menginstal atau memperbarui versi terbaru CLI AWS. Untuk informasi tentang mengonfigurasi AWS CLI, lihat Dasar-dasar konfigurasi.
- Pemahaman dasar pengalamatan IP dan notasi CIDR.
- Pengetahuan dasar tentang konsep Amazon VPC.
- Sekitar 30 menit untuk menyelesaikan tutorial.

Buat IPAM

Langkah pertama adalah membuat IPAM dengan wilayah operasi. IPAM membantu Anda merencanakan, melacak, dan memantau alamat IP untuk beban AWS kerja Anda.

Buat IPAM dengan wilayah operasi di us-east-1 dan us-west-2:

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

Perintah ini menciptakan IPAM dan memungkinkannya untuk mengelola alamat IP di wilayah yang ditentukan. Wilayah operasi adalah AWS Wilayah di mana IPAM diizinkan untuk mengelola alamat CIDRs IP.

Verifikasi bahwa IPAM Anda telah dibuat:

```
aws ec2 describe-ipams
```

Catat ID IPAM dari output, karena Anda akan membutuhkannya untuk langkah selanjutnya.

Tunggu IPAM sepenuhnya dibuat dan tersedia (sekitar 20 detik):

```
sleep 20
```

Dapatkan ID cakupan IPAM

Saat Anda membuat IPAM, AWS secara otomatis membuat ruang lingkup pribadi dan publik. Untuk tutorial ini, kita akan menggunakan ruang lingkup pribadi.

Ambil detail IPAM dan ekstrak ID cakupan pribadi:

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

Ganti `ipam-0abcd1234` dengan ID IPAM Anda yang sebenarnya.

Dari output, identifikasi dan catat ID cakupan pribadi dari `PrivateDefaultScopeId` bidang. Ini akan terlihat seperti`ipam-scope-0abcd1234`.

Buat kolam tingkat atas IPv4

Sekarang, mari kita buat kolam tingkat atas dalam lingkup pribadi. Pool ini akan berfungsi sebagai induk untuk semua pool lain dalam hierarki kami.

Buat IPv4 kolam tingkat atas:

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

Ganti `ipam-scope-0abcd1234` dengan ID cakupan pribadi Anda yang sebenarnya.

Tunggu hingga kolam sepenuhnya dibuat dan tersedia:

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

Ganti `ipam-pool-0abcd1234` dengan ID kolam tingkat atas Anda yang sebenarnya. Negara harus `create-complete` sebelum melanjutkan.

Setelah pool tersedia, berikan blok CIDR untuk itu:

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

Tunggu CIDR sepenuhnya disediakan:

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

Negara harus `provisioned` sebelum melanjutkan.

Buat IPv4 kolam regional

Selanjutnya, buat kolam regional di dalam kolam tingkat atas. Kolam ini akan khusus untuk AWS Wilayah tertentu.

Buat IPv4 kolam regional:

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

Ganti `ipam-scope-0abcd1234` dengan ID cakupan pribadi Anda yang sebenarnya dan `ipam-pool-0abcd1234` dengan ID kolam tingkat atas Anda.

Tunggu hingga kolam regional sepenuhnya dibuat dan tersedia:

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

Ganti `ipam-pool-1abcd1234` dengan ID kolam regional Anda yang sebenarnya. Negara harus `create-complete` sebelum melanjutkan.

Setelah pool tersedia, berikan blok CIDR untuk itu:

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

Tunggu CIDR sepenuhnya disediakan:

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

Negara harus `provisioned` sebelum melanjutkan.

Buat IPv4 kolam pengembangan

Sekarang, buat kolam pengembangan di dalam kolam regional. Kolam ini akan digunakan untuk lingkungan pengembangan.

Buat IPv4 kolam pengembangan:

```
aws ec2 create-ipam-pool \
  --ipam-scope-id ipam-scope-0abcd1234 \
```

```
  --source-ipam-pool-id ipam-pool-1abcd1234 \
  --locale us-east-1 \
  --address-family ipv4 \
  --description "Development pool"
```

Ganti `ipam-scope-0abcd1234` dengan ID cakupan pribadi Anda yang sebenarnya dan `ipam-pool-1abcd1234` dengan ID kumpulan regional Anda.

Catatan: Penting untuk menyertakan `--locale` parameter agar sesuai dengan lokal kumpulan induk.

Tunggu hingga kolam pengembangan sepenuhnya dibuat dan tersedia:

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

Ganti `ipam-pool-2abcd1234` dengan ID kumpulan pengembangan Anda yang sebenarnya. Negara harus `create-complete` sebelum melanjutkan.

Setelah pool tersedia, berikan blok CIDR untuk itu:

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

Tunggu CIDR sepenuhnya disediakan:

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

Negara harus `provisioned` sebelum melanjutkan.

Buat VPC menggunakan CIDR kolam IPAM

Terakhir, buat VPC yang menggunakan CIDR dari kolam IPAM Anda. Ini menunjukkan bagaimana IPAM dapat digunakan untuk mengalokasikan ruang alamat IP ke sumber daya. AWS

Buat VPC menggunakan CIDR kolam IPAM:

```
aws ec2 create-vpc \
  --ipv4-ipam-pool-id ipam-pool-2abcd1234 \
```

```
  --ipv4-netmask-length 26 \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=IPAM-VPC}]'
```

Ganti `ipam-pool-2abcd1234` dengan ID kumpulan pengembangan Anda yang sebenarnya.

`--ipv4-netmask-length 26`Parameter menentukan bahwa Anda ingin blok /26 CIDR (64 alamat IP) dialokasikan dari pool. Panjang netmask ini dipilih untuk memastikannya lebih kecil dari blok CIDR pool (/24).

Verifikasi bahwa VPC Anda telah dibuat:

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

Verifikasi alokasi kolam IPAM

Periksa apakah CIDR dialokasikan dari kolam IPAM Anda:

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

Ganti `ipam-pool-2abcd1234` dengan ID kumpulan pengembangan Anda yang sebenarnya.

Perintah ini menunjukkan semua alokasi dari kolam IPAM yang ditentukan, termasuk VPC yang baru saja Anda buat.

Pemecahan Masalah

Berikut adalah beberapa masalah umum yang mungkin Anda temui saat bekerja dengan IPAM:

- Kesalahan izin: Pastikan bahwa pengguna atau peran IAM Anda memiliki izin yang diperlukan untuk membuat dan mengelola sumber daya IPAM. Anda mungkin memerlukan`ec2:CreateIpam`,`ec2:CreateIpamPool`, dan izin terkait lainnya.
- Batas sumber daya terlampaui: Secara default, Anda hanya dapat membuat satu IPAM per akun. Jika Anda sudah memiliki IPAM, Anda harus menghapusnya sebelum membuat yang baru atau menggunakan yang sudah ada.
- Kegagalan alokasi CIDR: Saat menyediakan CIDRs ke pool, pastikan CIDR yang Anda coba sediakan tidak tumpang tindih dengan alokasi yang ada di pool lain.
- Batas waktu permintaan API: Jika Anda mengalami kesalahan RequestExpired "", mungkin karena latensi jaringan atau masalah sinkronisasi waktu. Coba perintahnya lagi.

- Kesalahan status salah: Jika Anda menerima kesalahan IncorrectState "", itu mungkin karena Anda mencoba melakukan operasi pada sumber daya yang tidak dalam keadaan benar. Tunggu sumber daya sepenuhnya dibuat atau disediakan sebelum melanjutkan.
- Kesalahan ukuran alokasi: Jika Anda menerima kesalahan InvalidParameterValue "" tentang ukuran alokasi, pastikan panjang netmask yang Anda minta sesuai untuk ukuran kolam. Misalnya, Anda tidak dapat mengalokasikan /25 CIDR dari kumpulan /24.
- Pelanggaran ketergantungan: Saat membersihkan sumber daya, Anda mungkin mengalami kesalahan DependencyViolation "". Ini karena sumber daya memiliki ketergantungan satu sama lain. Pastikan untuk menghapus sumber daya dalam urutan terbalik pembuatan dan deprovision CIDRs sebelum menghapus pool.

Pembersihan sumber daya

Setelah selesai dengan tutorial ini, Anda harus membersihkan sumber daya yang Anda buat untuk menghindari biaya yang tidak perlu.

1. Hapus VPC:

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

2. Penutupan CIDR dari kumpulan pengembangan:

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

3. Hapus kumpulan pengembangan:

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

4. Pembatalan CIDR dari kolam regional:

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

5. Hapus kolam regional:

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

6. Penutupan CIDR dari kolam tingkat atas:

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

7. Hapus kolam tingkat atas:

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

8. Hapus IPAM:

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

Ganti semua IDs dengan sumber daya Anda yang sebenarnya IDs.

> **Note**
>
> Anda mungkin perlu menunggu di antara operasi ini untuk memungkinkan sumber daya dihapus sepenuhnya sebelum melanjutkan ke langkah berikutnya. Jika Anda mengalami pelanggaran ketergantungan, tunggu beberapa detik dan coba lagi.

Langkah selanjutnya

Sekarang setelah Anda mempelajari cara membuat dan menggunakan IPAM dengan AWS CLI, Anda mungkin ingin menjelajahi fitur-fitur yang lebih canggih:

- Merencanakan penyediaan alamat IP— Pelajari cara merencanakan ruang alamat IP Anda secara efektif
- Memantau penggunaan CIDR berdasarkan sumber daya— Memahami cara memantau penggunaan alamat IP
- Bagikan kolam IPAM menggunakan AWS RAM— Pelajari cara berbagi kolam IPAM di seluruh akun AWS
- Integrasikan IPAM dengan akun di Organisasi AWS— Temukan cara menggunakan IPAM di seluruh organisasi Anda

Tutorial: Buat IPAM dan pool menggunakan konsol

Dalam tutorial ini, Anda membuat IPAM, mengintegrasikan dengan AWS 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 sebuah organisasi. Itu tidak mencakup bagaimana caranyaIntegrasikan IPAM dengan akun di luar organisasi Anda.

> **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

- Langkah 7: Buat VPC dengan CIDR yang dialokasikan dari kolam IPAM
- Langkah 8: Pembersihan

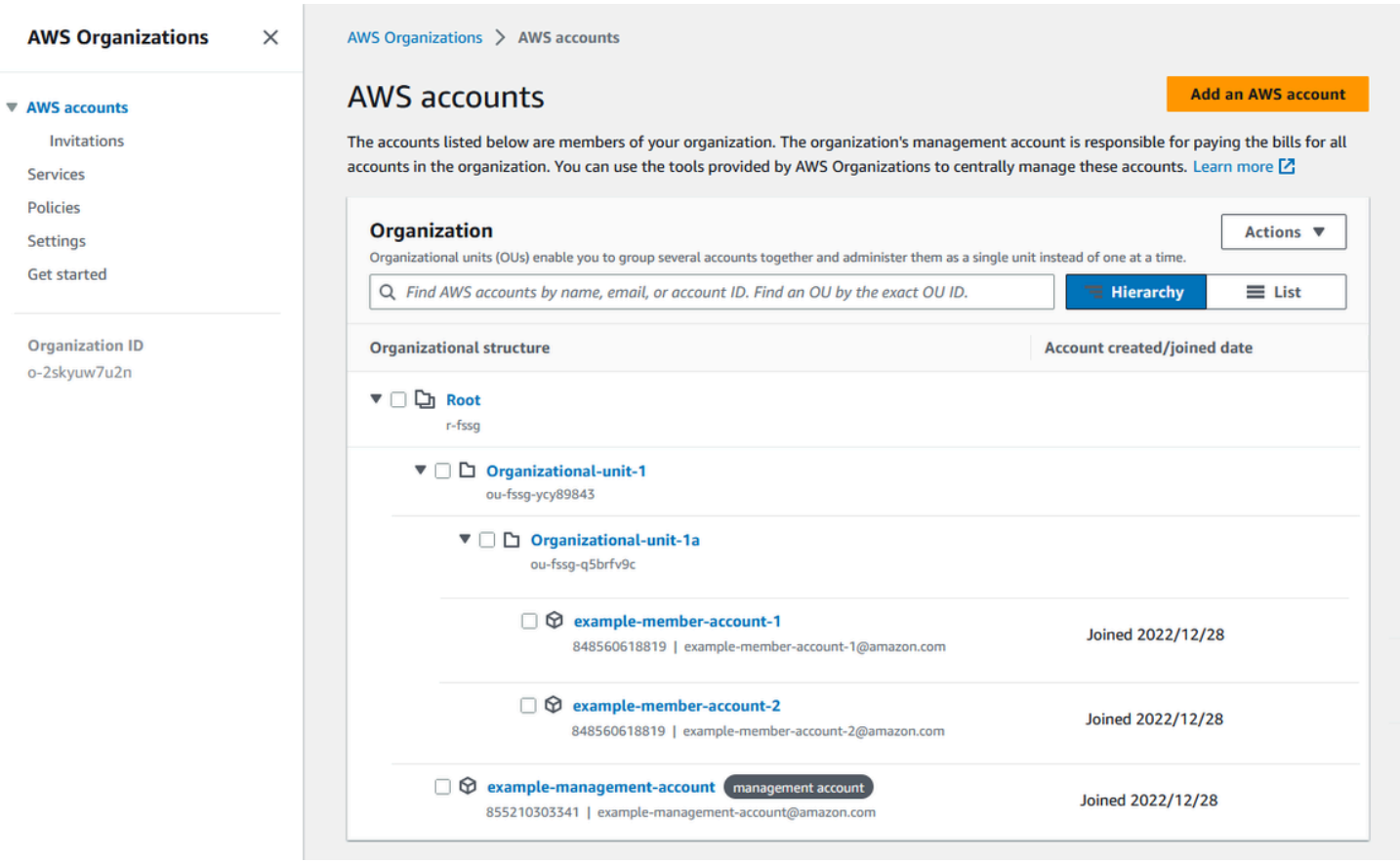
Prasyarat

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

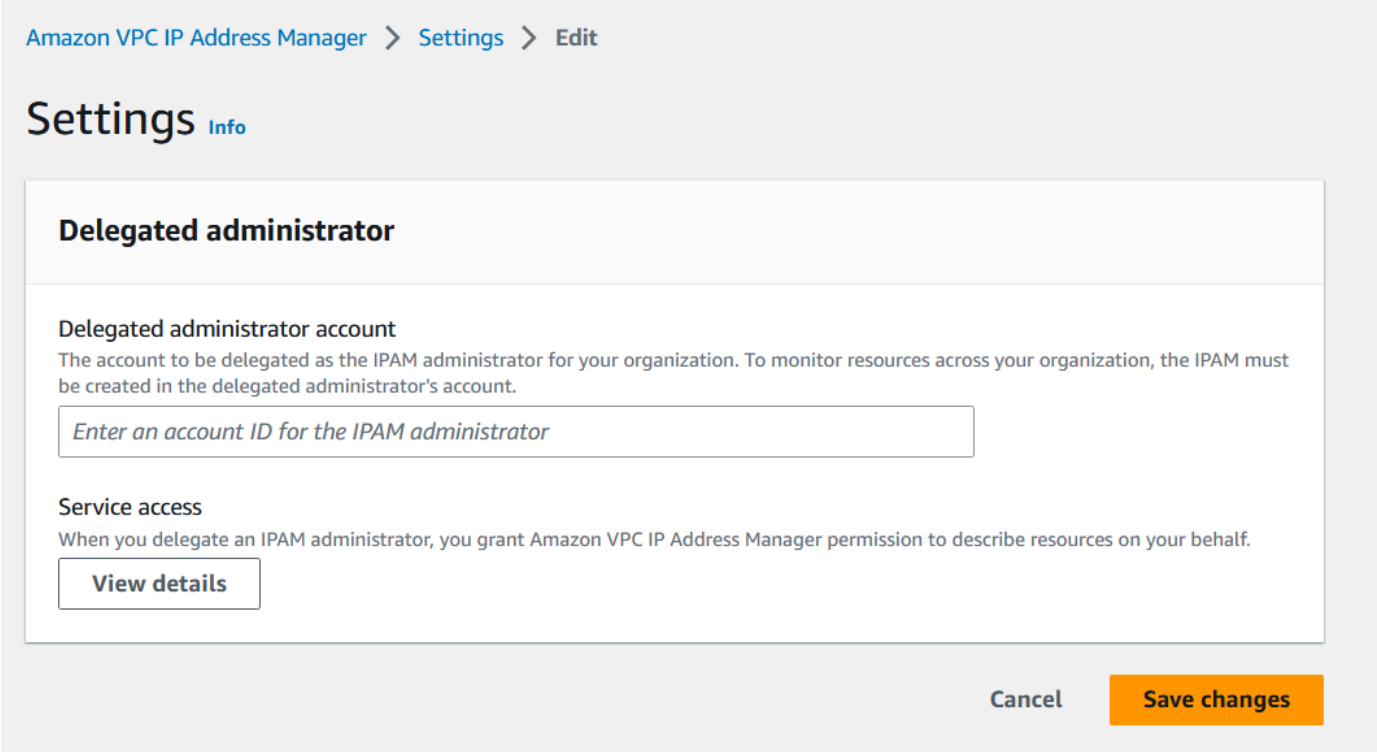
Langkah 1: Delegasikan administrator IPAM

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 mereka CIDRs 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. Dalam Konsol Manajemen AWS, pilih AWS Wilayah di mana 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.



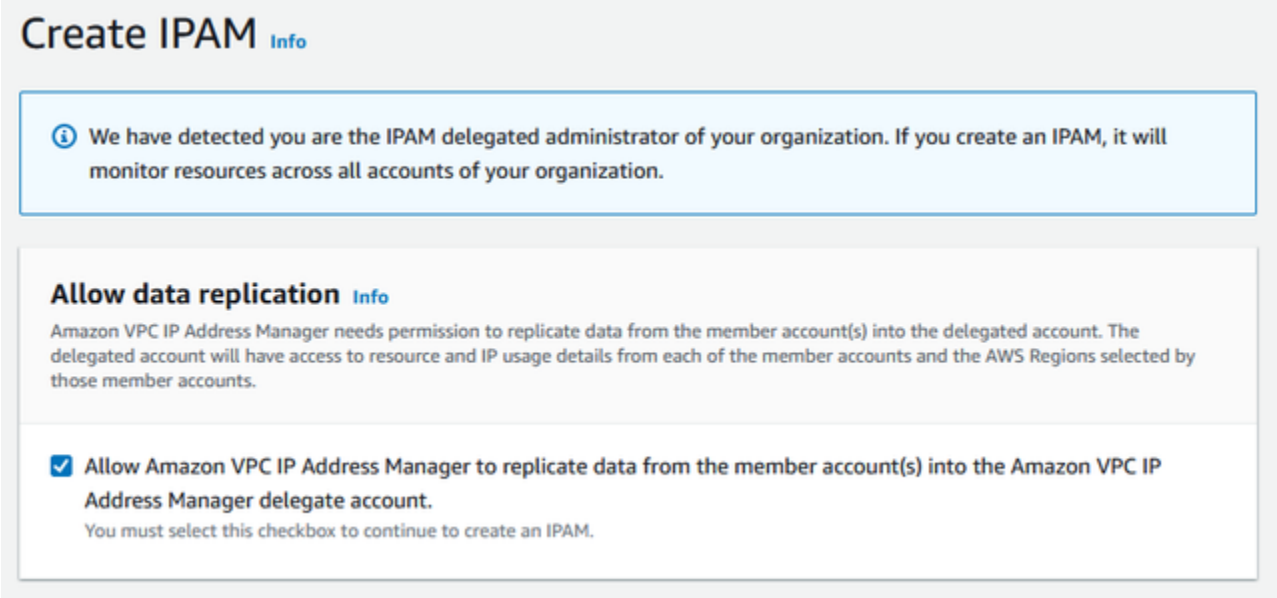
6. Pilih Simpan perubahan. Informasi administrator yang didelegasikan diisi dengan detail yang terkait dengan akun anggota.

Langkah 2: Buat IPAM

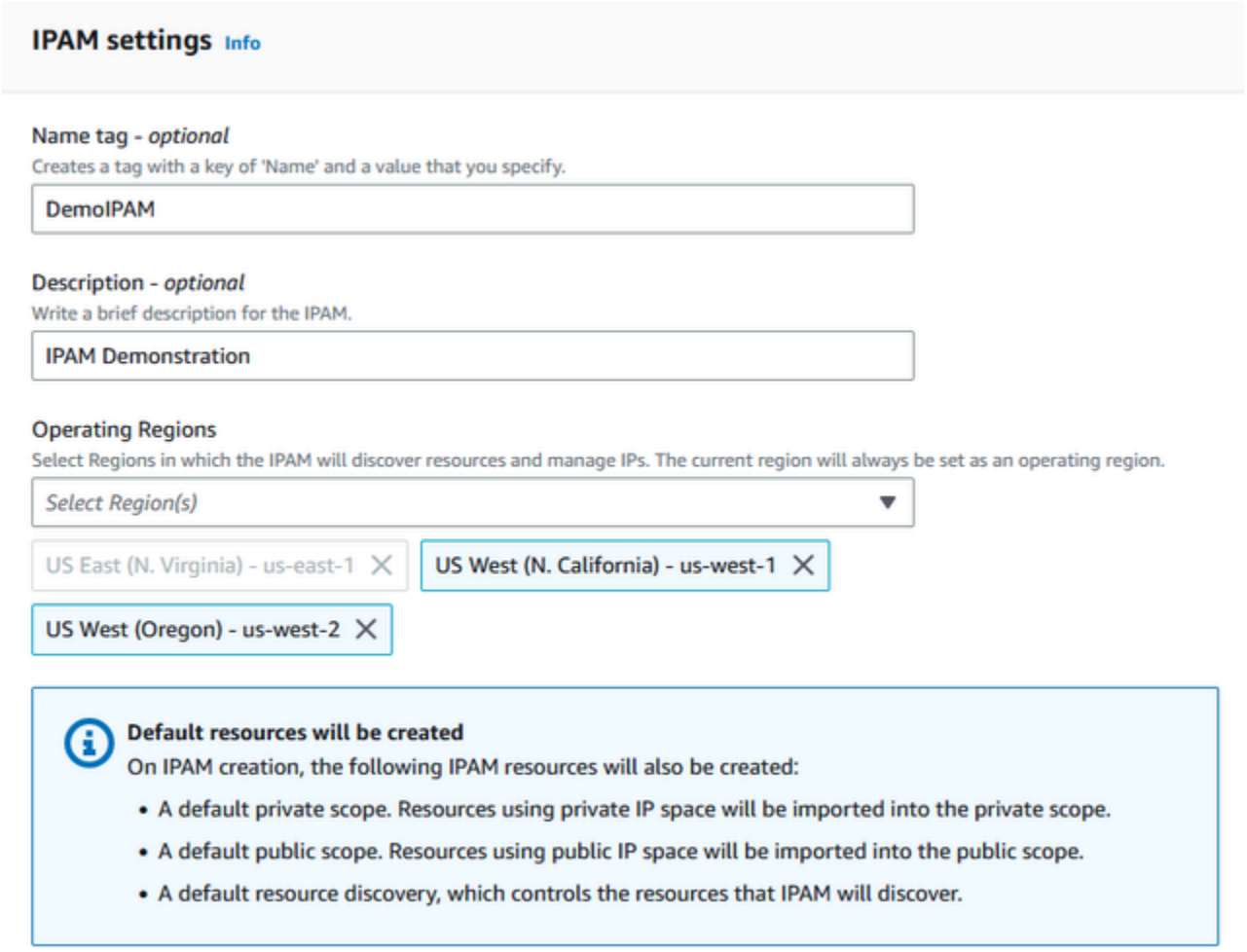
Pada langkah ini Anda akan membuat IPAM. Saat Anda membuat IPAM, IPAM secara otomatis membuat dua cakupan untuk IPAM: ruang lingkup pribadi yang ditujukan untuk semua ruang pribadi, dan ruang lingkup publik yang ditujukan untuk semua ruang publik. Cakupan, bersama dengan kumpulan dan alokasi, adalah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

Untuk membuat IPAM

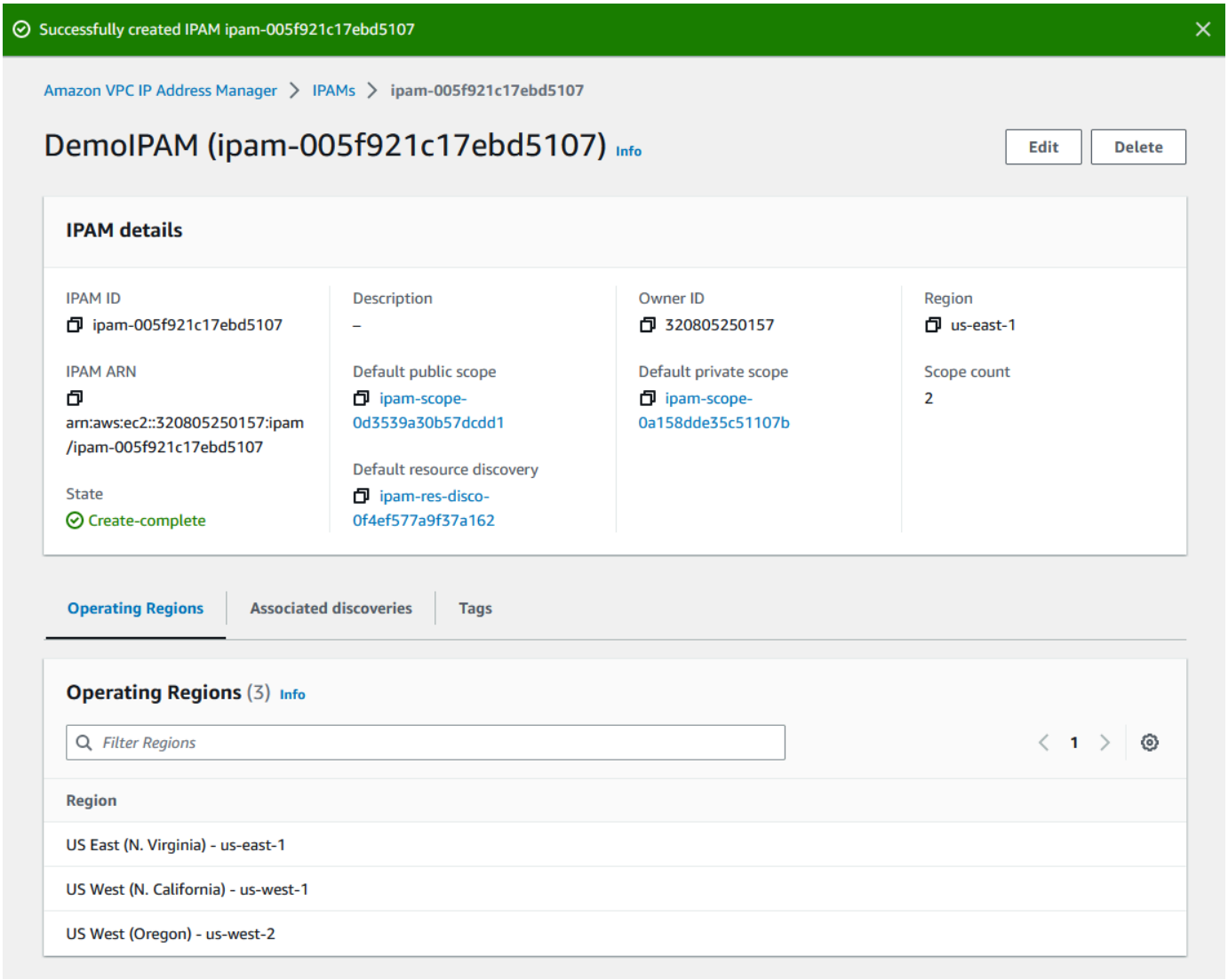
1. Menggunakan akun AWS Organizations anggota yang didelegasikan sebagai admin IPAM pada langkah sebelumnya, buka konsol IPAM di. https://console.aws.amazon.com/ipam/
2. Di Konsol AWS Manajemen, pilih AWS Wilayah tempat Anda ingin membuat IPAM. Buat IPAM di Wilayah operasi utama Anda.
3. Pada halaman beranda layanan, pilih Buat IPAM.
4. Pilih Izinkan Manajer 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. AWS Wilayah 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

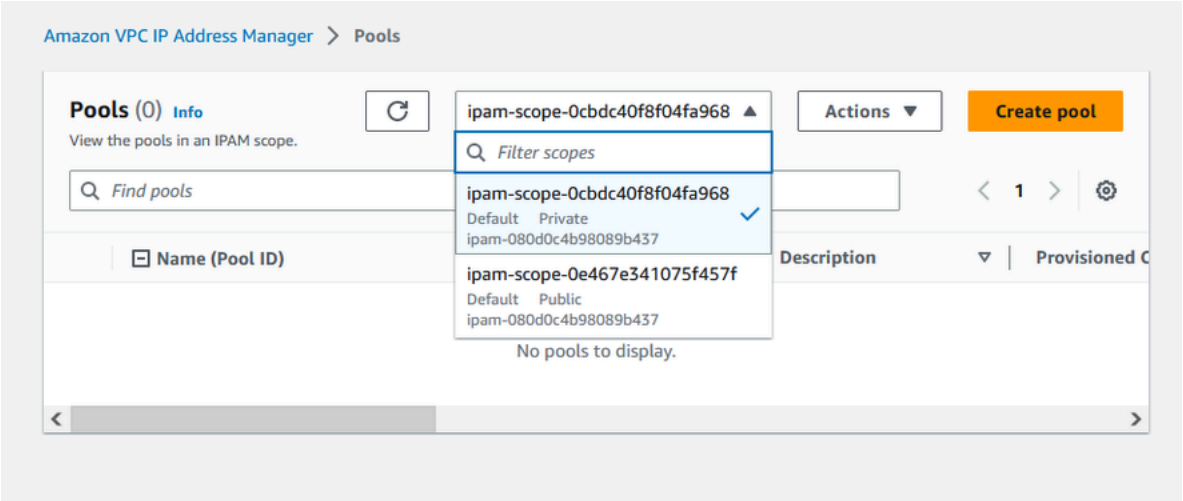
Dalam tutorial ini, Anda membuat hierarki pool dimulai dengan kolam IPAM tingkat atas. Pada langkah selanjutnya, Anda akan membuat sepasang kolam Regional dan kolam pengembangan pra-produksi di salah satu kolam regional.

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

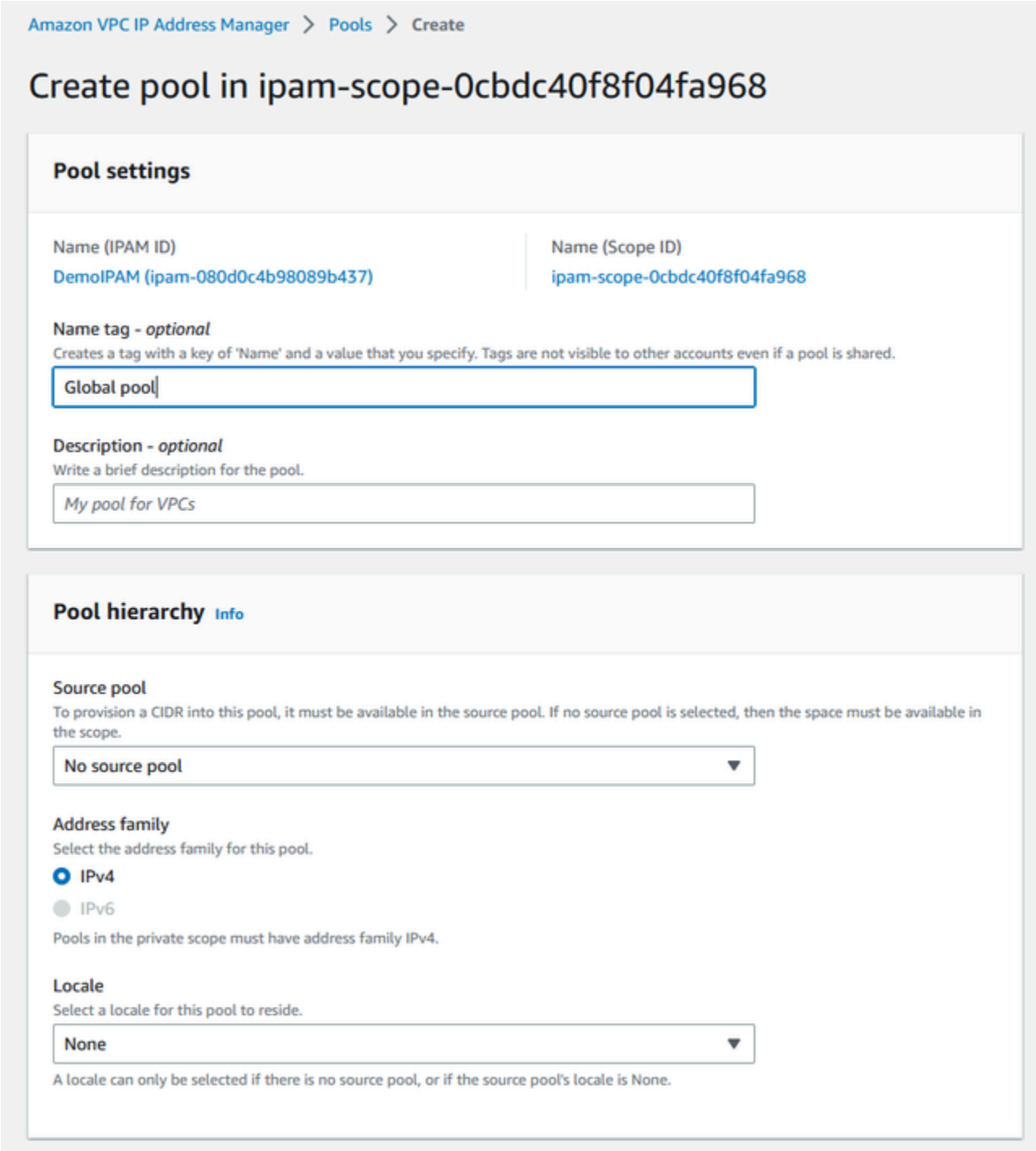
Untuk membuat kolam tingkat atas

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

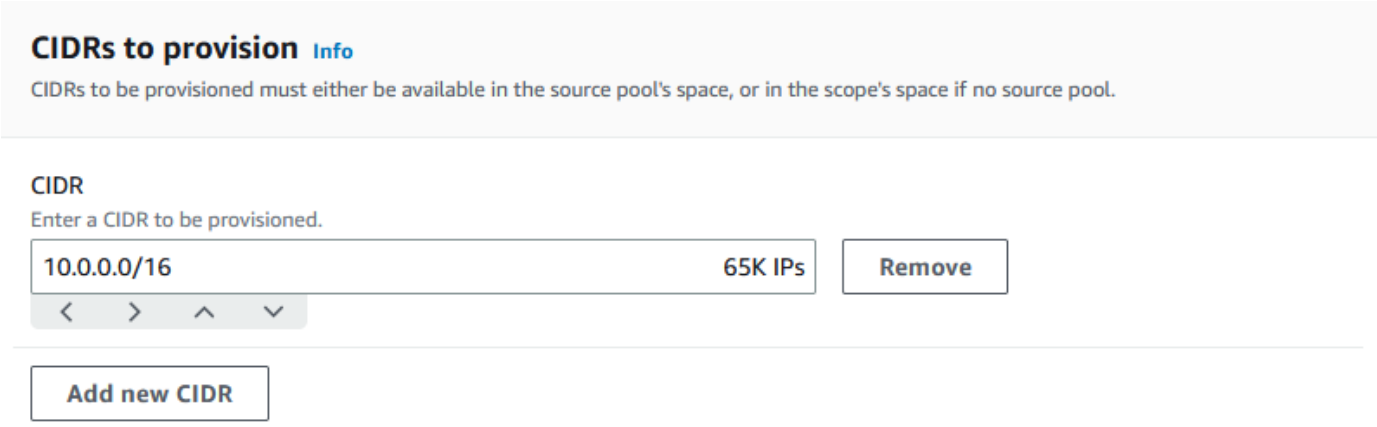
3. Pilih ruang lingkup pribadi.



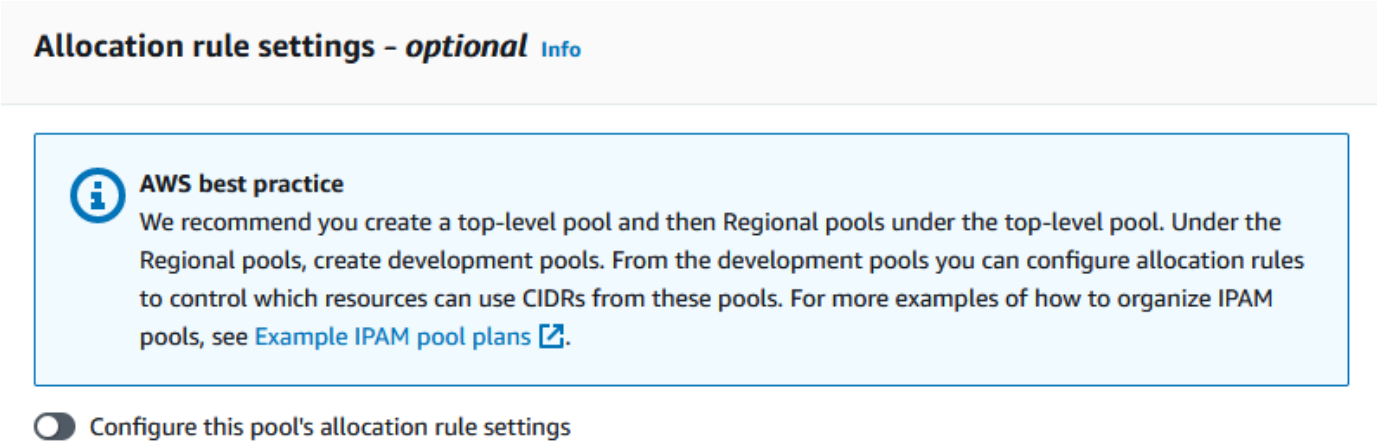
4. Pilih Buat kolam.
5. Di bawah lingkup IPAM, biarkan ruang lingkup pribadi dipilih.
6. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool, seperti “Global pool”.
7. Di bawah Sumber, pilih cakupan IPAM. Karena ini adalah kolam tingkat atas kami, itu tidak akan memiliki kolam sumber.
8. Di bawah Alamat keluarga, 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.



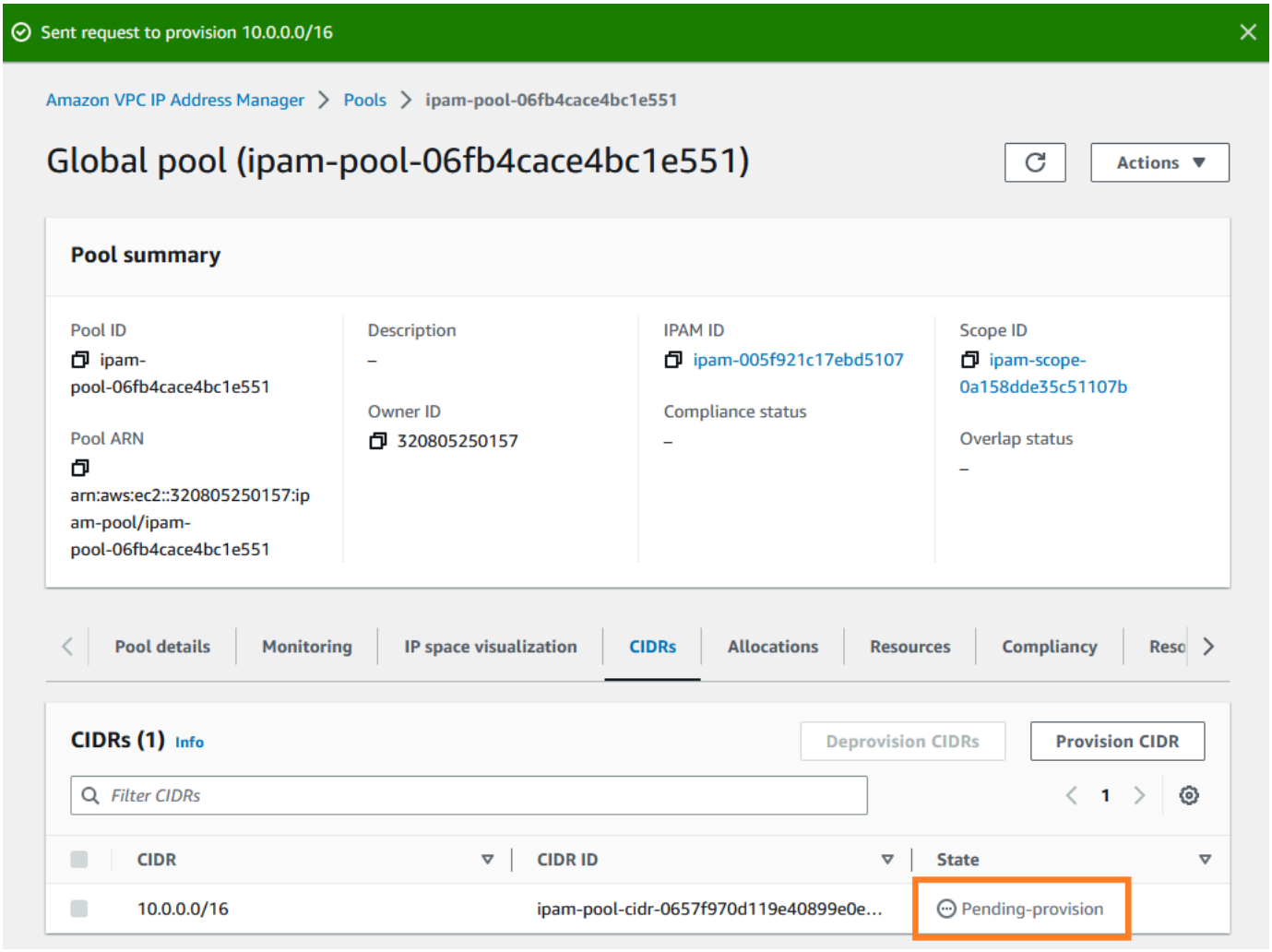
11. Pilih CIDR untuk penyediaan kolam renang. Dalam contoh ini, kami menyediakan 10.0.0.0/16.



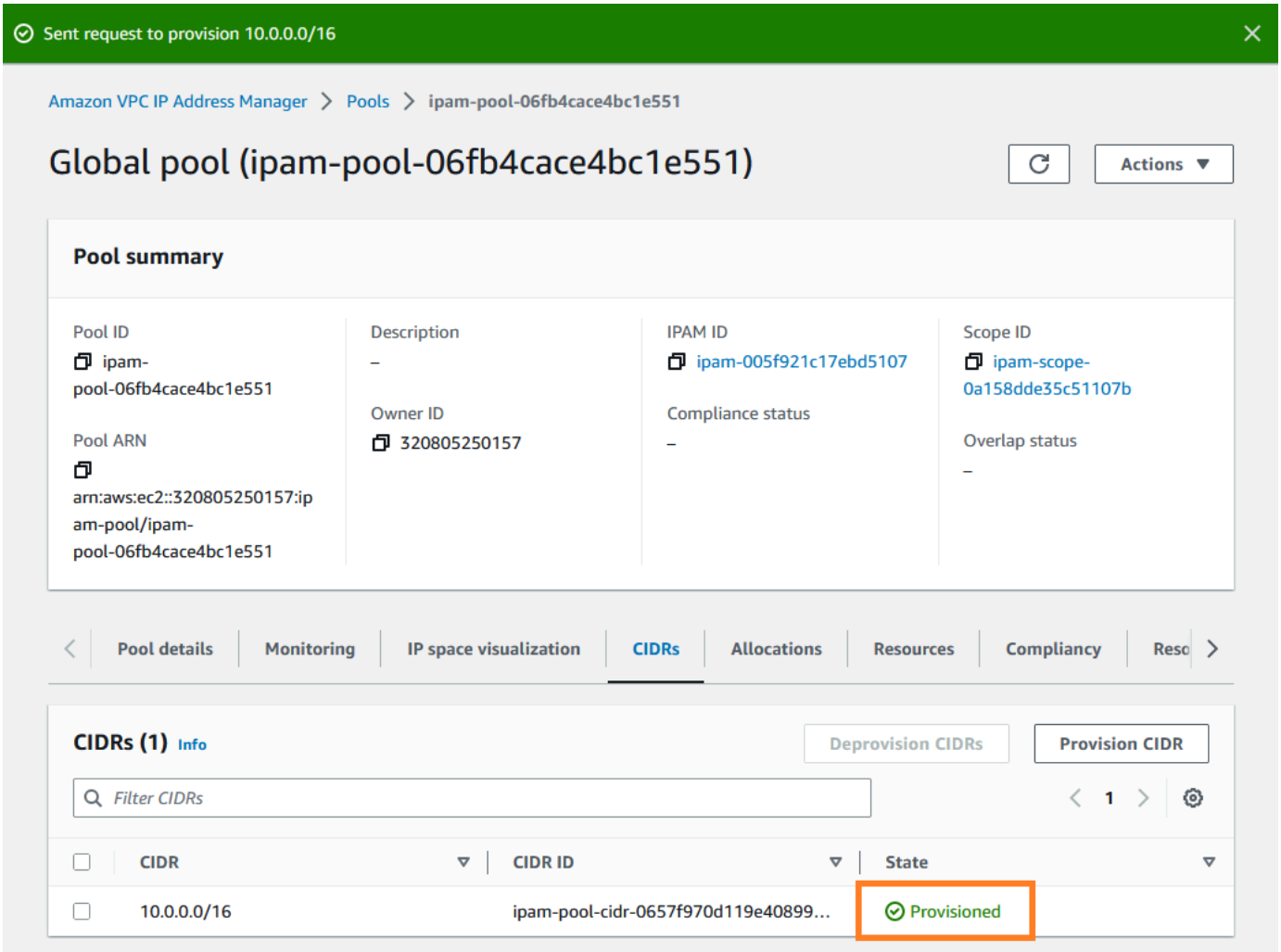
12. Biarkan Konfigurasi pengaturan aturan alokasi kumpulan ini dinonaktifkan. Ini adalah kolam tingkat atas kami, dan Anda tidak akan CIDRs mengalokasikan VPCs langsung dari kolam ini. Sebagai gantinya, Anda akan mengalokasikannya dari sub-pool yang Anda buat dari kolam ini.



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-west-1 dan us-west-2.

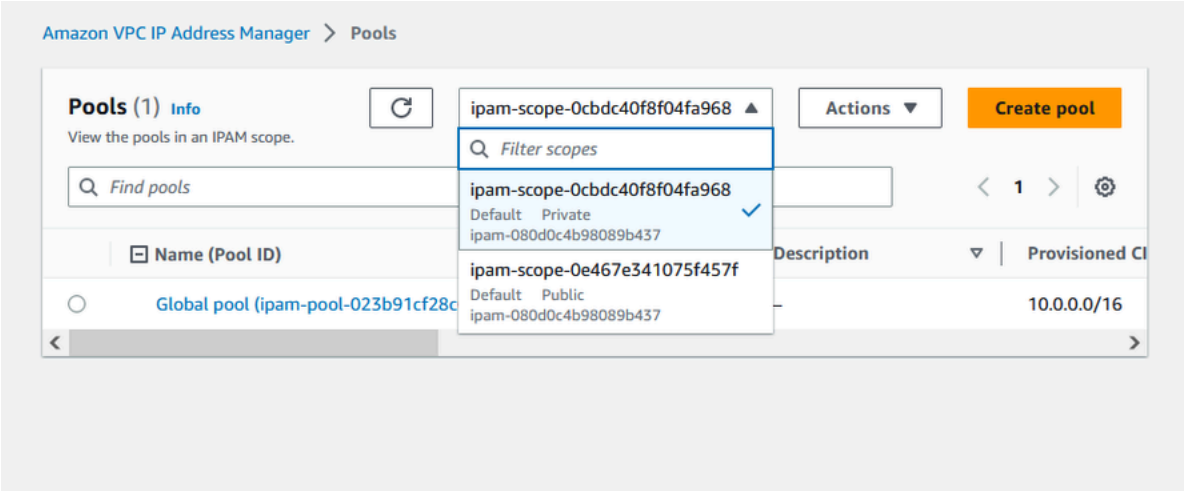
Langkah 4: Buat kolam IPAM Regional

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

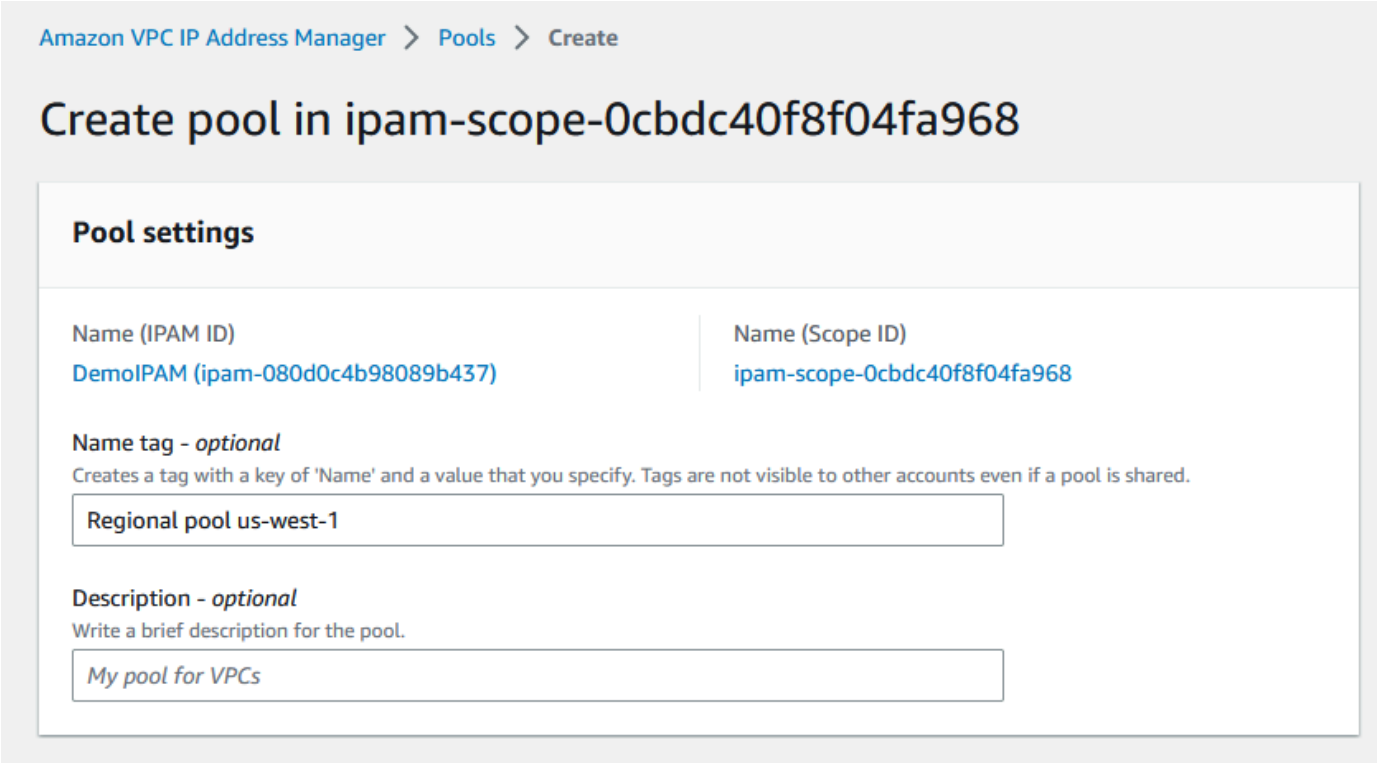
Untuk membuat kolam Regional

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

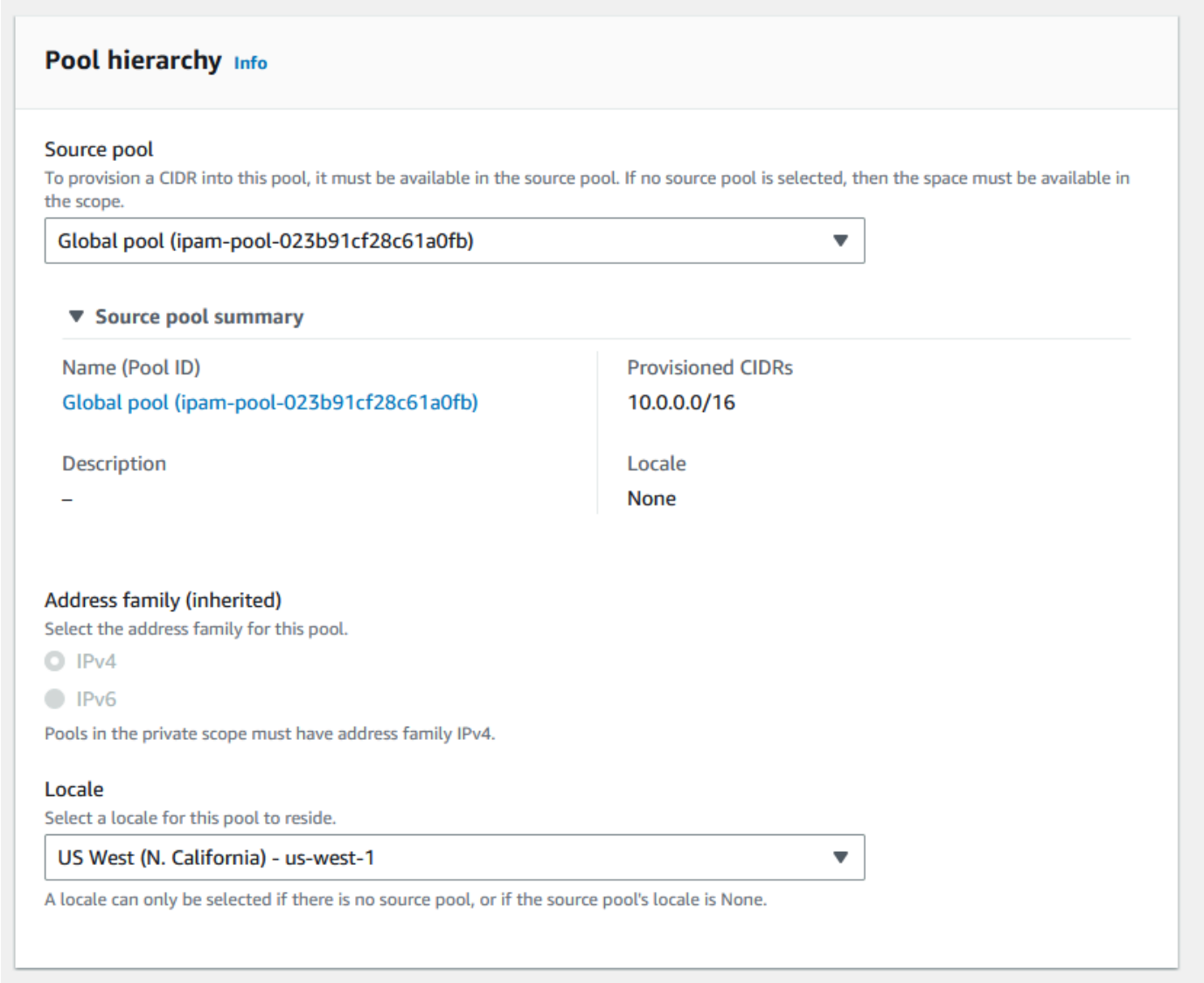
3. Pilih ruang lingkup pribadi.



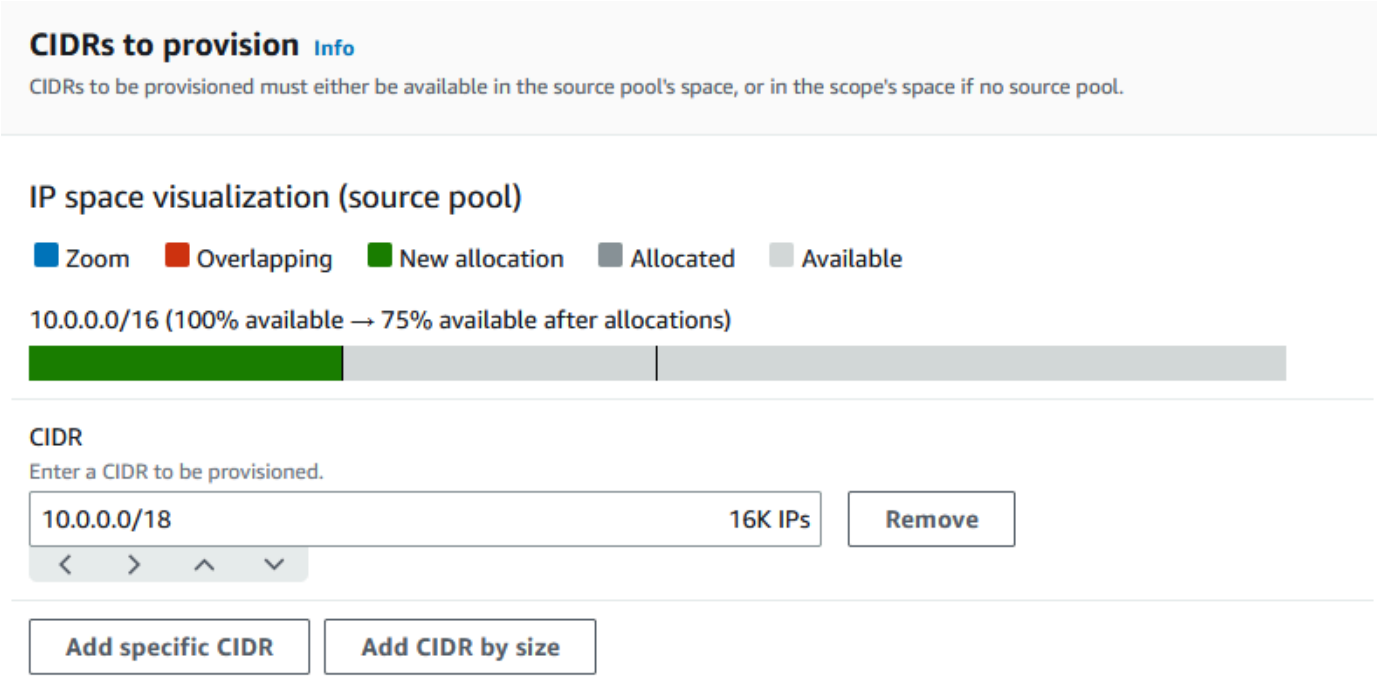
4. Pilih Buat kolam.
5. Di bawah lingkup IPAM, biarkan ruang lingkup pribadi dipilih.
6. (Opsional) Tambahkan tag Nama untuk pool dan deskripsi untuk pool, seperti Regional pool us-west-1.



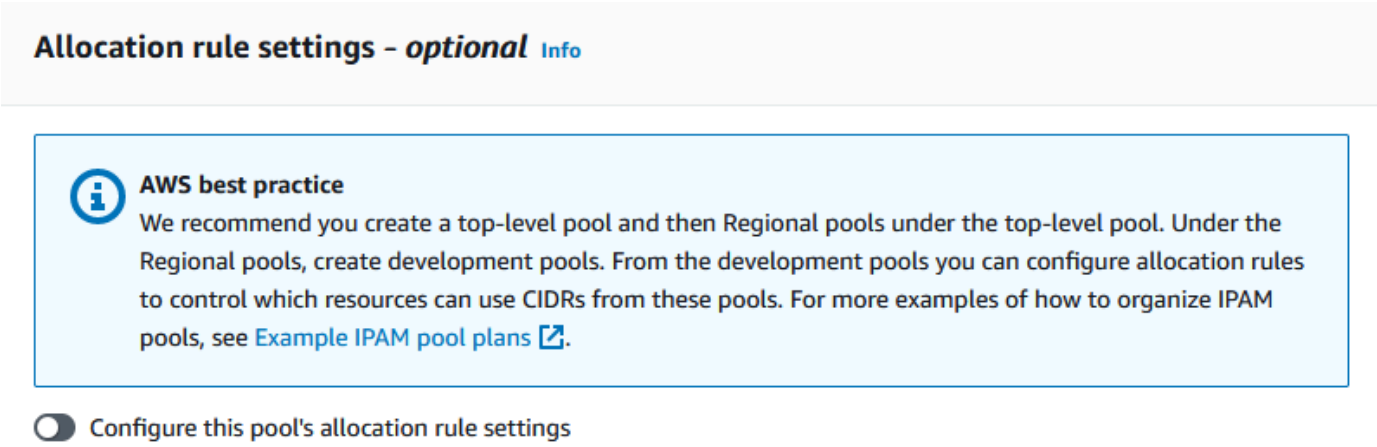
7. Di bawah Sumber, pilih kolam IPAM dan pilih kolam tingkat atas (“Kolam global”) yang Anda buat. Langkah 3: Buat kolam IPAM tingkat atas Kemudian, di bawah Locale, pilih us-west-1.



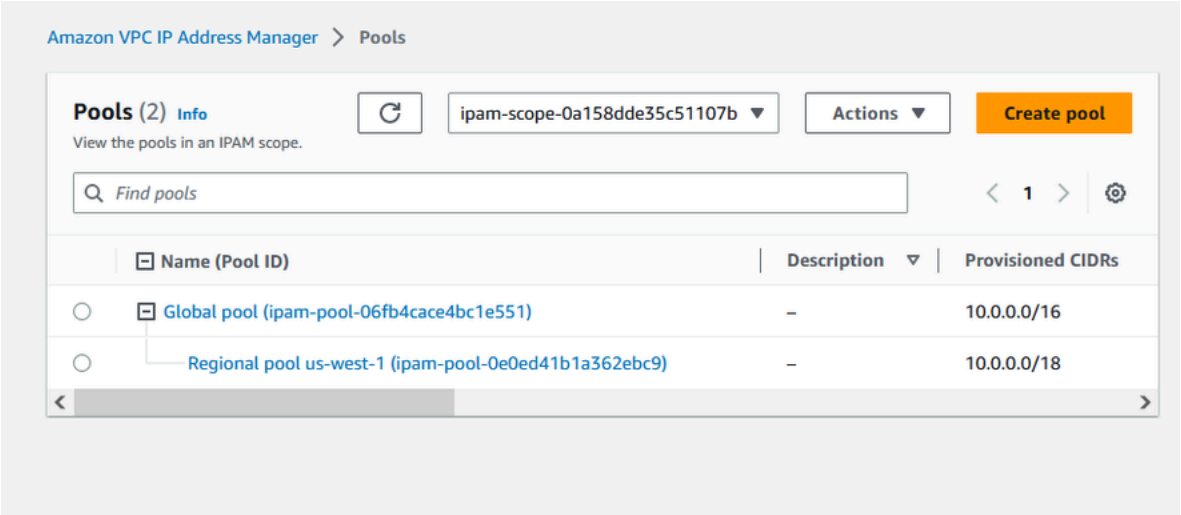
8. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih. Untuk informasi selengkapnya tentang menggunakan opsi ini untuk merencanakan ruang IP subnet dalam VPC, lihat. Tutorial: Rencanakan ruang alamat IP VPC untuk alokasi IP subnet
9. Berdasarkan CIDRs ketentuan, masukkan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



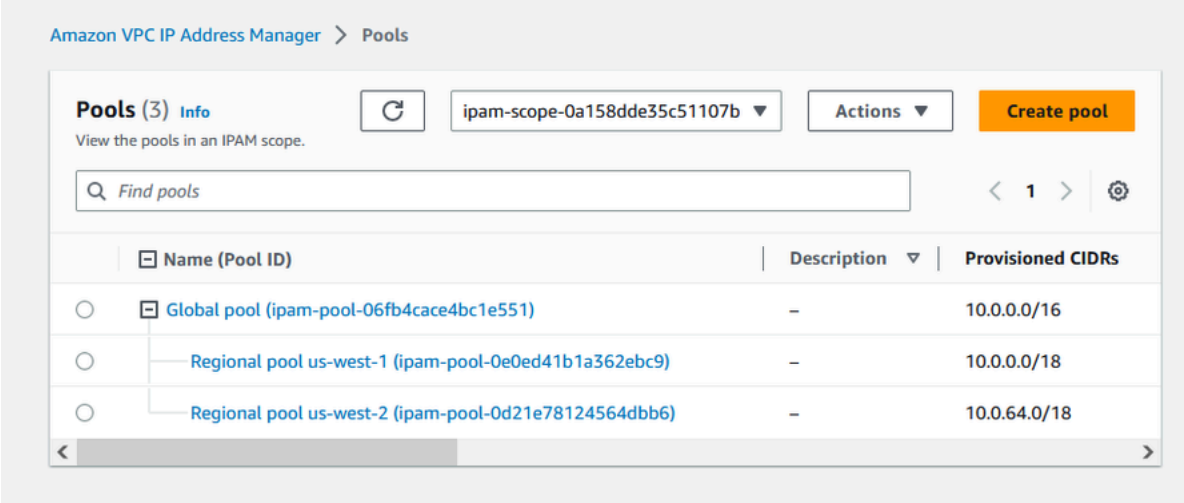
10. Biarkan Konfigurasi pengaturan aturan alokasi kumpulan ini dinonaktifkan. Anda tidak akan CIDRs mengalokasikan VPCs langsung dari kolam ini. Sebagai gantinya, Anda akan mengalokasikannya dari sub-pool yang Anda buat dari kolam ini.



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-west-2 dengan CIDR 10.0.64.0/18 yang disediakan untuknya. Saat Anda menyelesaikan proses itu, Anda akan memiliki tiga kumpulan dalam hierarki yang mirip dengan yang ini:

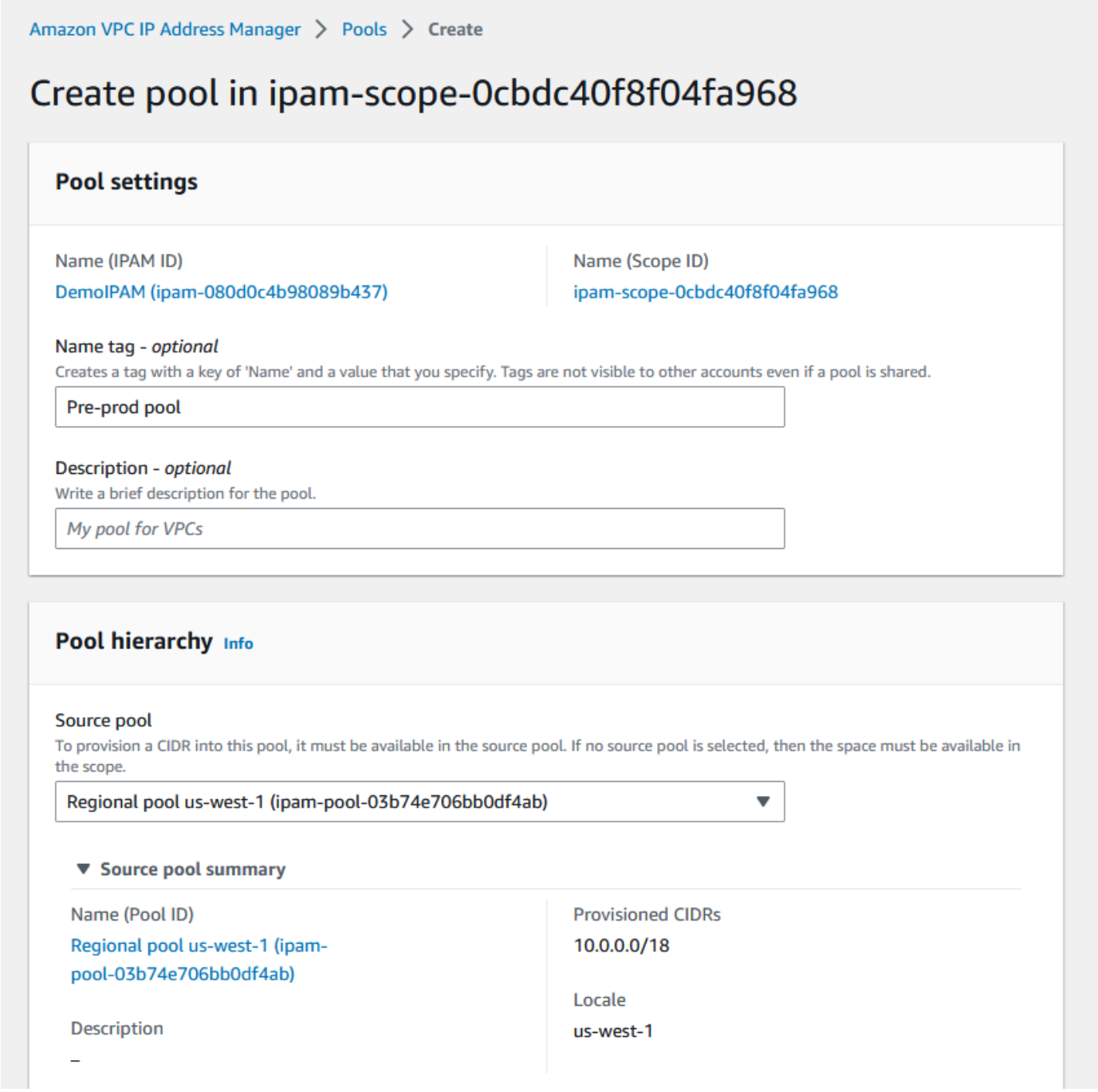


Langkah 5: Buat kumpulan pengembangan pra-produksi

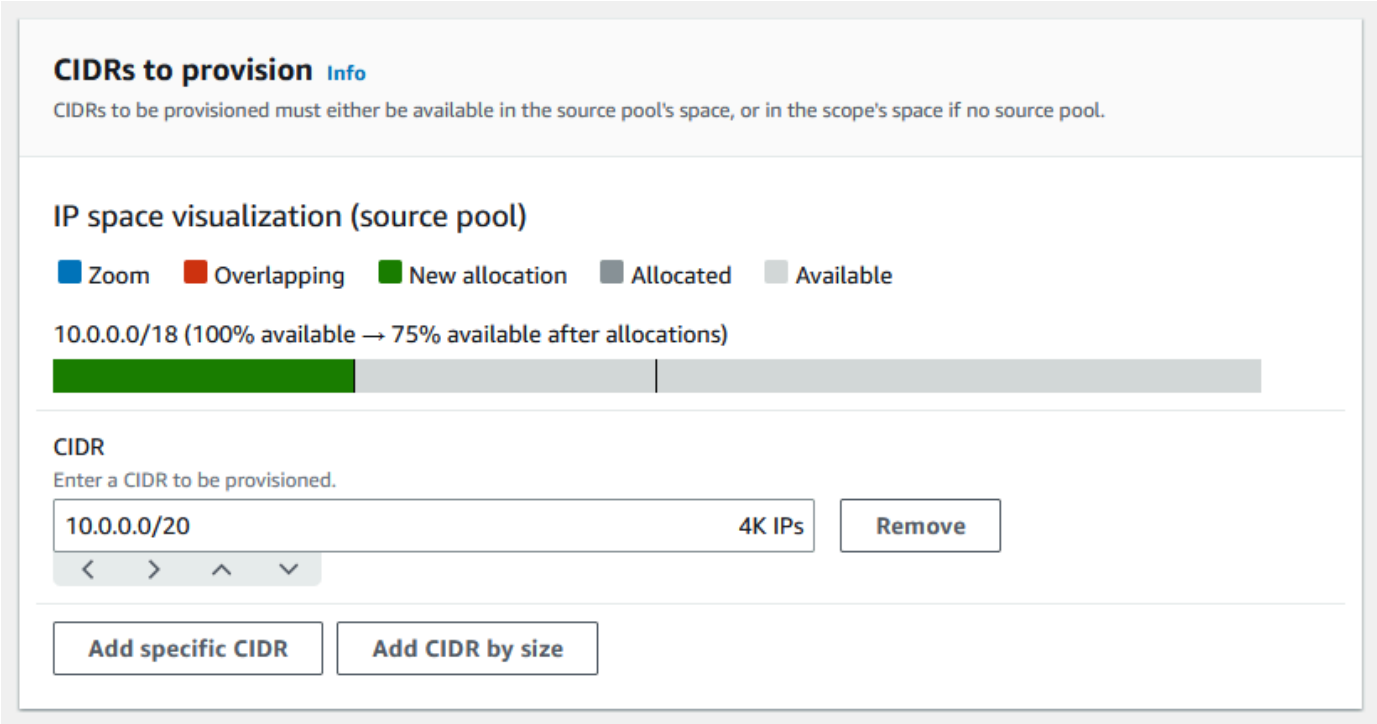
Ikuti langkah-langkah di bagian ini untuk membuat kumpulan pengembangan untuk sumber daya pra-produksi dalam salah satu kumpulan Regional Anda.

Untuk membuat kolam pengembangan pra-produksi

1. Dengan cara yang sama seperti yang Anda lakukan di bagian sebelumnya, menggunakan akun admin IPAM, buat kumpulan yang disebut kolam pra-Prod, tetapi kali ini gunakan kumpulan Regional us-west-1 sebagai kumpulan sumber.

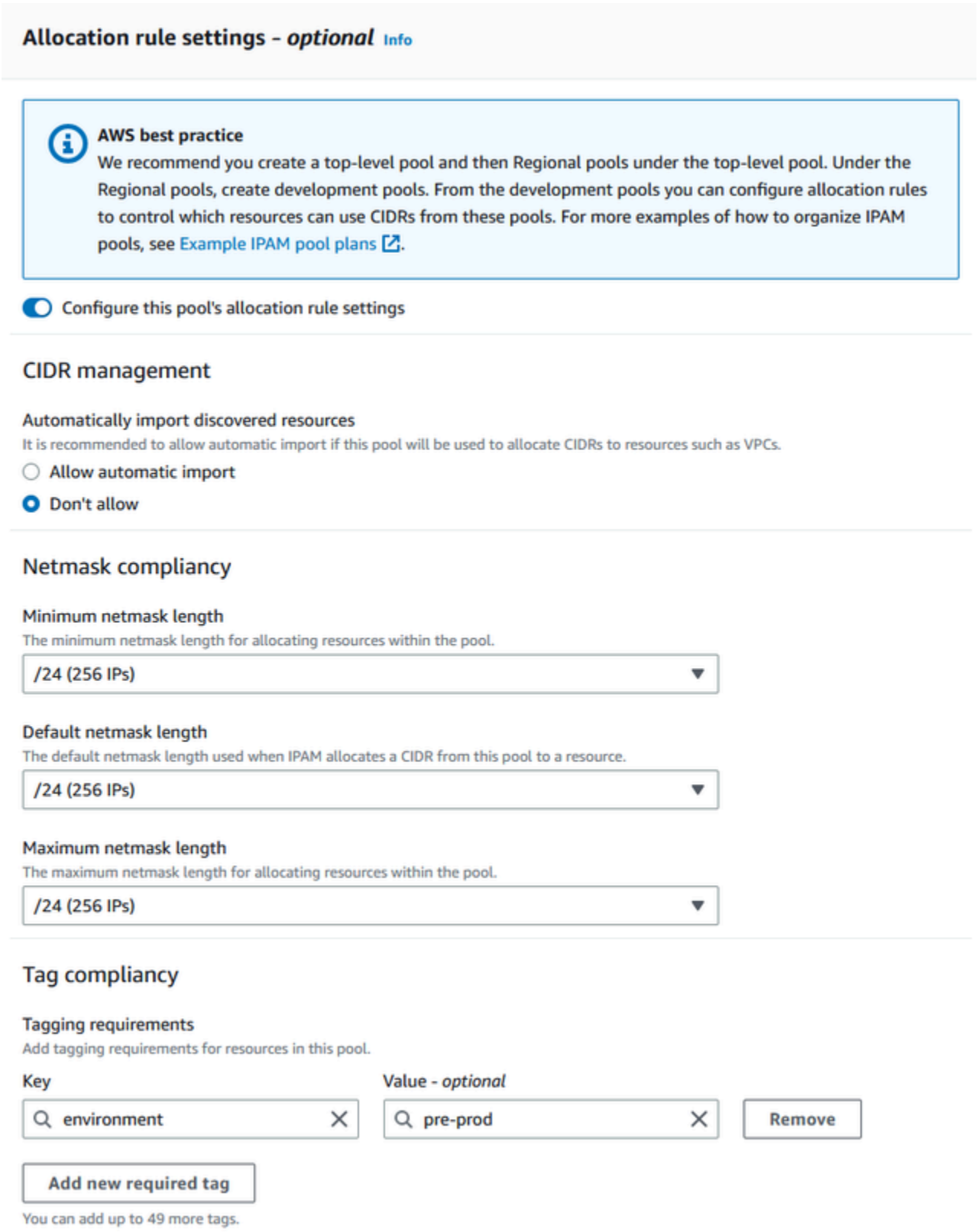


2. Tentukan CIDR 10.0.0.0/20 ke ketentuan, yang akan memberikan kumpulan ini sekitar 4.000 alamat IP.



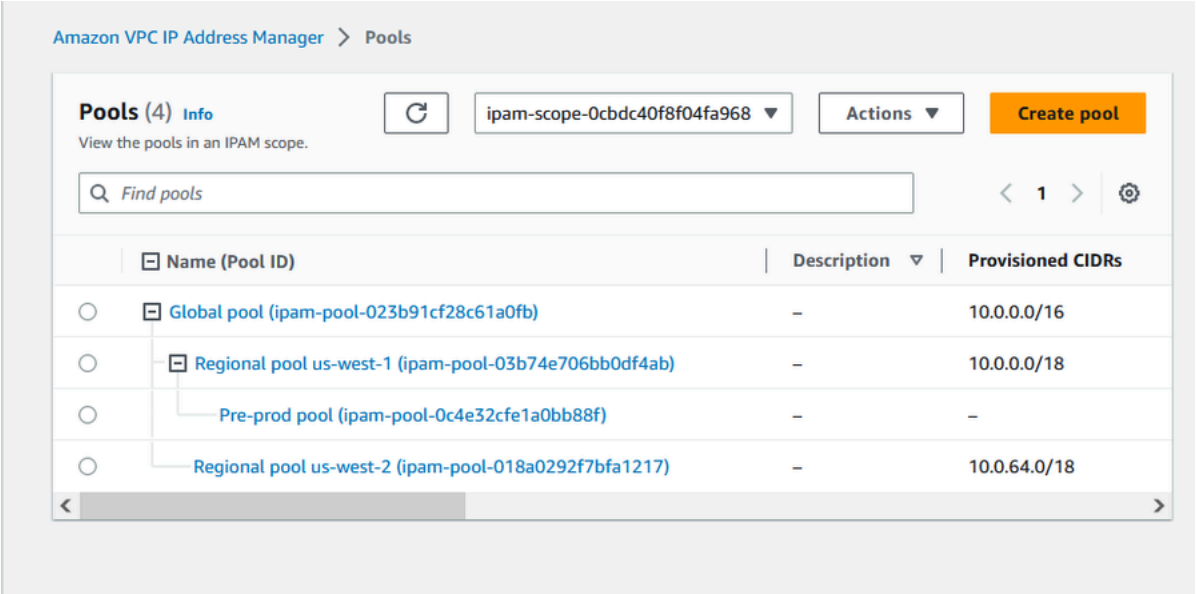
3. Alihkan opsi untuk Mengonfigurasi pengaturan aturan alokasi kumpulan ini. Lakukan hal-hal berikut:

    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 sumber daya CIDRs 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 tingkat atas IPv4.
    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 tingkat atas IPv4. 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 VPCs 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 kumpulan Regional 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:

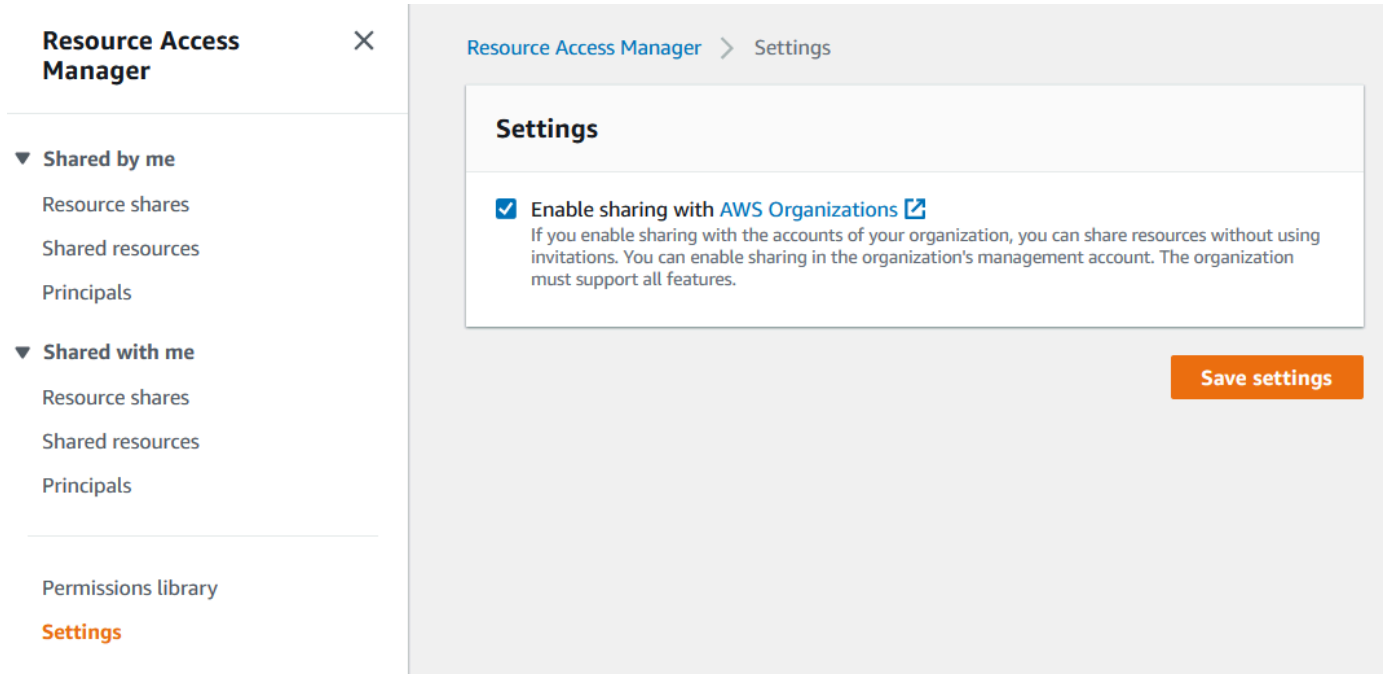
- Langkah 6.1. Aktifkan berbagi sumber daya di AWS RAM: Langkah ini harus dilakukan oleh akun AWS Organizations manajemen.
- Langkah 6.2. Bagikan kolam IPAM menggunakan AWS RAM: Langkah ini harus dilakukan oleh admin IPAM.

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.

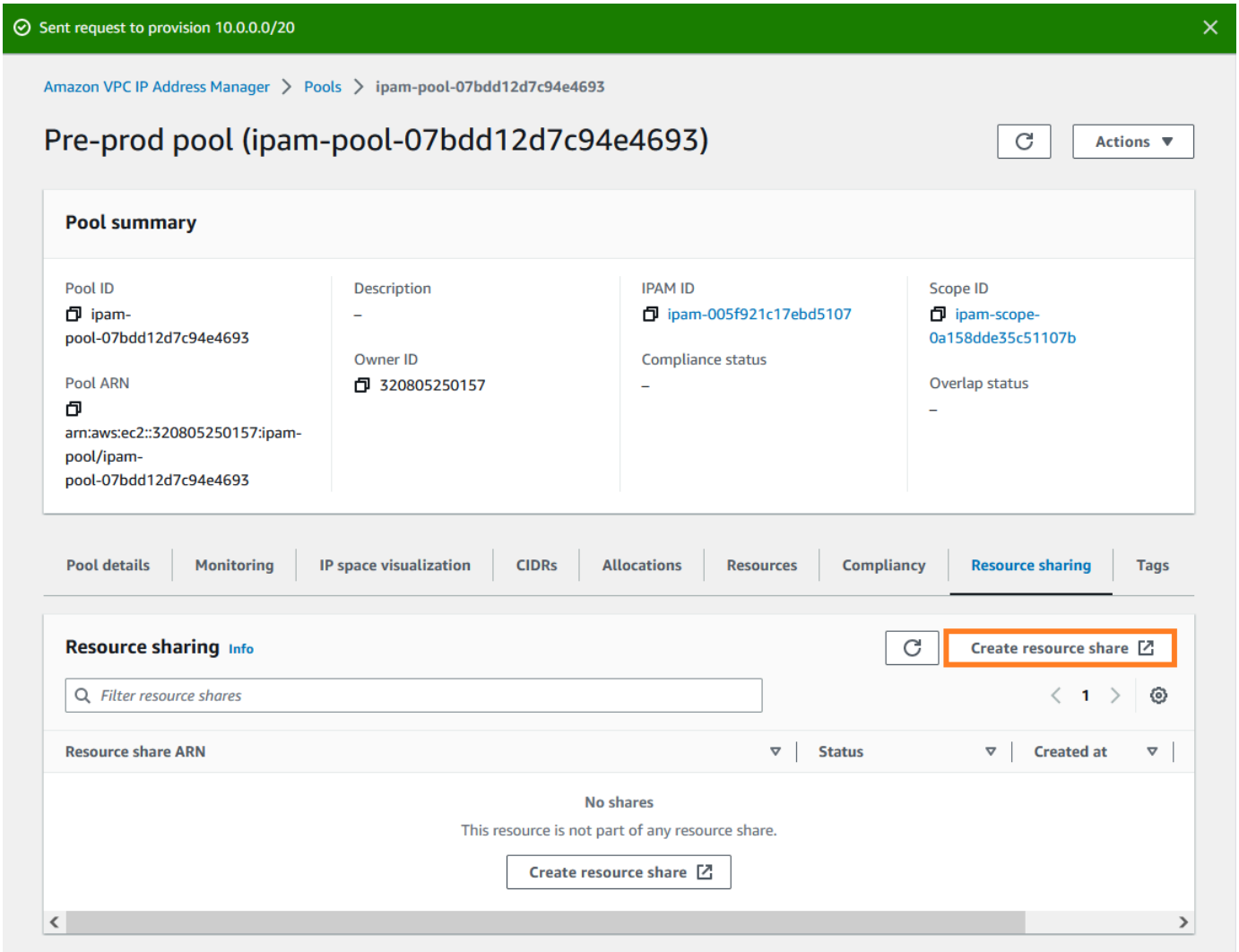
Langkah 6.2. Bagikan kolam IPAM menggunakan AWS RAM

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. Bagikan kolam IPAM menggunakan AWS RAM

Untuk berbagi kolam IPAM menggunakan AWS RAM

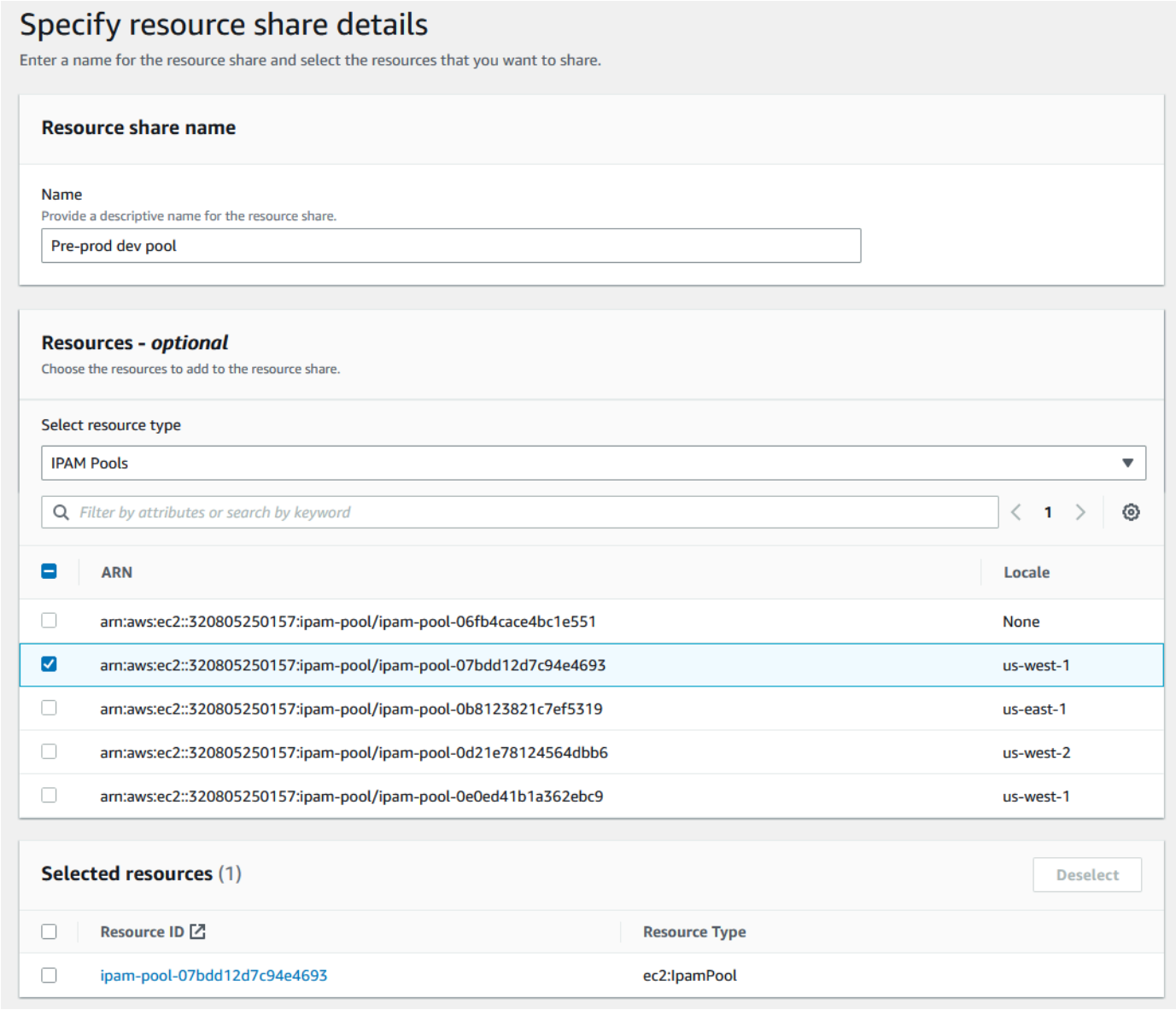
1. Menggunakan akun admin IPAM, buka konsol IPAM di. https://console.aws.amazon.com/ipam/
2. Di panel navigasi, pilih Pools.
3. Pilih ruang lingkup pribadi, pilih kolam IPAM pra-produksi, dan pilih Tindakan > Lihat detail.
4. Di bawah Berbagi sumber daya, pilih Buat berbagi sumber daya. AWS RAM Konsol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

5. Pilih Buat berbagi sumber daya.

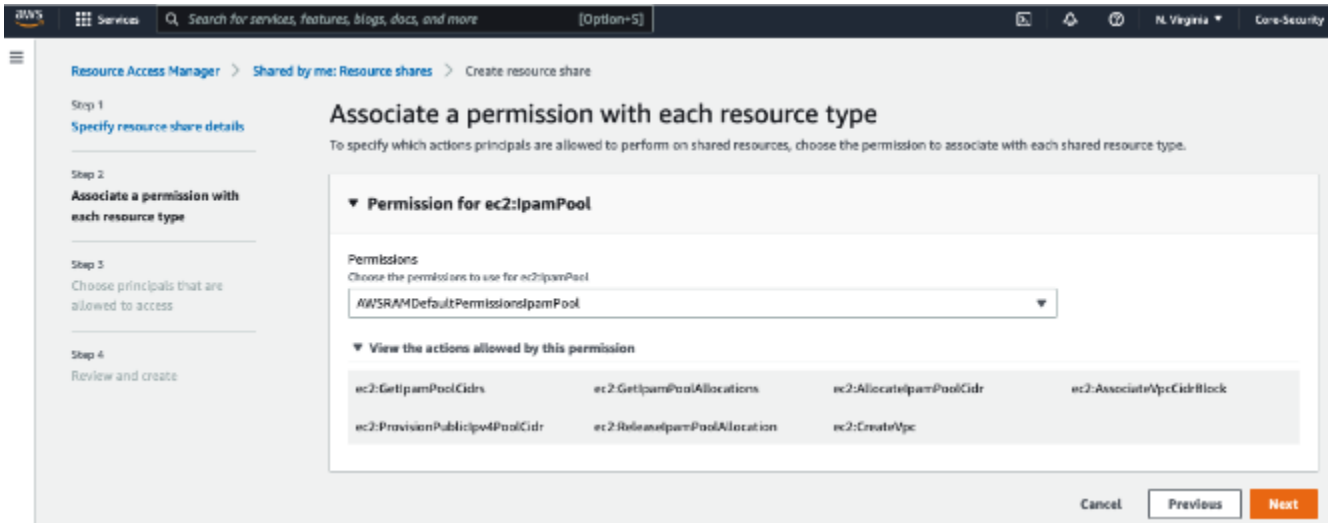


AWS RAM Konsol terbuka.

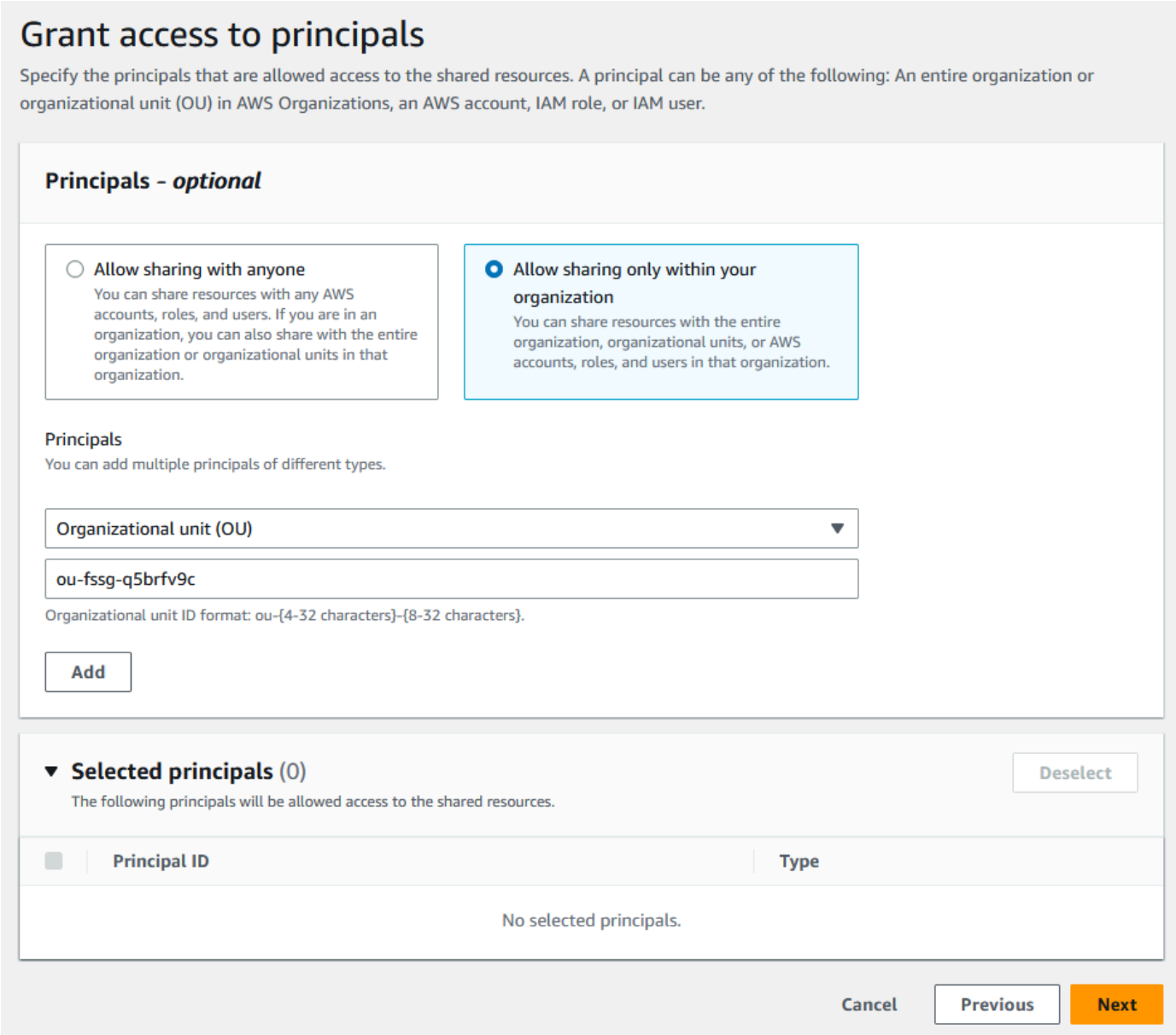
6. Di AWS RAM konsol, pilih Buat berbagi sumber daya lagi.
7. Tambahkan Nama untuk kolam bersama.
8. Di bawah Pilih jenis sumber daya, pilih kolam IPAM, lalu pilih ARN dari kumpulan pengembangan pra-produksi.



9. Pilih Berikutnya.
10. Biarkan AWSRAMDefaultPermissionsIpamPoolizin default dipilih. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diBagikan kolam IPAM menggunakan AWS RAM.



11. Pilih Berikutnya.
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 Berikutnya.
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.

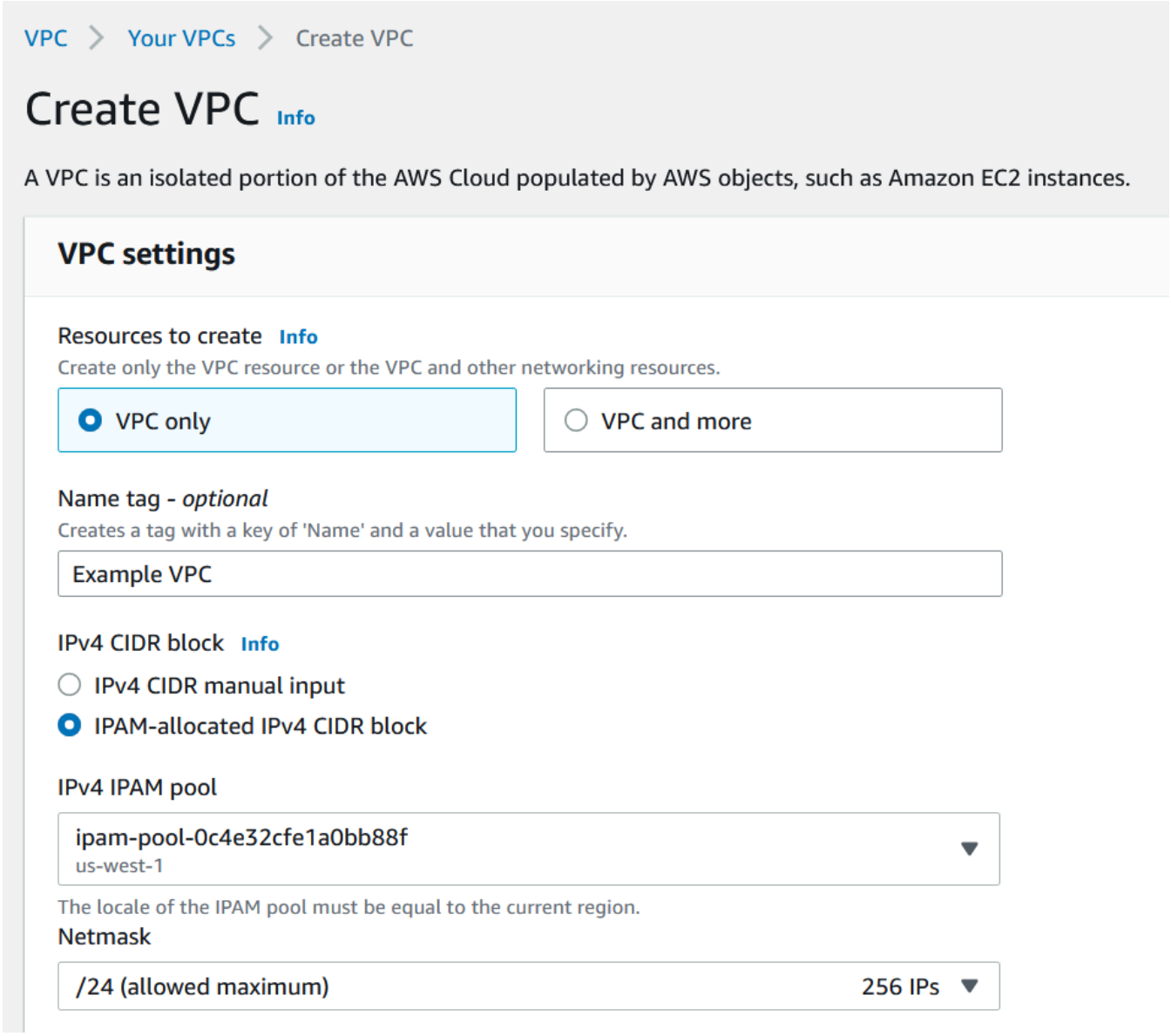
Langkah 7: Buat VPC dengan CIDR yang dialokasikan dari kolam IPAM

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 VPCs, lihat contoh kebijakan Amazon VPC di Panduan Pengguna Amazon VPC.

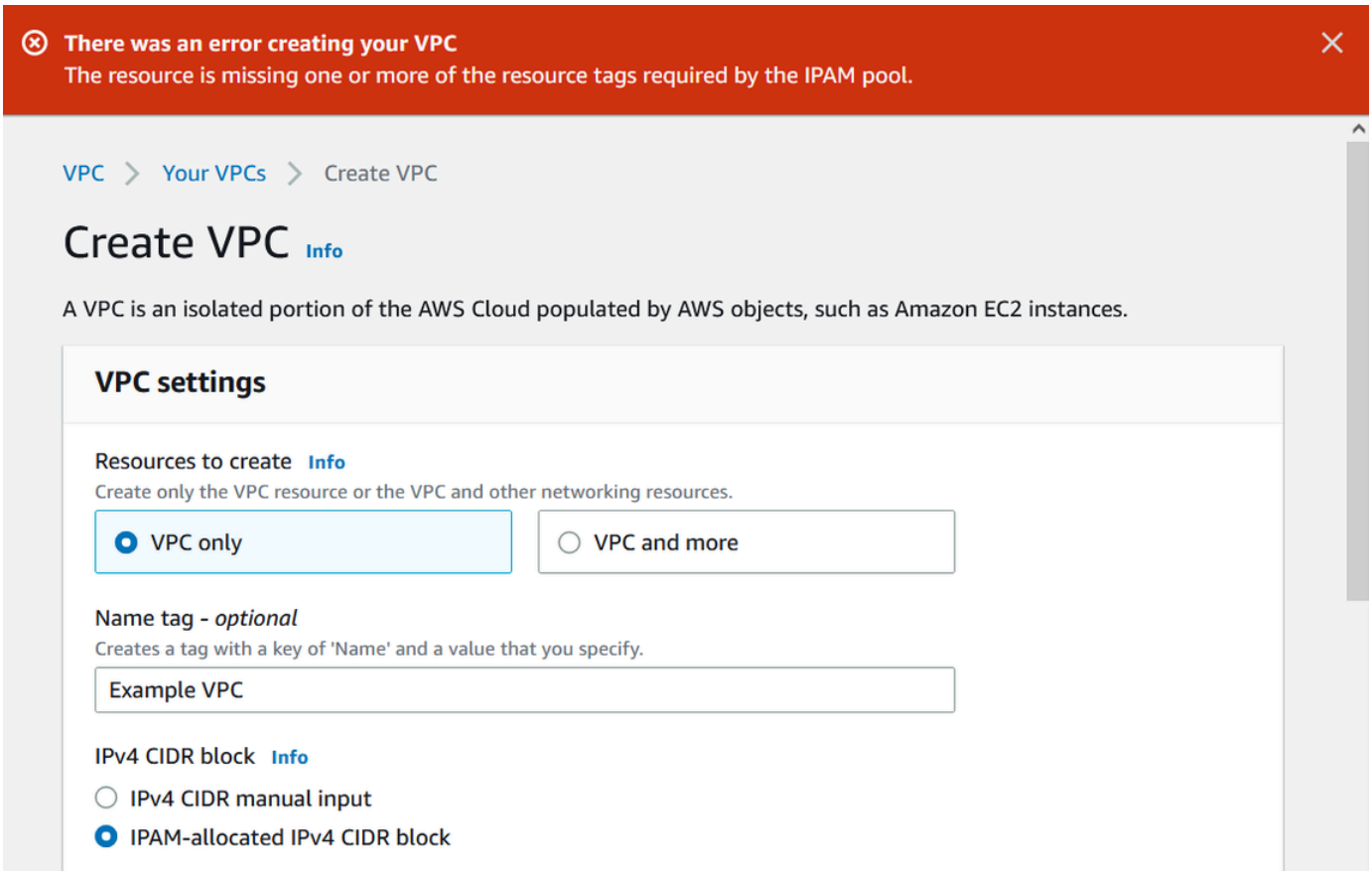
Untuk membuat VPC dengan CIDR yang dialokasikan dari kolam IPAM

1. Dengan menggunakan akun anggota, buka konsol VPC https://console.aws.amazon.com/vpc/sebagai akun anggota yang akan Anda gunakan sebagai akun pengembang.
2. Pilih Buat VPC.
3. Lakukan hal-hal berikut:
    1. Masukkan nama, seperti Contoh VPC.
    2. Pilih blok CIDR yang dialokasikan IPv4 IPAM.
    3. Di bawah kolam IPv4 IPAM, pilih ID 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.

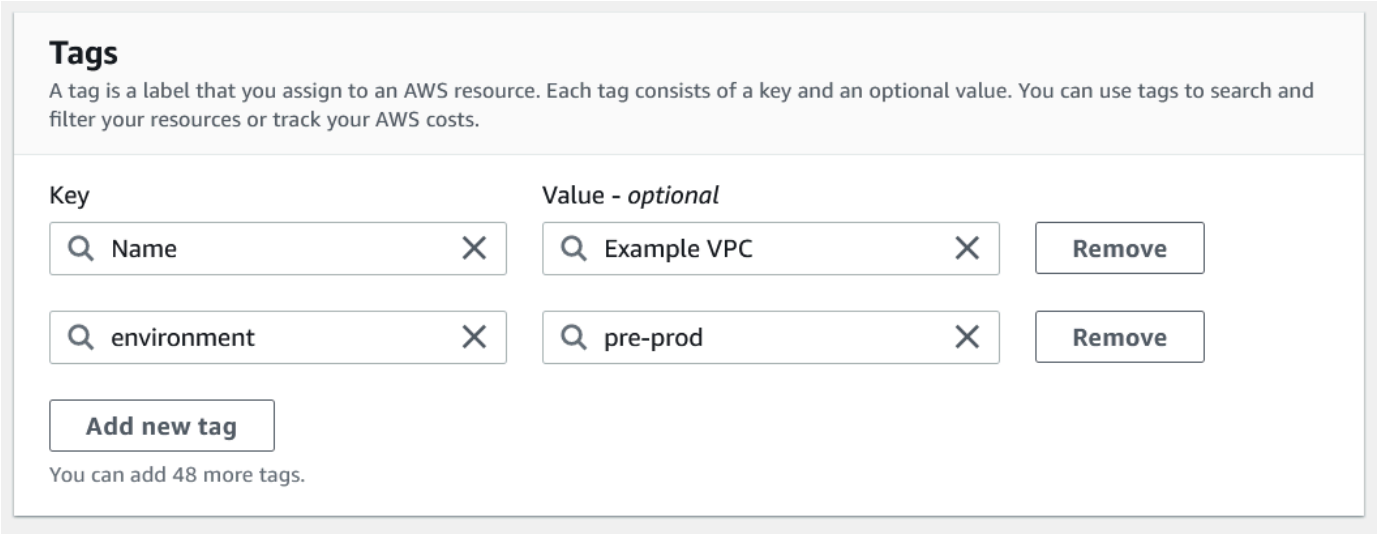


4. Untuk tujuan demonstrasi, di bawah Tag, jangan menambahkan tag tambahan saat ini. Saat Anda membuat pra-prod pool (inLangkah 5: Buat kumpulan pengembangan pra-produksi), Anda menambahkan aturan alokasi yang mengharuskan semua VPCs yang dibuat dengan CIDRs dari kumpulan ini untuk menonaktifkan tag environment/pre-prod tag. Leave the environment/pre - 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

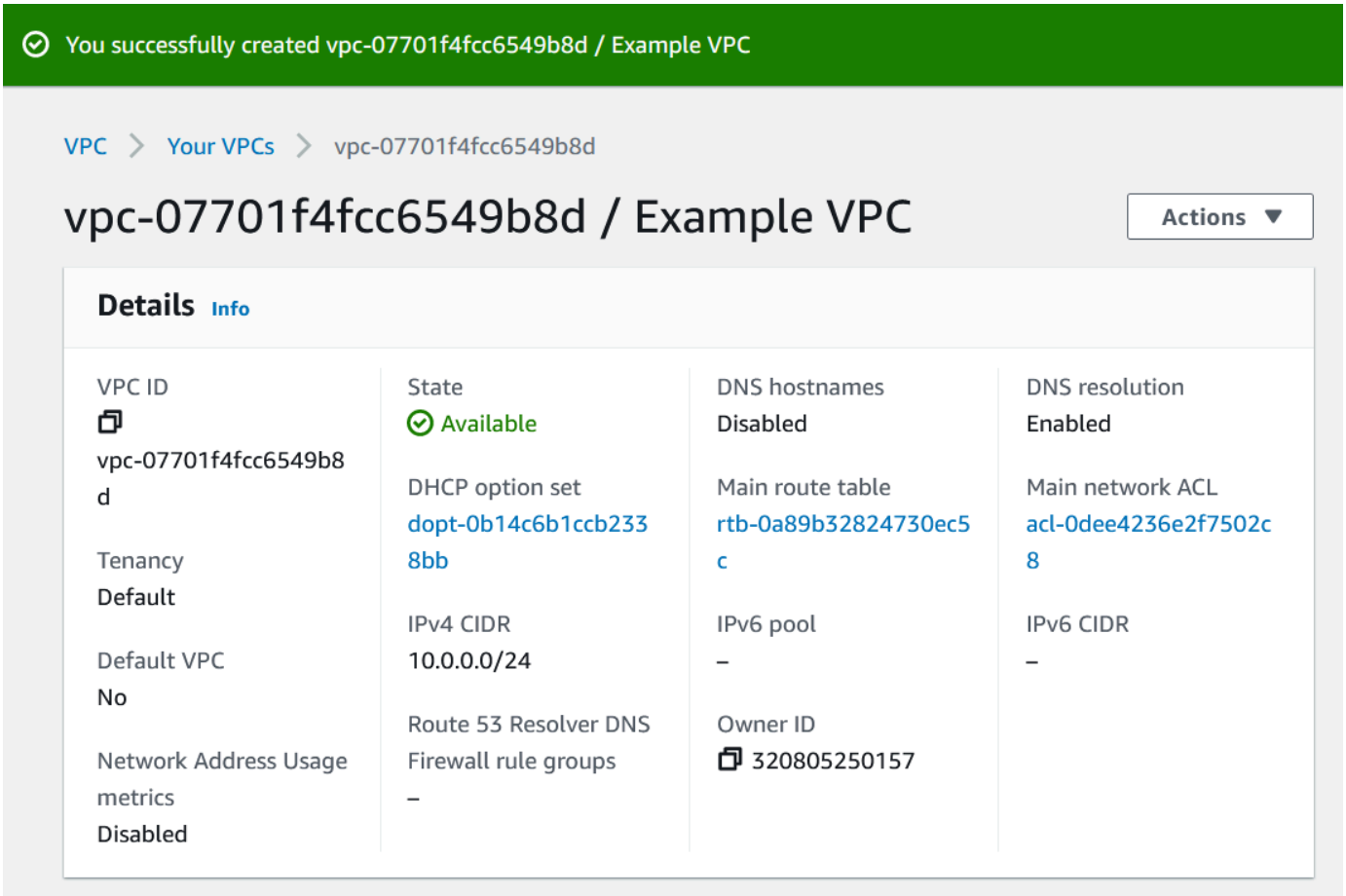
semua VPCs yang dibuat dengan CIDRs dari kumpulan ini untuk memiliki tag lingkungan/pra-prod.



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

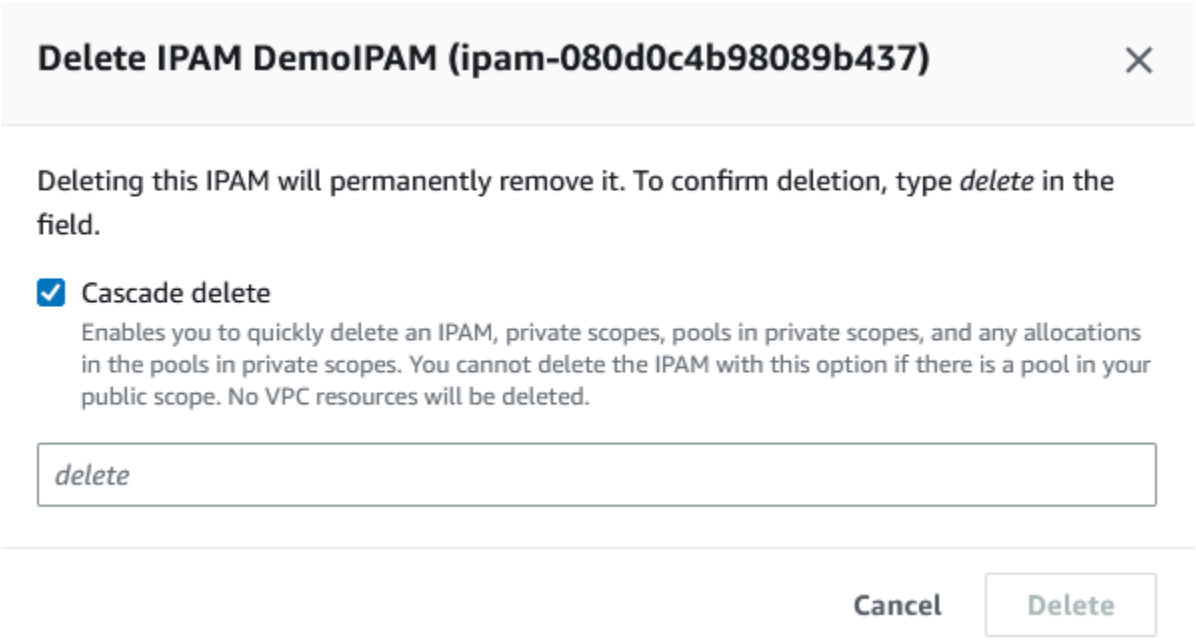
Dalam tutorial ini, Anda membuat IPAM dengan admin yang didelegasikan, membuat beberapa pool, dan mengaktifkan akun anggota di organisasi Anda untuk mengalokasikan CIDR VPC dari pool.

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 mendetail, 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 petunjuk mendetail, lihat Hapus 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 dengan AWS Organizations, IPAM secara otomatis membuat peran terkait layanan di setiap akun anggota. Menggunakan setiap akun AWS Organizations anggota, masuk ke IAM dan hapus peran terkait layanan AWSServiceRoleForIPAM di setiap akun anggota.
9. Pembersihan selesai.

Tutorial: Buat IPAM dan pool menggunakan AWS CLI

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

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

- IPAM beroperasi di AWS Wilayah 1, AWS Wilayah 2
  - Ruang lingkup pribadi
    - Kolam renang tingkat atas
      - Kolam renang regional di AWS 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 Anda

Langkah ini bersifat opsional. Selesaikan langkah ini untuk mengaktifkan IPAM di organisasi Anda dan mengkonfigurasi IPAM yang didelegasikan menggunakan CLI. AWS Untuk informasi selengkapnya tentang peran akun IPAM, lihatIntegrasikan IPAM dengan akun di Organisasi AWS.

Permintaan ini harus dibuat dari akun manajemen AWS 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, yang menunjukkan bahwa pengaktifan berhasil.

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

Langkah 2: Buat IPAM

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

> **Note**
>
> Opsi Wilayah operasi menentukan AWS Wilayah mana kolam IPAM dapat digunakan. Untuk informasi selengkapnya tentang Wilayah operasi, lihatBuat IPAM.

Untuk membuat IPAM menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat instance IPAM.

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

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

   - Mengembalikan ID sumber daya unik global (`IpamId`) untuk IPAM.
   - Membuat lingkup publik default (`PublicDefaultScopeId`) dan cakupan 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 untuk melihat 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 cakupan 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 kumpulan IPv4 alamat

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

> **Important**
>
> Anda tidak akan menggunakan `--locale` opsi di kolam tingkat atas ini. Anda akan mengatur opsi lokal nanti di kolam Regional. Lokalnya adalah Wilayah AWS tempat Anda ingin kumpulan tersedia untuk alokasi CIDR. Karena tidak menyetel lokal di kolam tingkat atas, lokal akan menjadi default. None Jika kolam memiliki lokalNone, kolam tidak akan tersedia

untuk sumber daya VPC di AWS Wilayah mana pun. Anda hanya dapat mengalokasikan ruang alamat IP secara manual di kolam untuk memesan ruang.

Untuk membuat kumpulan IPv4 alamat untuk semua sumber AWS daya Anda menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat kumpulan IPv4 alamat. Gunakan ID lingkup pribadi IPAM yang Anda buat pada 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 status `create-in-progress` untuk kolam.

```
{
    "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 status `create-complete` dalam output.

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

   Contoh output 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 ke kolam tingkat atas

Ikuti langkah-langkah di bagian ini untuk menyediakan CIDR ke kumpulan tingkat atas, lalu verifikasi bahwa CIDR telah disediakan. Untuk informasi selengkapnya, lihat Penyediaan CIDRs ke kolam.

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-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 status `provisioned` dalam output.

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

Contoh output 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 tingkat atas

Saat Anda membuat kolam IPAM, kolam tersebut milik AWS 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 saat membuat kolam untuk membuat kolam tersedia untuk layanan di Wilayah selain Wilayah IPAM. Ikuti langkah-langkah di bagian ini untuk membuat kumpulan Regional di lokal lain.

Untuk membuat pool dengan CIDR yang bersumber dari pool sebelumnya menggunakan AWS CLI

1. Jalankan perintah berikut untuk membuat pool dan menyisipkan spasi dengan CIDR yang tersedia 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
```

Dalam output, Anda akan melihat ID dari pool yang Anda buat. Anda akan memerlukan 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 status `create-complete` dalam output.

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

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.

```
{
    "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 kumpulan, dan memvalidasi bahwa blok tersebut telah berhasil disediakan.

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-0da89c821626f1e4b --cidr 10.0.0.0/16
```

   Dalam output, Anda melihat keadaan kolam.

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

```
        "Cidr": "10.0.0.0/16",
        "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-0da89c821626f1e4b
```

Contoh output berikut menunjukkan keadaan yang benar.

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

3. Jalankan perintah berikut untuk menanyakan kumpulan tingkat atas untuk melihat alokasi. Kolam Regional dianggap sebagai alokasi di dalam kolam tingkat atas.

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

Dalam output, Anda melihat kumpulan 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 penugasan IP di seluruh akun

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

Saat Anda membuat berbagi AWS RAM kolam IPAM, ini memungkinkan penetapan IP di seluruh akun. Berbagi RAM hanya tersedia di AWS Wilayah asal Anda. Perhatikan bahwa Anda membuat share ini di Region yang sama dengan IPAM, bukan di Region lokal untuk pool. Semua operasi administrasi pada sumber daya IPAM dilakukan melalui Wilayah asal IPAM Anda. Contoh dalam tutorial ini membuat 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, lihatBagikan kolam IPAM menggunakan AWS RAM.

Jalankan perintah berikut untuk membuat berbagi 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 pool 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 tetapkan blok CIDR ke VPC dari kumpulan di IPAM yang baru Anda buat.

```
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 daya IPAM yang telah Anda buat dalam tutorial ini.

1. Hapus VPC.

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

2. Hapus berbagi 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. Kolam deprovision CIDR dari kolam Regional.

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

4. Kolam deprovision 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 menggunakan AWS CLI

Skenario di bagian ini menunjukkan kepada Anda cara menganalisis dan mengaudit penggunaan alamat IP menggunakan AWS CLI. Untuk informasi umum tentang penggunaan AWS CLI, lihat Menggunakan AWS CLI dalam Panduan Pengguna Antarmuka Baris AWS Perintah.

Daftar Isi

Ikhtisar

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 historis untuk jenis sumber daya berikut:

- VPCs
- Subnet VPC
- Alamat IP elastis
- Instans EC2 yang sedang berjalan
- 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 antarmuka jaringan. CIDRs

Note

- Perintah dalam tutorial ini harus dijalankan menggunakan akun yang memiliki IPAM dan AWS Wilayah yang menghosting IPAM.
- Catatan perubahan CIDRs diambil dalam snapshot periodik, yang berarti perlu beberapa waktu untuk rekaman muncul atau diperbarui, dan nilai untuk SampledStartTime dan SampledEndTime dapat berbeda dari waktu aktual mereka terjadi.

Skenario

Skenario di bagian ini menunjukkan kepada Anda cara menganalisis dan mengaudit penggunaan alamat IP menggunakan AWS CLI. Untuk informasi lebih lanjut tentang nilai-nilai yang disebutkan dalam tutorial ini seperti contoh waktu akhir dan waktu mulai, lihatLihat riwayat alamat IP.

Skenario 1: Sumber daya apa yang dikaitkan **`10.2.1.155/32`** antara 1:00 dan 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. Dalam 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 selengkapnya tentang nilai-nilai yang ditunjukkan pada 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 instance tempat antarmuka jaringan terpasang berbeda dari ID pemilik antarmuka jaringan (seperti halnya gateway NAT, antarmuka jaringan Lambda, dan AWS layanan lainnya), itu `ResourceOwnerId` `amazon-aws` bukan ID akun pemilik antarmuka jaringan. VPCs Contoh berikut menunjukkan catatan untuk CIDR yang 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 **`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. Dalam contoh di bawah ini, CIDR dialokasikan ke subnet dan VPC selama periode waktu. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi selengkapnya tentang nilai-nilai yang ditunjukkan pada 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 **2605:9cc0:409::/56** dari 1 Desember 2021 hingga 27 Desember 2021 (UTC)?

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

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 2605:9cc0:409::/56 --
ipam-scope-id ipam-scope-07cb485c8b4a4d7cc --start-time 2021-12-01T01:00:00.000Z --
end-time 2021-12-27T23:59:59.000Z
```

2. Lihat hasil analisis. Dalam contoh di bawah ini, CIDR dialokasikan ke dua yang berbeda VPCs selama periode waktu di suatu Wilayah di luar Wilayah asal IPAM. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi selengkapnya tentang nilai-nilai yang ditunjukkan pada 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 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. Dalam contoh di bawah ini, CIDR telah dialokasikan ke banyak subnet dan VPCs selama periode waktu. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi selengkapnya tentang nilai-nilai yang ditunjukkan pada 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 apa 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. Dalam 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 selengkapnya tentang nilai-nilai yang ditunjukkan pada 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 apa 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. Dalam contoh di bawah ini, CIDR dialokasikan ke VPC dan subnet selama periode waktu. Hanya hasil yang cocok dengan /24 CIDR persis ini yang dikembalikan, tidak semua /32 dalam /24 CIDR. Perhatikan bahwa tidak ada SampledEndTimenilai berarti catatan masih aktif. Untuk informasi selengkapnya tentang nilai-nilai yang ditunjukkan pada 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 apa yang saat ini terkait**54.0.0.9/32**?

Dalam contoh ini, 54.0.0.9/32 ditetapkan ke alamat IP Elastis yang bukan bagian dari AWS 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. Karena 54.0.0.9/32 ditetapkan ke alamat IP Elastis yang bukan bagian dari AWS 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 (ASNs) yang diizinkan oleh mitra atau pelanggan Anda yang tercantum 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 (ISPs), misalnya, digunakan ASNs untuk mengidentifikasi sumber lalu lintas jaringan. Tidak semua organisasi membeli sendiri ASNs, tetapi untuk organisasi yang melakukannya, mereka dapat membawa ASN mereka. AWS

Bawa nomor sistem otonom Anda sendiri (BYOASN) memungkinkan Anda untuk mengiklankan IPv4 atau IPv6 alamat 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 Amazon. EC2
- Saat Anda membawa rentang IPv6 alamat IPv4 atauTutorial: Bawa alamat IP Anda ke IPAM, Anda membuat sertifikat X.509 dan mengunggah sertifikat X.509 ke catatan RDAP di RIR Anda. AWS 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.
- Saat Anda membawa rentang alamat IP ke IPAM, Anda membuat ROA untuk memverifikasi bahwa Anda mengontrol ruang alamat IP yang Anda bawa ke IPAM. Selain ROA itu, Anda harus memiliki ROA kedua di RIR Anda dengan ASN yang Anda bawa ke IPAM. Jika Anda tidak memiliki ROA kedua ini untuk ASN di RIR Anda, selesaikan 3. Buat objek ROA di RIR Anda. Abaikan langkah-langkah lainnya.

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 BYOASNstab dan pilih Ketentuan 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 ASNs. Untuk meningkatkan kuota ini, lihatKuota untuk IPAM Anda.
10. Pilih Ketentuan.
11. Lihat proses penyediaan di tab. BYOASNs Tunggu Negara berubah dari Pending-provision ke Provisioned. BYOASNs dalam status Gagal ketentuan 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, lihatBagaimana IPAM bekerja.
14. Pilih kolam regional yang memiliki BYOIP CIDR yang disediakan untuknya. Kolam harus memiliki Layanan yang disetel ke EC2dan harus memiliki lokal yang dipilih.
15. Pilih CIDRstab dan pilih BYOIP CIDR.
16. Pilih Tindakan > Kelola asosiasi BYOASN.

17. Di bawah Associated BYOASNs, pilih ASN yang Anda bawa. AWS Jika Anda memiliki beberapa ASNs, Anda dapat mengaitkan beberapa ASNs ke BYOIP CIDR. Anda dapat mengasosiasikan ASNs sebanyak yang dapat Anda bawa ke IPAM. Perhatikan bahwa Anda dapat membawa hingga 5 ASNs 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 CIDRstab kolam renang.
21. Pilih CIDR BYOIP dan pilih Actions > Advertise. Akibatnya, opsi ASN Anda ditampilkan: Amazon ASN dan apa pun yang ASNs 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 membatalkan ASN, di BYOASNs tab, pilih ASN dan pilih Deprovision ASN. Akibatnya, ASN dideprovisi. 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 Amazon ASNs 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 BYOIP CIDRs 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 ke sumber daya seperti instans EC2 dan penyeimbang beban aplikasi. Tanpa IPAM, Anda harus mengangkut publik Anda IPs untuk setiap AWS Wilayah.

Daftar Isi

Verifikasi kontrol domain

Sebelum Anda membawa rentang alamat IP AWS, Anda harus menggunakan salah satu opsi yang dijelaskan di bagian ini untuk memverifikasi bahwa Anda mengontrol ruang alamat IP. Kemudian, ketika Anda membawa rentang alamat IP ke AWS, AWS memvalidasi bahwa Anda mengontrol rentang alamat IP. Validasi ini memastikan bahwa pelanggan tidak dapat menggunakan rentang IP milik orang lain, mencegah masalah perutean dan keamanan.

Ada dua metode yang dapat Anda gunakan untuk memverifikasi bahwa Anda mengontrol rentang:

- Sertifikat X.509: Jika rentang alamat IP Anda terdaftar dengan Internet Registry yang mendukung RDAP (seperti ARIN, RIPE dan APNIC), Anda dapat menggunakan sertifikat X.509 untuk memverifikasi kepemilikan domain Anda.
- Catatan DNS TXT: Terlepas dari apakah Registri Internet Anda mendukung RDAP, Anda dapat menggunakan token verifikasi dan catatan DNS TXT untuk memverifikasi kepemilikan domain Anda.

Daftar Isi

Verifikasi domain Anda dengan sertifikat X.509

Bagian ini menjelaskan cara memverifikasi domain Anda dengan sertifikat X.509 sebelum Anda membawa rentang alamat IP Anda ke IPAM.

Untuk memverifikasi domain Anda dengan sertifikat X.509

1. Selesaikan tiga langkah dalam Prasyarat untuk BYOIP di Amazon EC2 di Panduan Pengguna Amazon EC2.

   > **Note**
   >
   > Saat Anda membuat ROAs, untuk IPv4 CIDRs Anda harus mengatur panjang maksimum awalan alamat IP ke`/24`. Karena IPv6 CIDRs, jika Anda menambahkannya ke kumpulan yang dapat diiklankan, panjang maksimum awalan 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 IPv4 blok terkecil dan `/48` merupakan IPv6 blok terkecil yang dapat Anda iklankan dari Wilayah ke internet.

2. Selesaikan langkah 1 dan 2 hanya di bawah Menyediakan rentang alamat yang dapat diiklankan secara publik AWS di Panduan Pengguna Amazon EC2, dan jangan berikan rentang alamat (langkah 3). Simpan `text_message` dan`signed_message`. Anda akan membutuhkannya nanti dalam proses ini.

Setelah Anda menyelesaikan langkah-langkah ini, lanjutkan dengan Bawa IP Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS atauBawa IP CIDR Anda sendiri ke IPAM hanya menggunakan CLI AWS.

Verifikasi domain Anda dengan catatan DNS TXT

Selesaikan langkah-langkah di bagian ini untuk memverifikasi domain Anda dengan catatan DNS TXT sebelum Anda membawa rentang alamat IP Anda ke IPAM.

Anda dapat menggunakan data DNS TXT untuk memvalidasi bahwa Anda mengontrol rentang alamat IP publik. Catatan DNS TXT adalah jenis catatan DNS yang berisi informasi tentang nama domain Anda. Fitur ini memungkinkan Anda untuk membawa alamat IP yang terdaftar dengan registri internet apa pun (seperti JPNIC, LACNIC, dan AFRINIC), bukan hanya alamat yang mendukung validasi berbasis catatan RDAP (Registration Data Access Protocol) (seperti ARIN, RIPE dan APNIC).

> **Important**
>
> Sebelum Anda dapat melanjutkan, Anda harus sudah membuat IPAM di Tingkat Gratis atau Tingkat Lanjut. Jika Anda tidak memiliki IPAM, selesaikan Buat IPAM terlebih dahulu.

Daftar Isi

Langkah 1: Buat ROA jika Anda tidak memilikinya

Anda harus memiliki Otorisasi Asal Rute (ROA) di Regional Internet Registry (RIR) untuk rentang alamat IP yang ingin Anda iklankan. Jika Anda tidak memiliki ROA di RIR Anda, selesaikan 3. Buat objek ROA di RIR Anda di Panduan Pengguna Amazon EC2. Abaikan langkah-langkah lainnya.

Rentang IPv4 alamat paling spesifik yang dapat Anda bawa adalah/24. Rentang IPv6 alamat paling spesifik yang dapat Anda bawa adalah/48 untuk CIDRs yang dapat diiklankan secara publik dan /60 untuk CIDRs yang tidak dapat diiklankan secara publik.

Langkah 2. Buat token verifikasi

Token verifikasi adalah nilai acak AWS yang dihasilkan yang dapat Anda gunakan untuk membuktikan kontrol sumber daya eksternal. Misalnya, Anda dapat menggunakan token verifikasi

untuk memvalidasi bahwa Anda mengontrol rentang alamat IP publik saat Anda membawa rentang alamat IP ke AWS (BYOIP).

Selesaikan langkah-langkah di bagian ini untuk membuat token verifikasi yang Anda perlukan di langkah selanjutnya dalam tutorial ini untuk membawa rentang alamat IP Anda ke IPAM. Gunakan petunjuk di bawah ini untuk AWS konsol atau AWS CLI.

AWS Management Console

Untuk membuat token verifikasi

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di Konsol AWS Manajemen, pilih AWS Wilayah tempat Anda membuat IPAM.
3. Di panel navigasi kiri, pilih IPAMs.
4. Pilih IPAM Anda dan kemudian pilih tab Token verifikasi.
5. Pilih Buat token verifikasi.
6. Setelah Anda membuat token, biarkan tab browser ini terbuka. Anda akan memerlukan nilai Token, nama Token di langkah berikutnya dan ID Token di langkah selanjutnya.

Perhatikan hal-hal berikut:

- Setelah Anda membuat token verifikasi, Anda dapat menggunakan kembali token untuk beberapa BYOIP CIDRs yang Anda berikan dari IPAM Anda dalam waktu 72 jam. Jika Anda ingin menyediakan lebih banyak CIDRs setelah 72 jam, Anda memerlukan token baru.
- Anda dapat membuat hingga 100 token. Jika Anda mencapai batas, hapus token yang kedaluwarsa.

Command line

- Minta IPAM membuat token verifikasi yang akan Anda gunakan untuk konfigurasi DNS dengan create-ipam-external-resource -verification-token:

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

Ini akan mengembalikan token IpamExternalResourceVerificationTokenId dan dengan `TokenName` dan`TokenValue`, dan waktu kedaluwarsa (`NotAfter`) token.

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

Perhatikan hal-hal berikut:

- Setelah Anda membuat token verifikasi, Anda dapat menggunakan kembali token untuk beberapa BYOIP CIDRs yang Anda berikan dari IPAM Anda dalam waktu 72 jam. Jika Anda ingin menyediakan lebih banyak CIDRs setelah 72 jam, Anda memerlukan token baru.
- Anda dapat melihat token Anda menggunakan describe-ipam-external-resource-verification-token.
- Anda dapat membuat hingga 100 token. Jika Anda mencapai batas, Anda dapat menghapus token kedaluwarsa menggunakan delete-ipam-external-resource-verification-token.

Langkah 3. Siapkan zona DNS dan catatan TXT

Selesaikan langkah-langkah di bagian ini untuk mengatur zona DNS dan catatan TXT. Jika Anda tidak menggunakan Route53 sebagai DNS Anda, ikuti dokumentasi yang disediakan oleh penyedia DNS Anda untuk menyiapkan Zona DNS dan menambahkan catatan TXT.

Jika Anda menggunakan Route53, perhatikan hal berikut:

- Untuk membuat Zona Pencarian Terbalik di AWS konsol, lihat Membuat zona yang dihosting publik di Panduan Pengembang Amazon Route 53 atau gunakan AWS CLI perintah create-hosted-zone.
- Untuk membuat rekaman di Zona Pencarian Terbalik di AWS konsol, lihat Membuat catatan menggunakan konsol Amazon Route 53 di Panduan Pengembang Amazon Route 53 atau gunakan AWS CLI perintah change-resource-record-sets.

- Setelah Anda selesai membuat zona yang dihosting, delegasikan zona yang dihosting dari RIR Anda ke server nama yang disediakan oleh Route53 (seperti untuk LACNIC atau APNIC).

Apakah Anda menggunakan penyedia DNS lain atau Route53, ketika Anda mengatur catatan TXT, perhatikan hal berikut:

- Nama rekaman harus nama token Anda.
- Jenis rekaman harus TXT.
- ResourceRecord Nilai harus menjadi nilai token.

Contoh:

- Nama: `86950620.113.0.203.in-addr.arpa`
- Jenis: TXT
- ResourceRecords Nilai: `a34597c3-5317-4238-9ce7-50da5b6e6dc8`

Di mana:

- `86950620`adalah nama token verifikasi.
- `113.0.203.in-addr.arpa`adalah nama Reverse Lookup Zone.
- `TXT`adalah tipe rekaman.
- `a34597c3-5317-4238-9ce7-50da5b6e6dc8`adalah nilai token verifikasi.

> **Note**
>
> Bergantung pada ukuran awalan yang akan dibawa ke IPAM dengan BYOIP, satu atau lebih catatan otentikasi harus dibuat di DNS. Catatan otentikasi ini adalah tipe rekaman TXT dan harus ditempatkan ke zona terbalik dari awalan itu sendiri atau awalan induknya.
>
> - Untuk IPv4, catatan otentikasi perlu menyelaraskan ke rentang pada batas oktet yang membentuk awalan.
>   - Contoh
>   - Untuk 198.18.123.0/24, yang sudah disejajarkan pada batas oktet, Anda perlu membuat catatan otentikasi tunggal di:

    - *token-name*.123.18.198.in-addr.arpa. IN TXT “*token-value*”
  - Untuk 198.18.12.0/22, yang dengan sendirinya tidak selaras dengan batas oktet, Anda perlu membuat empat catatan otentikasi. Catatan ini harus mencakup subnet 198.18.12.0/24, 198.18.13.0/24, 198.18.14.0/24, dan 198.18.15.0/24 yang disejajarkan pada batas oktet. Entri DNS yang sesuai harus:
    - *token-name*.12.18.198.in-addr.arpa. IN TXT “*token-value*”
    - *token-name*.13.18.198.in-addr.arpa. IN TXT “*token-value*”
    - *token-name*.14.18.198.in-addr.arpa. IN TXT “*token-value*”
    - *token-name*.15.18.198.in-addr.arpa. IN TXT “*token-value*”
  - Untuk 198.18.0.0/16, yang sudah disejajarkan pada batas oktet, Anda perlu membuat catatan otentikasi tunggal:
    - *token-name*.18.198.in-addr.arpa. IN TXT “*token-value*”
- Untuk IPv6, catatan otentikasi perlu disejajarkan ke rentang pada batas gigitan yang membentuk awalan. Nilai gigitan yang valid adalah misalnya 32, 36, 40, 44, 48, 52, 56, dan 60.
  - Contoh
    - Untuk 2001:0 db8: :/40, yang sudah disejajarkan pada batas nibble, Anda perlu membuat catatan otentikasi tunggal:
      - *token-name*.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT “*token-value*”
    - Untuk 2001:0 db 8:80: :/42, yang dengan sendirinya tidak selaras pada batas menggigit, Anda perlu membuat empat catatan otentikasi. Catatan ini harus mencakup subnet 2001:db 8:80: :/44, 2001:db 8:90: :/44, 2001:db8:a0: :/44, dan 2001:db8:b0: :/44 yang disejajarkan pada batas menggigit. Entri DNS yang sesuai harus:
      - *token-name*.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT “*token-value*”
      - *token-name*.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT “*token-value*”
      - *token-name*.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”
      - *token-name*.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”
    - Untuk rentang yang tidak diiklankan 2001:db 8:0:1000: :/54, yang dengan sendirinya tidak selaras pada batas menggigit, Anda perlu membuat empat catatan otentikasi. Catatan ini harus mencakup subnet 2001:db 8:0:1000: :/56, 2001:db 8:0:1100: :/56, 2001:db 8:0:1200: :/56, dan 2001:db 8:0:1300: :/56 yang disejajarkan pada batas menggigit. Entri DNS yang sesuai harus:

    - *token-name*.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”
    - *token-name*.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”
    - *token-name*.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”
    - *token-name*.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT “*token-value*”
  - Untuk memvalidasi jumlah angka heksadesimal yang benar antara nama token dan string “ip6.arpa”, kalikan angka dengan empat. Hasilnya harus sesuai dengan panjang awalan. Misalnya, untuk awalan /56 Anda harus memiliki 14 digit heksadesimal.

Setelah Anda menyelesaikan langkah-langkah ini, lanjutkan dengan Bawa IP Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS atauBawa IP CIDR Anda sendiri ke IPAM hanya menggunakan CLI AWS.

Bawa IP Anda sendiri ke IPAM menggunakan AWS Management Console dan CLI AWS

Membawa IP Anda Sendiri (BYOIP) ke IPAM memungkinkan Anda untuk menggunakan rentang IPv6 alamat IPv4 dan alamat yang ada di organisasi Anda. AWS Hal ini memungkinkan Anda untuk mempertahankan branding yang konsisten, meningkatkan kinerja jaringan, meningkatkan keamanan, dan menyederhanakan manajemen dengan menyatukan lingkungan lokal dan cloud di bawah ruang alamat IP Anda sendiri.

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

> **Note**
>
> Sebelum memulai, Anda harus memiliki kontrol domain yang diverifikasi terlebih dahulu.

Setelah Anda membawa rentang IPv4 alamat 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

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

Important

- 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 CIDRs dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

- Langkah 8: Pembersihan
- Alternatif untuk Langkah 6

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

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 CIDRs 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, lihatBagaimana IPAM bekerja.

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 Alamat keluarga, 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.

   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 BYOIP.
11. Berdasarkan CIDRs ketentuan, lakukan salah satu hal berikut:

    - Jika Anda memverifikasi kontrol domain Anda dengan sertifikat X.509, Anda harus menyertakan CIDR dan pesan BYOIP dan tanda tangan sertifikat yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.
    - Jika Anda memverifikasi kontrol domain Anda dengan catatan DNS TXT, Anda harus menyertakan token verifikasi CIDR dan IPAM yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.

    Perhatikan bahwa saat menyediakan IPv4 CIDR ke kolam dalam kumpulan tingkat atas, IPv4 CIDR minimum yang dapat Anda berikan adalah`/24`; lebih spesifik CIDRs (seperti`/25`) tidak diizinkan.

> **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.

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

Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan di CIDRstab 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 bagian dari salah satu Wilayah operasi yang Anda konfigurasikan saat Anda membuat IPAM. Misalnya, lokal us-east-1 berarti bahwa us-east-1 harus menjadi Wilayah operasi untuk IPAM. Lokal us-east-1-scl-1 (grup perbatasan jaringan yang digunakan untuk Local Zones) berarti bahwa IPAM harus memiliki Wilayah operasi us-east-1.

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, lihatBagaimana IPAM bekerja.
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.

   Tempat untuk pool harus salah satu berikut ini:

   - AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi.
   - Grup perbatasan jaringan untuk Zona AWS Lokal tempat Anda ingin kolam IPAM ini tersedia untuk alokasi (didukung Local Zones). Opsi ini hanya tersedia untuk IPv4 kolam IPAM di ruang lingkup publik.
   - Zona Lokal Khusus AWS. Untuk membuat kolam dalam Zona Lokal AWS Khusus, masukkan Zona Lokal AWS Khusus di input pemilih.
   - `Global`ketika Anda ingin menggunakan alamat IP secara global di semua AWS Wilayah, seperti CloudFront lokasi. `Global`Lokal ini hanya tersedia untuk IPv4 kolam renang umum.

   Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari pool IPAM dengan tempat yang sama dengan Wilayah VPC tersebut. Harap diingat bahwa setelah Anda memilih tempat untuk sebuah pool, Anda tidak dapat memodifikasinya. Jika Wilayah asal IPAM tidak tersedia karena pemadaman dan pool memiliki tempat yang berbeda dari Wilayah asal IPAM, pool 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 Amazon VPC (untuk terkait dengan). CIDRs VPCs
10. Berdasarkan CIDRs ketentuan, pilih CIDR untuk penyediaan kolam renang.

> **Note**
>
> Saat menyediakan CIDR ke kolam Regional dalam kumpulan tingkat atas, IPv4 CIDR paling spesifik yang dapat Anda sediakan adalah/24; lebih spesifik CIDRs (seperti/25) tidak diizinkan. Setelah Anda membuat kolam Regional, Anda dapat membuat kolam yang lebih kecil (seperti/25) dalam kolam Regional yang sama. Perhatikan bahwa jika Anda berbagi kolam Regional atau kolam renang di dalamnya, kolam ini hanya dapat digunakan di lokasi yang ditetapkan pada kolam Regional yang sama.

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 tingkat atas IPv4 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 pool.
13. Setelah selesai mengonfigurasi pool, pilih Create pool.

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

Langkah 4: 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, itulah kumpulan Regional Anda. Secara default CIDR tidak diiklankan, yang berarti tidak dapat diakses publik melalui internet.

Langkah ini harus dilakukan oleh akun IPAM.

> **Note**
>
> Status iklan tidak membatasi kemampuan Anda untuk mengalokasikan alamat IP Elastis. Bahkan jika BYOIPv4 CIDR Anda tidak diiklankan, Anda masih dapat membuat EIPs dari kolam 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, lihatBagaimana IPAM bekerja.
4. Pilih kolam Regional yang Anda buat dalam tutorial ini.
5. Pilih CIDRstab.
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 5. 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. Bagikan kolam IPAM menggunakan AWS 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 Berikutnya.
10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diBagikan kolam IPAM menggunakan AWS RAM.
11. Pilih Berikutnya.
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 Berikutnya.
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` 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 6: Alokasikan alamat IP Elastis dari kolam

Selesaikan langkah-langkah di bagian ini untuk mengalokasikan alamat IP Elastis dari kolam. Perhatikan bahwa jika Anda menggunakan IPv4 kolam publik untuk mengalokasikan alamat IP

Elastic, Anda dapat menggunakan langkah-langkah alternatif Alternatif untuk Langkah 6 daripada langkah-langkah di bagian ini.

> **Important**
>
> Jika Anda melihat kesalahan terkait tidak memiliki izin untuk memanggil ec2:AllocateAddress, izin terkelola yang saat ini ditetapkan ke kumpulan IPAM yang dibagikan dengan Anda perlu diperbarui. Hubungi orang yang membuat pembagian 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

Ikuti langkah-langkah di Alokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk mengalokasikan alamat, tetapi perhatikan hal berikut:

- Langkah ini harus dilakukan oleh akun anggota.
- Pastikan AWS Wilayah tempat Anda berada di konsol EC2 cocok dengan opsi Lokal yang Anda pilih saat membuat kumpulan Regional.
- Saat Anda memilih kumpulan alamat, pilih opsi untuk Mengalokasikan menggunakan kolam IPv4 IPAM dan pilih kumpulan Regional yang Anda buat.

Command line

Alokasikan alamat dari pool dengan perintah allocate-address. Yang `--region` Anda gunakan harus sesuai dengan `-locale` opsi yang Anda pilih saat Anda membuat kumpulan di Langkah 2. Sertakan ID kolam IPAM yang Anda buat di Langkah 2 di`--ipam-pool-id`. Secara opsional, Anda juga dapat memilih yang spesifik `/32` di kolam IPAM Anda dengan menggunakan opsi. `--address`

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

Contoh respons:

```
{
```

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

Untuk informasi selengkapnya, lihat Mengalokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2.

Langkah 7: Kaitkan alamat IP Elastis dengan instans EC2

Selesaikan langkah-langkah di bagian ini untuk mengaitkan alamat IP Elastis dengan instans EC2.

AWS Management Console

Ikuti langkah-langkah di Kaitkan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk mengalokasikan alamat IP Elastis dari kumpulan IPAM, tetapi perhatikan hal berikut: Saat Anda menggunakan opsi Konsol AWS Manajemen, AWS Wilayah tempat Anda mengaitkan alamat IP Elastis harus sesuai dengan opsi Lokal yang Anda pilih saat membuat kumpulan Regional.

Langkah ini harus dilakukan oleh akun anggota.

Command line

Langkah ini harus dilakukan oleh akun anggota. Gunakan `--profile` **`member-account`** opsi.

Kaitkan alamat IP Elastis dengan instance dengan perintah asosiasi-alamat. `--region`Anda mengaitkan alamat IP Elastis harus sesuai dengan `--locale` opsi yang Anda pilih saat Anda membuat kumpulan Regional.

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

Contoh respons:

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

Untuk informasi selengkapnya, lihat Mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan di Panduan Pengguna Amazon EC2.

Langkah 8: 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 CIDRstab.
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: 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 5: Membatalkan CIDRs 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 Pembuangan CIDRs dari kolam untuk menghentikan penyediaan CIDRs dari kolam Regional dan kemudian kolam tingkat atas, dalam urutan itu.

Langkah 6: 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 Hapus kolam untuk menghapus kolam Regional dan kemudian kolam tingkat atas, dalam urutan itu.

Alternatif untuk Langkah 6

Jika Anda menggunakan IPv4 kolam publik untuk mengalokasikan alamat IP Elastic, Anda dapat menggunakan langkah-langkah di bagian ini daripada langkah-langkah di dalamnyaLangkah 6: Alokasikan alamat IP Elastis dari kolam.

Daftar Isi

Langkah 1: Buat IPv4 kolam umum

Langkah ini harus dilakukan oleh akun anggota yang akan memberikan alamat IP Elastis.

> **Note**
>
> - Langkah ini harus dilakukan oleh akun anggota menggunakan AWS CLI.
> - IPv4 Kolam renang umum dan kolam IPAM dikelola oleh sumber daya yang berbeda di AWS. Public IPv4 pool adalah sumber daya akun tunggal yang memungkinkan Anda mengonversi alamat IP milik publik CIDRs ke alamat IP Elastic. Kolam IPAM dapat digunakan untuk mengalokasikan ruang publik Anda ke kolam renang umum IPv4 .

Untuk membuat IPv4 kolam umum 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 IPv4 kolam publik. Anda akan membutuhkan ID ini di langkah berikutnya.

  ```
  {
  ```

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

Langkah 2: Berikan IPv4 CIDR publik ke kolam renang umum IPv4 Anda

Berikan IPv4 CIDR publik ke IPv4 kolam renang umum 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. Paling tidak spesifik yang dapat `--netmask-length` Anda definisikan 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.
> - Langkah ini harus dilakukan oleh akun anggota menggunakan AWS CLI.

Untuk membuat IPv4 kolam umum 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 umum. IPv4

```
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 IPv4 kolam renang umum, untuk melihat kolam IPv4 renang umum yang dialokasikan di kolam Regional IPAM, buka konsol IPAM dan lihat alokasi di kolam Regional di bawah Alokasi atau Sumber Daya.

Langkah 3: Alokasikan alamat IP Elastis dari kolam umum IPv4

Selesaikan langkah-langkah di Alokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk mengalokasikan 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.

Setelah Anda menyelesaikan tiga langkah ini, kembali ke Langkah 7: Kaitkan alamat IP Elastis dengan instans EC2 dan lanjutkan sampai Anda menyelesaikan tutorial.

Alternatif untuk pembersihan Langkah 6

Selesaikan langkah-langkah ini untuk membersihkan IPv4 kolam umum yang dibuat dengan alternatif Langkah 9. Anda harus menyelesaikan langkah-langkah ini setelah Anda merilis alamat IP Elastis selama proses pembersihan standar diLangkah 8: Pembersihan.

Langkah 1: Singkirkan IPv4 CIDR publik dari kolam renang umum Anda IPv4

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

1. Lihat BYOIP CIDRs 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 CIDR dari IPv4 kolam umum.

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

3. Lihat BYOIP Anda CIDRs 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 IPv4 kolam 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 IPv4 kolam umum telah dihapus. Anda tidak dapat terus membersihkan dan menghentikan penyediaan CIDR kolam IPAM sampai Anda melihat bahwa alokasi telah dihapus dari IPAM.

Langkah 2: Hapus IPv4 kolam umum

Langkah ini harus dilakukan oleh akun anggota.

- Jalankan perintah berikut untuk menghapus IPv4 kolam 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.

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

Jika Anda tidak perlu mengiklankan IPv6 alamat Anda melalui Internet, Anda dapat memberikan IPv6 alamat GUA pribadi ke IPAM. Untuk informasi selengkapnya, lihat Aktifkan penyediaan GUA pribadi IPv6 CIDRs.

Important

- 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 CIDRs dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

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, lihatBagaimana IPAM bekerja.
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 Alamat keluarga, pilih IPv6.

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. 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 pool IPAM dengan tempat yang sama dengan Wilayah VPC tersebut. Harap diingat bahwa setelah Anda memilih tempat untuk sebuah pool, Anda tidak dapat memodifikasinya. Jika Wilayah asal IPAM tidak tersedia karena pemadaman dan pool memiliki tempat yang berbeda dari Wilayah asal IPAM, pool 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.

10. Di bawah sumber IP Publik, BYOIP dipilih secara default.
11. Berdasarkan CIDRs ketentuan, lakukan salah satu hal berikut:

    - Jika Anda memverifikasi kontrol domain Anda dengan sertifikat X.509, Anda harus menyertakan CIDR dan pesan BYOIP dan tanda tangan sertifikat yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.
    - Jika Anda memverifikasi kontrol domain Anda dengan catatan DNS TXT, Anda harus menyertakan token verifikasi CIDR dan IPAM yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.

    Perhatikan bahwa saat menyediakan IPv6 CIDR ke kolam dalam kumpulan tingkat atas, rentang IPv6 alamat paling spesifik yang dapat Anda bawa adalah /48 untuk yang dapat diiklankan secara publik dan /60 untuk CIDRs yang tidak dapat diiklankan secara publik. CIDRs

> **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.

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

Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan di CIDRstab 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, lihatBagaimana IPAM bekerja.
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 pool IPAM dengan tempat yang sama dengan Wilayah VPC tersebut. Harap diingat bahwa setelah Anda memilih tempat untuk sebuah pool, Anda tidak dapat memodifikasinya. Jika Wilayah asal IPAM tidak tersedia karena pemadaman dan pool memiliki tempat yang berbeda dari Wilayah asal IPAM, pool 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 terkait dengan). CIDRs VPCs
10. Berdasarkan CIDRs ketentuan, pilih CIDR untuk penyediaan kolam renang. Perhatikan bahwa saat menyediakan IPv6 CIDR ke kolam dalam kumpulan tingkat atas, rentang IPv6 alamat paling spesifik yang dapat Anda bawa adalah /48 untuk yang dapat diiklankan secara publik dan /60 untuk CIDRs yang tidak dapat diiklankan secara publik. CIDRs
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 dari kumpulan ini dan secara otomatis mengimpornya sebagai alokasi ke IPAM Anda. Perhatikan hal-hal berikut:
        - CIDRs 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 CIDRs yang tumpang tindih, IPAM akan mengimpor CIDR terbesar saja.
        - Jika IPAM menemukan beberapa CIDRs dengan pencocokan CIDRs, 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 IPv4 alamat adalah `0` -. `32` Kemungkinan panjang netmask untuk IPv6 alamat 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 digunakan CIDRs 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. Setelah selesai mengonfigurasi pool, pilih Create pool.

Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan di CIDRstab 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. Bagikan kolam IPAM menggunakan AWS 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 Berikutnya.
10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diBagikan kolam IPAM menggunakan AWS RAM.
11. Pilih Berikutnya.
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 Berikutnya.
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`

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 4: Buat VPC

Selesaikan langkah-langkah di Buat 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, lihatBagaimana IPAM bekerja.

4. Pilih kolam Regional yang Anda buat dalam tutorial ini.
5. Pilih CIDRstab.
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 CIDRstab.
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 di Hapus 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 CIDRs dari kolam Regional dan kolam tingkat atas

Langkah ini harus dilakukan oleh akun IPAM.

- Selesaikan langkah-langkah Pembuangan CIDRs dari kolam untuk menghentikan penyediaan CIDRs 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 Hapus kolam untuk menghapus kolam Regional dan kemudian kolam tingkat atas, dalam urutan itu.

Bawa IP CIDR Anda sendiri ke IPAM hanya menggunakan CLI AWS

Membawa IP Anda Sendiri (BYOIP) ke IPAM memungkinkan Anda untuk menggunakan rentang IPv6 alamat IPv4 dan alamat yang ada di organisasi Anda. AWS Hal ini memungkinkan Anda untuk mempertahankan branding yang konsisten, meningkatkan kinerja jaringan, meningkatkan keamanan, dan menyederhanakan manajemen dengan menyatukan lingkungan lokal dan cloud di bawah ruang alamat IP Anda sendiri.

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

> **Note**
>
> Sebelum memulai, Anda harus memiliki kontrol domain yang diverifikasi terlebih dahulu.

Setelah Anda membawa rentang IPv4 alamat 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

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

> **Important**
>
> - 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 CIDRs dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

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

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 CIDRs 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 CIDRs 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 IPv4 alamat untuk semua sumber AWS 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; lebih spesifik CIDRs (seperti/25) tidak diizinkan.

> **Note**
>
> - Jika Anda memverifikasi kontrol domain Anda dengan sertifikat X.509, Anda harus menyertakan CIDR dan pesan BYOIP dan tanda tangan sertifikat yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.

- Jika Anda memverifikasi kontrol domain Anda dengan catatan DNS TXT, Anda harus menyertakan token verifikasi CIDR dan IPAM yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.

Anda hanya perlu memverifikasi kontrol domain saat Anda menyediakan BYOIP CIDR ke kumpulan tingkat atas. Untuk kumpulan Regional dalam kumpulan tingkat atas, Anda dapat menghilangkan opsi verifikasi kepemilikan domain.

Langkah ini harus dilakukan oleh akun IPAM.

Important

Anda hanya perlu memverifikasi kontrol domain saat Anda menyediakan BYOIP CIDR ke kumpulan tingkat atas. Untuk kumpulan Regional dalam kumpulan tingkat atas, Anda dapat menghilangkan opsi kontrol domain. 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. Untuk memberikan CIDR dengan informasi sertifikat, gunakan contoh perintah berikut. Selain mengganti nilai sesuai kebutuhan dalam contoh, pastikan bahwa Anda mengganti `Message` dan `Signature` nilai dengan `text_message` dan `signed_message` nilai yang Anda dapatkanVerifikasi domain Anda dengan sertifikat X.509.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-
pool-id ipam-pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --
verification-method remarks-x509 --cidr-authorization-context
 Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsMaU0P7ENO7VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRYOdRaNx8yt-uoZWzxct2yIhWngy-
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

   Untuk menyediakan CIDR dengan informasi token verifikasi, gunakan contoh perintah berikut. Selain mengganti nilai sesuai kebutuhan dalam contoh, pastikan

Anda mengganti `ipam-ext-res-ver-token-0309ce7f67a768cf0` dengan ID `IpamExternalResourceVerificationTokenId` token yang Anda dapatkanVerifikasi domain Anda dengan catatan DNS TXT.

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

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.

Tempat untuk pool harus salah satu berikut ini:

- AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi.
- Grup perbatasan jaringan untuk Zona AWS Lokal tempat Anda ingin kolam IPAM ini tersedia untuk alokasi (didukung Local Zones). Opsi ini hanya tersedia untuk IPv4 kolam IPAM dalam lingkup publik.
- Zona Lokal Khusus AWS. Untuk membuat kolam dalam Zona Lokal AWS Khusus, masukkan Zona Lokal AWS Khusus di input pemilih.
- `Global`ketika Anda ingin menggunakan alamat IP secara global di semua AWS Wilayah, seperti CloudFront lokasi. `Global`Lokal ini hanya tersedia untuk IPv4 kolam renang umum.

Misalnya, Anda hanya dapat mengalokasikan CIDR untuk VPC dari pool IPAM dengan tempat yang sama dengan Wilayah VPC tersebut. Harap diingat bahwa setelah Anda memilih tempat untuk sebuah pool, Anda tidak dapat memodifikasinya. Jika Wilayah asal IPAM tidak tersedia karena pemadaman dan pool memiliki tempat yang berbeda dari Wilayah asal IPAM, pool masih dapat digunakan untuk mengalokasikan alamat IP.

Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus menyertakan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan yang akan digunakan untuk CIDR BYOIP. Misalnya, jika Anda membuat kumpulan BYOIP dengan lokal us-east-1, seharusnya us-east-1. `--region` Jika Anda membuat kumpulan BYOIP dengan lokal us-east-1-scl-1 (grup perbatasan jaringan yang digunakan untuk Local Zones), `--region` seharusnya us-east-1 karena Wilayah tersebut mengelola lokal us-east-1-scl-1.

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 terkait dengan). CIDRs VPCs

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, kita membuat top-level dan pool Regional, sehingga Anda akan melihat keduanya.

Langkah 6: Menyediakan CIDR ke kolam Regional

Menyediakan blok CIDR ke kolam Regional.

> **Note**
>
> Saat menyediakan CIDR ke kolam Regional dalam kumpulan tingkat atas, IPv4 CIDR paling spesifik yang dapat Anda sediakan adalah/24; lebih spesifik CIDRs (seperti/25) tidak diizinkan. Setelah Anda membuat kolam Regional, Anda dapat membuat kolam yang lebih kecil (seperti/25) dalam kolam Regional yang sama. Perhatikan bahwa jika Anda berbagi kolam Regional atau kolam renang di dalamnya, kolam ini hanya dapat digunakan di lokasi yang ditetapkan pada kolam Regional yang sama.

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: 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.

> **Note**
>
> Status iklan tidak membatasi kemampuan Anda untuk mengalokasikan alamat IP Elastis. Bahkan jika BYOIPv4 CIDR Anda tidak diiklankan, Anda masih dapat membuat EIPs dari kolam 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 8: 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. Bagikan kolam IPAM menggunakan AWS 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 Berikutnya.
10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diBagikan kolam IPAM menggunakan AWS RAM.
11. Pilih Berikutnya.
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 Berikutnya.
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`

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 9: Alokasikan alamat IP Elastis dari kolam

Selesaikan langkah-langkah di bagian ini untuk mengalokasikan alamat IP Elastis dari kolam. Perhatikan bahwa jika Anda menggunakan IPv4 kolam publik untuk mengalokasikan alamat IP Elastic, Anda dapat menggunakan langkah-langkah alternatif Alternatif untuk Langkah 9 daripada langkah-langkah di bagian ini.

> **Important**
>
> Jika Anda melihat kesalahan terkait tidak memiliki izin untuk memanggil ec2:AllocateAddress, izin terkelola yang saat ini ditetapkan ke kumpulan IPAM yang dibagikan dengan Anda perlu diperbarui. Hubungi orang yang membuat pembagian 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

Ikuti langkah-langkah di Alokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk mengalokasikan alamat, tetapi perhatikan hal berikut:

- Langkah ini harus dilakukan oleh akun anggota.
- Pastikan AWS Wilayah tempat Anda berada di konsol EC2 cocok dengan opsi Lokal yang Anda pilih saat membuat kumpulan Regional.
- Saat Anda memilih kumpulan alamat, pilih opsi untuk Mengalokasikan menggunakan kolam IPv4 IPAM dan pilih kumpulan Regional yang Anda buat.

Command line

Alokasikan alamat dari pool dengan perintah allocate-address. Yang `--region` Anda gunakan harus sesuai dengan `-locale` opsi yang Anda pilih saat Anda membuat kumpulan di Langkah 2. Sertakan ID kolam IPAM yang Anda buat di Langkah 2 di`--ipam-pool-id`. Secara opsional,

Anda juga dapat memilih yang spesifik `/32` di kolam IPAM Anda dengan menggunakan opsi. `--address`

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

Contoh respons:

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

Untuk informasi selengkapnya, lihat Mengalokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2.

Langkah 10: Kaitkan alamat IP Elastis dengan instans EC2

Selesaikan langkah-langkah di bagian ini untuk mengaitkan alamat IP Elastis dengan instans EC2.

AWS Management Console

Ikuti langkah-langkah di Kaitkan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk mengalokasikan alamat IP Elastis dari kumpulan IPAM, tetapi perhatikan hal berikut: Saat Anda menggunakan opsi Konsol AWS Manajemen, AWS Wilayah tempat Anda mengaitkan alamat IP Elastis harus sesuai dengan opsi Lokal yang Anda pilih saat membuat kumpulan Regional.

Langkah ini harus dilakukan oleh akun anggota.

Command line

Langkah ini harus dilakukan oleh akun anggota. Gunakan `--profile` **`member-account`** opsi.

Kaitkan alamat IP Elastis dengan instance dengan perintah asosiasi-alamat. `--region`Anda mengaitkan alamat IP Elastis harus sesuai dengan `--locale` opsi yang Anda pilih saat Anda membuat kumpulan Regional.

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

Contoh respons:

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

Untuk informasi selengkapnya, lihat Mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan di Panduan Pengguna Amazon EC2.

Langkah 11: 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 menyertakan `--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 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. Saat Anda menjalankan perintah di bagian ini, nilai untuk `--region` harus menyertakan `--locale` opsi yang Anda masukkan saat Anda membuat kumpulan 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": []
}
```

5. 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"

    }

}
```

6. 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.

7. 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"
    }
}
```

8. 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"

    }

}
```

9. 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"
    }
}
```

10. 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"
            }
        ],
    }
}
```

Alternatif untuk Langkah 9

Jika Anda menggunakan IPv4 kolam publik untuk mengalokasikan alamat IP Elastic, Anda dapat menggunakan langkah-langkah di bagian ini daripada langkah-langkah di dalamnyaLangkah 9: Alokasikan alamat IP Elastis dari kolam.

Daftar Isi

Langkah 1: Buat kolam IPv4 renang umum

Langkah ini biasanya dilakukan oleh AWS akun lain yang ingin memberikan alamat IP Elastis, seperti akun anggota.

> **Important**
>
> IPv4 Kolam renang umum dan kolam IPAM dikelola oleh sumber daya yang berbeda di AWS. Public IPv4 pool adalah sumber daya akun tunggal yang memungkinkan Anda mengonversi alamat IP milik publik CIDRs ke alamat IP Elastic. Kolam IPAM dapat digunakan untuk mengalokasikan ruang publik Anda ke kolam renang umum IPv4 .

Untuk membuat IPv4 kolam umum 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 IPv4 kolam publik. Anda akan membutuhkan ID ini di langkah berikutnya.

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

Langkah 2: Berikan IPv4 CIDR publik ke kolam renang umum IPv4 Anda

Berikan IPv4 CIDR publik ke IPv4 kolam renang umum Anda. Nilai untuk `--region` harus sesuai dengan `--locale` nilai yang Anda masukkan saat Anda membuat pool yang akan digunakan

untuk BYOIP CIDR. Yang paling tidak spesifik yang dapat `--netmask-length` Anda definisikan adalah`24`.

Langkah ini harus dilakukan oleh akun anggota.

Untuk membuat IPv4 kolam umum 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 umum. IPv4

```
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 3: Buat alamat IP Elastis dari IPv4 kolam umum

Buat alamat IP Elastis (EIP) dari IPv4 kolam umum. 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 IPv4 kolam umum 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"
        }
    ]
}
```

Alternatif untuk pembersihan Langkah 9

Selesaikan langkah-langkah ini untuk membersihkan IPv4 kolam umum yang dibuat dengan alternatif Langkah 9. Anda harus menyelesaikan langkah-langkah ini setelah Anda merilis alamat IP Elastis selama proses pembersihan standar diLangkah 10: Pembersihan.

1. Lihat BYOIP CIDRs 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": []
   ```

```
        }
    ]
}
```

2. Lepaskan CIDR dari IPv4 kolam renang umum. 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 130.137.245.0/24 --profile member-account
```

3. Lihat BYOIP Anda CIDRs 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 IPv4 kolam publik Anda.

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

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

Jika Anda tidak perlu mengiklankan IPv6 alamat Anda melalui Internet, Anda dapat memberikan IPv6 alamat GUA pribadi ke IPAM. Untuk informasi selengkapnya, lihat Aktifkan penyediaan GUA pribadi IPv6 CIDRs.

⚠ Important

- 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 CIDRs dari kolam IPAM. Dalam tutorial ini, akun ini akan disebut akun anggota.

Daftar Isi

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

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 CIDRs 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 IPv6 alamat untuk semua sumber AWS 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 IPv6 alamat paling spesifik yang dapat Anda bawa adalah /48 untuk yang dapat diiklankan secara publik dan /60 untuk CIDRs yang tidak dapat diiklankan secara publik. CIDRs

> **Note**
>
> - Jika Anda memverifikasi kontrol domain Anda dengan sertifikat X.509, Anda harus menyertakan CIDR dan pesan BYOIP dan tanda tangan sertifikat yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.
> - Jika Anda memverifikasi kontrol domain Anda dengan catatan DNS TXT, Anda harus menyertakan token verifikasi CIDR dan IPAM yang Anda buat pada langkah itu sehingga kami dapat memverifikasi bahwa Anda mengontrol ruang publik.

Anda hanya perlu memverifikasi kontrol domain saat Anda menyediakan BYOIP CIDR ke kumpulan tingkat atas. Untuk kumpulan Regional dalam kumpulan tingkat atas, Anda dapat menghilangkan opsi kepemilikan domain.

Langkah ini harus dilakukan oleh akun IPAM.

Untuk menyediakan blok CIDR ke kolam menggunakan AWS CLI

1. Untuk memberikan CIDR dengan informasi sertifikat, gunakan contoh perintah berikut. Selain mengganti nilai sesuai kebutuhan dalam contoh, pastikan bahwa Anda mengganti `Message` dan `Signature` nilai dengan `text_message` dan `signed_message` nilai yang Anda dapatkanVerifikasi domain Anda dengan sertifikat X.509.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-
x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|
20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
```

```
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

Untuk menyediakan CIDR dengan informasi token verifikasi, gunakan contoh perintah berikut. Selain mengganti nilai sesuai kebutuhan dalam contoh, pastikan Anda mengganti `ipam-ext-res-ver-token-0309ce7f67a768cf0` dengan ID `IpamExternalResourceVerificationTokenId` token yang Anda dapatkan[Verifikasi domain Anda dengan catatan DNS TXT](#).

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

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 terkait dengan). CIDRs VPCs

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 IPv6 alamat paling spesifik yang dapat Anda bawa adalah /48 untuk yang dapat diiklankan secara publik dan /60 untuk CIDRs yang tidak dapat diiklankan secara publik. CIDRs

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. Bagikan kolam IPAM menggunakan AWS 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 Berikutnya.

10. Pilih AWSRAMPermissionIpamPoolByoipCidrImportizin. Rincian opsi izin berada di luar cakupan untuk tutorial ini, tetapi Anda dapat mengetahui lebih lanjut tentang opsi ini diBagikan kolam IPAM menggunakan AWS RAM.
11. Pilih Berikutnya.
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 Berikutnya.
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` 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 VPC menggunakan CIDR IPv6

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, 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 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 menyelesaikannya. 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 menyelesaikannya. 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"
            }
        ]
    }
}
```

Bawa IP Anda sendiri untuk CloudFront menggunakan IPAM

BYOIP IPAM untuk layanan global memungkinkan Anda menggunakan IPv4 alamat Anda sendiri dengan layanan AWS global seperti. CloudFront Tidak seperti BYOIP regional, alamat IP Anda diiklankan dari beberapa lokasi tepi secara bersamaan melalui perutean anycast.

Mengapa menggunakan fitur ini?

- Pertahankan IP allowlisting — Gunakan alamat IP yang sudah disetujui alih-alih memperbarui konfigurasi firewall
- Sederhanakan migrasi - Migrasi dari yang lain CDNs tanpa mengubah infrastruktur IP
- Pencitraan merek yang konsisten — Pertahankan ruang alamat IP yang ada saat pindah AWS

Siapa yang harus menggunakan fitur ini?

Organizations yang membutuhkan alamat IP mereka sendiri dengan pengiriman konten global:

- Perusahaan besar dengan persyaratan IP allowlisting
- Perusahaan yang bermigrasi dari yang lain CDNs dengan alamat IP yang ada
- Organizations dengan kebijakan keamanan ketat yang membutuhkan rentang IP tertentu

Kapan menggunakan fitur ini?

Gunakan BYOIP untuk layanan global saat Anda perlu:

- Pertahankan daftar izin IP yang ada dengan mitra/klien
- Migrasi dari CDN lain menggunakan alamat IP Anda
- Memenuhi persyaratan kepatuhan untuk rentang IP tertentu

> **Note**
>
> Membutuhkan /24 blok IPv4 CIDR. Saat ini CloudFront hanya tersedia untuk.

Prasyarat

Selesaikan langkah-langkah ini sebelum memulai:

- Penyiapan IPAM — Integrasikan IPAM dengan akun di Organisasi AWS dan Buat IPAM
- Verifikasi domain - Verifikasi kontrol domain
- Buat kolam tingkat atas — Ikuti langkah 1-2 dalam Bawa IPv4 CIDR Anda sendiri ke IPAM

Langkah-langkah konfigurasi layanan global

Langkah-langkah berikut berbeda dari proses BYOIP regional standar dan menetapkan pola untuk layanan global:

Langkah 1: Buat kolam global untuk layanan anycast

Alih-alih membuat kolam regional, buat kolam global untuk layanan anycast:

Konsol

Untuk membuat kumpulan global menggunakan konsol:

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools
3. Pilih Buat kolam
4. Sumber: Pilih kolam BYOIP tingkat atas Anda

5. Lokal: Pilih Global
6. Layanan: Pilih layanan Global (muncul saat Global dipilih)
7. Sumber IP publik: Pilih BYOIP
8. CIDRs untuk menyediakan: Tentukan rentang CIDR /24 Anda
9. Pilih Buat kolam

CLI

Gunakan `aws ec2 create-ipam-pool` dengan lokal disetel ke “Global” dan alamat keluarga “ipv4".

Kemudian berikan CIDR menggunakan`aws ec2 provision-ipam-pool-cidr`.

> **Important**
>
> Anda harus mengalokasikan blok /24 penuh ke kolam ini. Anda dapat menyediakan rentang yang lebih spesifik dalam blok ini untuk penggunaan yang berbeda.

Langkah 2: Buat sumber daya khusus layanan

Untuk CloudFront, buat daftar IP anycast yang menggunakan kolam IPAM Anda. Untuk petunjuk rinci, lihat dokumentasi CloudFront BYOIP (link TBD).

Parameter kunci untuk integrasi IPAM:

- Jenis alamat IP - Pilih BYOIP
- Kolam IPAM — Pilih kolam global Anda dari Langkah 1
- Jumlah IP - Masukkan 3 (diperlukan untuk CloudFront)

Langkah 3: Kaitkan dengan sumber daya layanan

Kaitkan daftar IP Statis Anycast Anda dengan CloudFront distribusi. Untuk petunjuk rinci, lihat dokumentasi CloudFront BYOIP (link TBD).

Konfigurasi kunci:

- Dalam pengaturan distribusi, pilih Daftar IP Anycast Anda dari Langkah 2

Langkah 4: Bersiaplah untuk Migrasi

- Turunkan DNS TTL - Setel DNS TTL untuk catatan Anda ke 60 detik atau lebih rendah
- Tunggu propagasi - Berikan waktu untuk TTL baru berlaku di internet

Langkah 5: Iklankan CIDR secara global

Gunakan perintah iklan global IPAM:

Konsol

Untuk mengiklankan CIDR menggunakan konsol:

1. Buka konsol IPAM di https://console.aws.amazon.com/ipam/.
2. Di panel navigasi, pilih Pools
3. Pilih kolam global Anda
4. Pilih CIDRstab
5. Pilih CIDR Anda dan pilih Tindakan > Iklan CIDR
6. Konfirmasikan iklan

CLI

Gunakan `aws ec2 advertise-ipam-byoip-cidr` dengan ID kolam IPAM dan CIDR Anda.

> **Important**
>
> - Tarik iklan dari penyedia Anda sebelumnya sebelum menjalankan perintah ini
> - Perbarui catatan DNS untuk menunjuk CloudFront untuk menyelesaikan migrasi

Pembersihan

Untuk membersihkan sumber daya yang dibuat dalam tutorial ini:

- Hapus CloudFront sumber daya - Ikuti petunjuk pembersihan dalam dokumentasi CloudFront BYOIP (tautan TBD)

- Tarik CIDR dan hapus kolam IPAM — Ikuti proses pembersihan standar di Langkah 8: Pembersihan

> **Important**
>
> Hapus CloudFront sumber daya terlebih dahulu, lalu lanjutkan dengan pembersihan IPAM untuk menghindari gangguan layanan.

Tutorial: Transfer IPv4 CIDR BYOIP ke IPAM

Ikuti langkah-langkah ini untuk mentransfer IPv4 CIDR yang ada ke IPAM. Jika Anda sudah memiliki IPv4 BYOIP CIDR AWS, Anda dapat memindahkan CIDR ke IPAM dari kolam renang umum. IPv4 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 IPv4 kolam umum ke IPAM, tidak ada dampak pada alokasi yang ada. Setelah Anda mentransfer IPv4 kolam umum ke IPAM, tergantung pada jenis sumber daya, Anda mungkin dapat memantau alokasi yang ada. Untuk informasi selengkapnya, lihat Memantau penggunaan CIDR berdasarkan sumber daya.

> **Note**
>
> - 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

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

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 terkait dengan). CIDRs VPCs

Untuk membuat kumpulan IPv4 alamat 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 IPV4 CIDR BYOIP yang ada ke kolam IPAM dan menggunakan kolam IPAM. Langkah ini harus dilakukan oleh **`ipam-account`** akun.

Untuk berbagi kumpulan IPv4 alamat menggunakan AWS CLI

1. Lihat AWS RAM izin yang tersedia untuk kolam IPAM. Anda membutuhkan keduanya ARNs 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 CIDRs 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 IPv4 kolam publik setelah transfer selesai, salin ARN untuk `AWSRAMDefaultPermissionsIpamPool` dan buat pembagian 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 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 pindah CIDRs ke IPAM.

Langkah 5: Transfer IPV4 CIDR BYOIP yang ada ke IPAM

Ikuti langkah-langkah di bagian ini untuk mentransfer IPV4 CIDR BYOIP yang ada ke IPAM. Langkah ini harus dilakukan oleh **`byoip-owner-account`** akun.

> **Important**
>
> Setelah Anda membawa rentang IPv4 alamat 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 Konsol Manajemen AWS 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 CIDR dari IPv4 kolam renang umum. 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 130.137.249.0/24
```

6. Lihat BYOIP Anda CIDRs 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 IPv4 kolam 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 IPv4 alamat pribadi dalam lingkup IPAM pribadi ke VPCs dan subnet. Anda juga dapat menyelesaikan tutorial ini menggunakan rentang IPv6 CIDR dengan membuat VPC dengan opsi blok CIDR yang IPv6 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 CIDRs 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 yang CIDRs 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 VPCs, 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 IPv4 CIDR. Dalam tutorial ini, kami menggunakan 10.0.0.0/20.
5. Lewati opsi untuk menambahkan blok IPv6 CIDR.
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 CIDRs ke kolam perencanaan sumber daya.
9. Di bawah CIDRs ketentuan, pilih CIDR VPC untuk menyediakan 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. Berdasarkan CIDRs ketentuan, 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, lihatBagikan kolam IPAM menggunakan AWS 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 CIDR yang dialokasikan IPAM dan pilih IPV4 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 mengatur CloudWatch alarm pada IPUsage metrik Subnet, 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% dari IPs 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 tinggal dengan CIDRs disediakan untuk mereka, meskipun tidak CIDRs lagi dari kolam IPAM.
6. Pilih Hapus.
7. Hapus subnet.
8. Hapus VPC.

Pembersihan selesai.

Alokasikan alamat IP Elastis berurutan dari kolam IPAM

IPAM memungkinkan Anda untuk menyediakan IPv4 blok publik milik Amazon ke kolam IPAM dan mengalokasikan alamat IP Elastis berurutan dari kumpulan tersebut ke sumber daya. AWS

Alamat IP Elastic yang dialokasikan secara bersebelahan adalah alamat publik yang dialokasikan secara berurutan IPv4 . Misalnya, jika Amazon memberi Anda blok IPv4 CIDR publik `192.0.2.0/30` dan Anda mengalokasikan empat IPv4 alamat publik yang tersedia dari blok CIDR tersebut, contoh empat alamat IP Elastis berurutan adalah`192.0.2.0`,, `192.0.2.1` dan. `192.0.2.2` `192.0.2.3`

Alamat IP Elastis yang dialokasikan secara berdekatan memungkinkan Anda menyederhanakan aturan keamanan dan jaringan dengan cara berikut:

- Administrasi keamanan: Menggunakan IPv4 alamat berurutan mengurangi overhead manajemen firewall Anda. Anda dapat menambahkan seluruh awalan dengan satu aturan dan mengaitkan IPs dari awalan yang sama saat Anda menskalakan, menghemat waktu dan tenaga.
- Akses perusahaan: Anda dapat menyederhanakan ruang alamat yang dibagikan dengan klien Anda dengan menggunakan seluruh blok CIDR alih-alih daftar panjang alamat publik IPv4 individual. Ini menghindari kebutuhan untuk terus-menerus mengkomunikasikan perubahan IP saat aplikasi Anda meningkat. AWS
- Manajemen IP yang disederhanakan: Menggunakan IPv4 alamat berurutan menyederhanakan manajemen IP publik untuk tim jaringan pusat Anda, karena mengurangi kebutuhan untuk melacak publik individu IPs dan sebaliknya memungkinkan mereka untuk fokus pada sejumlah awalan IP yang terbatas.

Dalam tutorial ini, Anda akan melalui langkah-langkah yang diperlukan untuk mengalokasikan alamat IP Elastis berurutan dari kolam IPAM. Anda akan membuat kolam IPAM dengan blok IPv4 CIDR publik bersebelahan yang disediakan Amazon, mengalokasikan alamat IP Elastis dari kolam, dan mempelajari cara memantau alokasi kolam IPAM.

> **Note**
>
> - Ada biaya yang terkait dengan penyediaan blok CIDR publik milik Amazon. IPv4 Untuk informasi selengkapnya, lihat IPv4 tab blok bersebelahan yang disediakan Amazon di halaman harga Amazon VPC.
> - Tutorial ini mengasumsikan Anda ingin membuat IPAM menggunakan IPAM dengan satu akun. Jika Anda ingin berbagi IPv4 blok publik bersebelahan milik Amazon di seluruh akun, pertama dan kemudian. Integrasikan IPAM dengan akun di Organisasi AWS Bagikan kolam IPAM menggunakan AWS RAM Jika Anda berintegrasi dengan AWS Organizations, Anda memiliki opsi untuk membuat kebijakan kontrol layanan untuk mencegah deprovisioning IPv4 blok contig yang ditetapkan ke pool.
> - Anda tidak dapat mentransfer alamat IP Elastis berurutan yang dialokasikan dari kolam IPAM ke akun lain. AWS Sebaliknya, IPAM memungkinkan Anda untuk berbagi kolam IPAM di seluruh AWS akun dengan mengintegrasikan IPAM dengan AWS Organizations (seperti yang disebutkan di atas).
> - Ada batasan jumlah blok IPv4 CIDR publik milik Amazon yang dapat Anda berikan dan ukurannya. Untuk informasi selengkapnya, lihat Kuota untuk IPAM Anda.

Daftar Isi

Langkah 1: Buat IPAM

Selesaikan langkah-langkah di bagian ini untuk membuat IPAM.

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 Manajer 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. AWS Wilayah tempat Anda membuat IPAM 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 CIDRs untuk in`us-west-2`, pilih VPCs `us-west-2` di sini. 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.

Buat IPAM dengan perintah create-ipam:

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

Contoh respons:

```
{
    "Ipam": {
        "OwnerId": "320805250157",
        "IpamId": "ipam-0755477df834ea06b",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-01bc7290e4a9202f9",
        "PrivateDefaultScopeId": "ipam-scope-0a50983b97a7a583a",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "State": "create-in-progress",
        "Tags": [],
        "DefaultResourceDiscoveryId": "ipam-res-disco-02cc5b34cc3f04f09",
        "DefaultResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-06b3a4dccfc81f7c1",
        "ResourceDiscoveryAssociationCount": 1,
        "Tier": "advanced"
    }
}
```

Anda akan membutuhkannya PublicDefaultScopeId di langkah berikutnya. Untuk informasi lebih lanjut tentang cakupan, lihatBagaimana IPAM bekerja.

Langkah 2: Buat kolam IPAM dan sediakan CIDR

Selesaikan langkah-langkah di bagian ini untuk membuat kolam IPAM dari mana Anda akan mengalokasikan alamat IP Elastis.

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 ruang lingkup publik. Untuk informasi lebih lanjut tentang cakupan, lihatBagaimana IPAM bekerja.
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 Alamat keluarga, pilih IPv4.
8. Di bawah Perencanaan sumber daya, biarkan ruang IP Paket dalam lingkup yang dipilih.
9. Di bawah Locale, pilih lokasi untuk kolam renang. Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Opsi yang tersedia berasal dari Wilayah operasi yang Anda pilih saat Anda membuat IPAM Anda.
10. Di bawah Layanan, pilih EC2 (EIP/VPC). Layanan yang Anda pilih menentukan AWS layanan tempat CIDR akan diiklankan. Saat ini, satu-satunya pilihan adalah EC2 (EIP/VPC), yang berarti bahwa CIDR yang dialokasikan dari kumpulan ini akan diiklankan untuk layanan Amazon EC2 (untuk alamat IP Elastis).
11. Di bawah Sumber IP Publik, pilih milik Amazon.
12. Di bawah CIDR untuk ketentuan, pilih Tambahkan CIDR publik milik Amazon. Pilih panjang Netmask antara `/29` (8 alamat IP) dan `/30` (4 alamat IP). Anda dapat menambahkan hingga 2 secara CIDRs default. Untuk informasi tentang meningkatkan batas pada publik bersebelahan yang disediakan Amazon, lihat. IPv4 CIDRs Kuota untuk IPAM Anda
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 CIDRstab di halaman detail kumpulan.

Command line

Untuk membuat kolam

1. Buat kolam IPAM dengan create-ipam-poolperintah. Lokal adalah AWS Wilayah di mana Anda ingin kolam IPAM ini tersedia untuk alokasi. Opsi yang tersedia berasal dari Wilayah operasi yang Anda pilih saat Anda membuat IPAM Anda.

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

Contoh respons dengan statuscreate-in-progress:

```
{

    "IpamPool": {

        "OwnerId": "320805250157",

        "IpamPoolId": "ipam-pool-07ccc86aa41bef7ce",

        "IpamPoolArn": "arn:aws:ec2::320805250157:ipam-pool/ipam-
pool-07ccc86aa41bef7ce",
        "IpamScopeArn": "arn:aws:ec2::320805250157:ipam-scope/ipam-
scope-01bc7290e4a9202f9",
        "IpamScopeType": "public",

        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",

        "IpamRegion": "us-east-1",

        "Locale": "us-east-1",

        "PoolDepth": 1,

        "State": "create-in-progress",

        "AutoImport": false,

        "AddressFamily": "ipv4",
```

```
        "Tags": [],

        "AwsService": "ec2",

        "PublicIpSource": "amazon"

    }

}
```

2. Periksa apakah pool berhasil dibuat dengan describe-ipam-poolsperintah.

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

Contoh respons dengan status`create-complete`:

```
{

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

3. Menyediakan CIDR ke kolam dengan provision-ipam-pool-cidrperintah. Pilih `--netmask-length` antara `/29` (8 alamat IP) dan `/30` (4 alamat IP). Anda dapat menambahkan hingga 2 secara CIDRs default. Untuk informasi tentang meningkatkan batas pada publik bersebelahan yang disediakan Amazon, lihat. IPv4 CIDRs Kuota untuk IPAM Anda

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

Contoh respons dengan status`pending-provision`:

```
{

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

4. Pastikan CIDR ini telah disediakan sebelum Anda melanjutkan. Anda dapat melihat status penyediaan menggunakan perintah. get-ipam-pool-cidrs

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

Contoh respons dengan status`provisioned`:

```
{

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

Langkah 3: Alokasikan alamat IP Elastis dari kolam

Selesaikan langkah-langkah di bagian ini untuk mengalokasikan alamat IP Elastis dari kolam.

AWS Management Console

Ikuti langkah-langkah di Alokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk mengalokasikan alamat, tetapi perhatikan hal berikut:

- Pastikan AWS Wilayah tempat Anda berada di konsol EC2 cocok dengan opsi Lokal yang Anda pilih saat membuat kumpulan di Langkah 2.
- Saat Anda memilih kumpulan alamat, pilih opsi untuk Mengalokasikan menggunakan kolam IPv4 IPAM dan pilih kolam yang Anda buat di Langkah 1.

Command line

Alokasikan alamat dari pool dengan perintah allocate-address. Yang `--region` Anda gunakan harus sesuai dengan `-locale` opsi yang Anda pilih saat Anda membuat kumpulan di Langkah 2. Sertakan ID kolam IPAM yang Anda buat di Langkah 2 di`--ipam-pool-id`.

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

Contoh respons:

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

Secara opsional, Anda juga dapat memilih yang spesifik `/32` di kolam IPAM Anda dengan menggunakan opsi. `--address`

```
aws ec2 allocate-address --region us-east-1 --ipam-pool-id ipam-
pool-07ccc86aa41bef7ce --address 18.97.0.41
```

Contoh respons:

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

Untuk informasi selengkapnya, lihat Mengalokasikan alamat IP Elastis di Panduan Pengguna Amazon EC2.

Langkah 4: Kaitkan alamat IP Elastis dengan instans EC2

Selesaikan langkah-langkah di bagian ini untuk mengaitkan alamat IP Elastis dengan instans EC2.

AWS Management Console

Ikuti langkah-langkah di Kaitkan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk mengalokasikan alamat IP Elastis dari kumpulan IPAM, tetapi perhatikan hal berikut: Saat Anda menggunakan opsi Konsol AWS Manajemen, AWS Wilayah tempat Anda mengaitkan alamat IP Elastis harus sesuai dengan opsi Lokal yang Anda pilih saat membuat kumpulan di Langkah 2.

Command line

Kaitkan alamat IP Elastis dengan instance dengan perintah asosiasi-alamat. `--region`Anda mengaitkan alamat IP Elastis harus sesuai dengan `--locale` opsi yang Anda pilih saat Anda membuat kumpulan di Langkah 2.

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

Contoh respons:

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

Untuk informasi selengkapnya, lihat Mengaitkan alamat IP Elastis dengan instans atau antarmuka jaringan di Panduan Pengguna Amazon EC2.

Langkah 5: Lacak dan pantau penggunaan kolam

Setelah Anda mengalokasikan alamat IP Elastis dari kolam IPAM, Anda dapat melacak dan memantau alokasi kolam IPAM.

AWS Management Console

- Lihat tab Alokasi detail kolam IPAM di konsol IPAM. Setiap alamat IP Elastis yang dialokasikan dari kolam IPAM memiliki Jenis Sumber Daya EIP.
- Gunakan wawasan IP Publik:
  - Di bawah jenis IP Publik, filter menurut milik Amazon EIPs. Ini menunjukkan jumlah total IPv4 alamat publik yang dialokasikan ke alamat IP Elastic milik Amazon. Jika Anda memfilter berdasarkan ukuran ini dan menggulir ke alamat IP Publik di bagian bawah halaman, Anda akan melihat alamat IP Elastis yang telah Anda alokasikan.
  - Di bawah penggunaan EIP, filter menurut milik Associated Amazon EIPs atau milik Amazon yang tidak terkait. EIPs Ini menunjukkan jumlah total alamat IP Elastic yang telah Anda alokasikan di AWS akun Anda dan yang Anda miliki atau belum terkait dengan instans EC2, antarmuka jaringan, atau AWS sumber daya. Jika Anda memfilter berdasarkan ukuran ini dan menggulir ke alamat IP Publik di bagian bawah halaman, Anda akan melihat detail tentang sumber daya yang difilter.
  - Di bawah penggunaan IPv4 bersebelahan milik Amazon, pantau IPs penggunaan IPv4 alamat publik berurutan dari waktu ke waktu dan kumpulan IPAM milik Amazon terkait. IPv4
- Gunakan Amazon CloudWatch untuk melacak dan memantau metrik yang terkait dengan IPv4 blok publik berdekatan yang disediakan Amazon yang telah disediakan ke kolam IPAM. Untuk metrik yang tersedia khusus untuk IPv4 blok yang berdekatan, lihat Metrik IP Publik di bawah. Metrik IPAM Selain melihat metrik, Anda dapat membuat alarm di Amazon CloudWatch untuk memberi tahu Anda saat ambang batas tercapai. Membuat alarm dan mengatur notifikasi dengan Amazon CloudWatch berada di luar cakupan tutorial ini. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch alarm Amazon di Panduan CloudWatch Pengguna Amazon.

Command line

- Lihat alokasi kolam IPAM dengan perintah. get-ipam-pool-allocations Setiap alamat IP Elastis yang dialokasikan dari kolam IPAM memiliki Jenis Sumber Daya eip.

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

Contoh respons:

```
{
     "IpamPoolAllocations": [
        {
            "Cidr": "18.97.0.40/32",
            "IpamPoolAllocationId": "ipam-pool-
alloc-0bd07df786e8148aba2763e2b6c1c44bd",
            "ResourceId": "eipalloc-0c9decaa541d89aa9",
            "ResourceType": "eip",
            "ResourceRegion": "us-east-1",
            "ResourceOwner": "320805250157"
        }
    ]
}
```

- Gunakan Amazon CloudWatch untuk melacak dan memantau metrik yang terkait dengan IPv4 blok publik berdekatan yang disediakan Amazon yang telah disediakan ke kolam IPAM. Untuk metrik yang tersedia khusus untuk IPv4 blok yang berdekatan, lihat Metrik IP Publik di bawah. Metrik IPAM Selain melihat metrik, Anda dapat membuat alarm di Amazon CloudWatch untuk memberi tahu Anda saat ambang batas tercapai. Membuat alarm dan mengatur notifikasi dengan Amazon CloudWatch berada di luar cakupan tutorial ini. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch alarm Amazon di Panduan CloudWatch Pengguna Amazon.

Tutorialnya sekarang sudah lengkap. Anda telah membuat kolam IPAM dengan blok IPv4 CIDR publik bersebelahan yang disediakan Amazon, mengalokasikan alamat IP Elastis dari kolam, dan mempelajari cara memantau alokasi kolam IPAM. Lanjutkan ke bagian berikutnya untuk menghapus sumber daya yang telah Anda buat dalam tutorial ini.

Pembersihan

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

Langkah 1: Putuskan alamat IP Elastis

Selesaikan langkah-langkah dalam Memutuskan alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk memisahkan alamat IP Elastis.

Langkah 2: Lepaskan alamat IP Elastis

Selesaikan langkah-langkah dalam Rilis alamat IP Elastis di Panduan Pengguna Amazon EC2 untuk merilis alamat IP Elastis dari kolam publik IPv4 .

Langkah 3: Pembatalan CIDR dari kolam IPAM

Selesaikan langkah-langkah Pembuangan CIDRs dari kolam untuk menghentikan penyediaan CIDR publik milik Amazon dari kolam IPAM. Langkah ini diperlukan untuk penghapusan kolam renang. Anda akan ditagih untuk IPv4 blok berdekatan yang disediakan Amazon sampai langkah ini selesai.

Langkah 4: Hapus kolam IPAM

Selesaikan langkah-langkah Hapus kolam untuk menghapus kolam IPAM.

Langkah 5: Hapus IPAM

Selesaikan langkah-langkah Hapus IPAM untuk menghapus IPAM.

Pembersihan tutorial selesai.

Manajemen identitas dan akses di IPAM

AWS menggunakan kredensi keamanan untuk mengidentifikasi Anda dan memberi Anda akses ke sumber daya Anda AWS . Anda dapat menggunakan fitur AWS Identity and Access Management (IAM) untuk memungkinkan pengguna, layanan, dan aplikasi lain menggunakan AWS sumber daya Anda sepenuhnya atau dengan cara yang terbatas, tanpa membagikan kredensi keamanan Anda.

Bagian ini menjelaskan peran AWS terkait layanan yang dibuat khusus untuk IPAM dan kebijakan terkelola yang dilampirkan 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 identitas dan manajemen akses untuk VPC, lihat Identitas dan manajemen akses untuk Amazon VPC di Panduan Pengguna Amazon VPC.

Konten

Peran terkait layanan untuk IPAM

IPAM menggunakan peran AWS Identity and Access Management terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM yang unik. Peran terkait layanan telah ditentukan sebelumnya oleh IPAM dan mencakup semua izin yang diperlukan layanan untuk memanggil layanan lain AWS atas nama Anda.

Peran terkait layanan membuat pengaturan IPAM lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. IPAM mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya IPAM yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Izin peran terkait layanan

IPAM menggunakan peran terkait layanan AWSServiceRoleForIPAM untuk memanggil tindakan dalam kebijakan terkelola terlampir. AWSIPAMServiceRolePolicy Untuk informasi selengkapnya tentang tindakan yang diizinkan dalam kebijakan tersebut, lihatAWS kebijakan terkelola untuk IPAM.

Juga melekat pada peran terkait layanan adalah kebijakan kepercayaan IAM yang memungkinkan `ipam.amazonaws.com` layanan untuk mengambil peran terkait layanan.

Membuat peran terkait layanan

IPAM memantau penggunaan alamat IP dalam satu atau lebih akun dengan mengasumsikan peran terkait layanan dalam akun, menemukan sumber daya dan mereka CIDRs, dan mengintegrasikan sumber daya dengan IPAM.

Peran terkait layanan dibuat dengan salah satu dari dua cara:

- Ketika Anda berintegrasi dengan AWS Organizations

  Jika Anda Integrasikan IPAM dengan akun di Organisasi AWS menggunakan konsol IPAM atau menggunakan `enable-ipam-organization-admin-account` AWS CLI perintah, peran terkait layanan AWSServiceRoleForIPAM secara otomatis dibuat di setiap akun anggota Organizations AWS Anda. Akibatnya, sumber daya dalam semua akun anggota dapat ditemukan oleh IPAM.

  > **Important**
  >
  > Agar IPAM dapat membuat peran terkait layanan atas nama Anda:
  >
  > - Akun manajemen AWS Organizations yang memungkinkan integrasi IPAM dengan AWS Organizations harus memiliki kebijakan IAM yang memungkinkan tindakan berikut:
  >   - `ec2:EnableIpamOrganizationAdminAccount`
  >   - `organizations:EnableAwsServiceAccess`
  >   - `organizations:RegisterDelegatedAdministrator`
  >   - `iam:CreateServiceLinkedRole`
  > - Akun IPAM harus memiliki kebijakan IAM yang melekat padanya yang memungkinkan tindakan. `iam:CreateServiceLinkedRole`

- Saat Anda membuat IPAM menggunakan satu akun AWS

  Jika AndaGunakan IPAM dengan satu akun, peran terkait layanan AWSServiceRoleForIPAM akan dibuat secara otomatis saat Anda membuat IPAM sebagai akun tersebut.

> **Important**
>
> Jika Anda menggunakan IPAM dengan satu AWS akun, sebelum Anda membuat IPAM, Anda harus memastikan bahwa AWS akun yang Anda gunakan memiliki kebijakan IAM yang melekat padanya yang mengizinkan tindakan tersebut. `iam:CreateServiceLinkedRole` Saat membuat IPAM, Anda secara otomatis membuat peran terkait layanan AWSServiceRoleForIPAM. Untuk informasi selengkapnya tentang mengelola kebijakan IAM, lihat Mengedit deskripsi peran terkait layanan di Panduan Pengguna IAM.

Mengedit peran terkait layanan

Anda tidak dapat mengedit peran terkait layanan AWSServiceRoleForIPAM.

Menghapus peran terkait layanan

Jika Anda tidak perlu lagi menggunakan IPAM, kami sarankan Anda menghapus peran terkait layanan AWSServiceRoleForIPAM.

> **Note**
>
> Anda dapat menghapus peran terkait layanan hanya setelah Anda menghapus semua sumber daya IPAM di akun Anda. AWS Ini memastikan bahwa Anda tidak dapat secara tidak sengaja menghapus kemampuan pemantauan IPAM.

Ikuti langkah-langkah berikut ini untuk menghapus peran yang terkait layanan menggunakan: AWS CLI

1. Hapus sumber daya IPAM Anda menggunakan deprovision-ipam-pool-cidrdan hapus-ipam. Untuk informasi selengkapnya, lihat Pembuangan CIDRs dari kolam dan Hapus 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 terkait layanan:. delete-service-linked-role Saat Anda menghapus peran terkait layanan, kebijakan terkelola IPAM juga akan dihapus. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

AWS kebijakan 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 secara otomatis dibuat di akun IAM Anda dan di setiap akun anggota AWS Organizations Anda, dan kebijakan terkelola dilampirkan ke peran terkait layanan AWSServiceRoleForIPAM.

Kebijakan terkelola ini memungkinkan IPAM untuk melakukan hal berikut:

- Pantau CIDRs yang terkait dengan sumber daya jaringan di semua anggota AWS Organisasi Anda.
- Simpan metrik yang terkait dengan IPAM di Amazon CloudWatch, seperti ruang alamat IP yang tersedia di kolam IPAM Anda dan jumlah sumber daya CIDRs yang mematuhi aturan alokasi.
- Ubah dan baca daftar awalan terkelola.

Contoh berikut menunjukkan detail kebijakan terkelola yang dibuat.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "IPAMDiscoveryDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeIpv6Pools",
```

```
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:ListByoipCidrs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsPublishActions",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

Pernyataan pertama dalam contoh sebelumnya memungkinkan IPAM untuk memantau yang CIDRs 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 Konsol Manajemen AWS untuk menampilkan data tentang alokasi di kolam dan cakupan IPAM Anda. Untuk informasi selengkapnya, lihat Pantau 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.

Ubah	Deskripsi	Date
AWSIPAMServiceRolePolicy	Tindakan ditambahkan ke kebijakan AWSIPAMService RolePolicy terkelola (ec2:ModifyManagedPrefixList,ec2:DescribeManagedPrefixLists, danec2:GetManagedPrefixListEntries) untuk mengaktifkan IPAM mengubah dan membaca daftar awalan terkelola.	Oktober 31, 2025
AWSIPAMServiceRolePolicy	Tindakan ditambahkan ke kebijakan AWSIPAMService RolePolicy terkelola (`organizations:ListChildren organizations:ListParents` ,, danorganizations:DescribeOrganizationalUnit) untuk memungkinkan IPAM mendapatkan rincian Unit Organisasi (OUs) dalam AWS Organizations sehingga	November 21, 2024

Ubah	Deskripsi	Date
	pelanggan dapat menggunakan IPAM di tingkat OU.	
AWSIPAMServiceRolePolicy	Tindakan ditambahkan ke kebijakan AWSIPAMService RolePolicy terkelola (`ec2:GetIpamDiscoveredPublicAddresses`) untuk mengaktifkan IPAM mendapatkan alamat IP publik selama penemuan sumber daya.	13 November 2023
AWSIPAMServiceRolePolicy	Tindakan ditambahkan ke kebijakan AWSIPAMService RolePolicy 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.	1 November 2023

Ubah	Deskripsi	Date
AWSIPAMServiceRolePolicy	Dua tindakan ditambahkan ke kebijakan AWSIPAMSe rvice RolePolicy terkelola (`ec2:GetIp amDiscoveredAccoun ts` dan`ec2:GetIp amDiscoveredResour ceCidrs`) untuk mengaktif kan IPAM agar AWS akun dan sumber daya CIDRs dipantau selama penemuan sumber daya.	Januari 25, 2023
IPAM mulai melacak perubahan	IPAM mulai melacak perubahan untuk kebijakan yang AWS dikelola.	2 Desember 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 (AWS RAM), dan Amazon. CloudWatch

JSON

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

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

```
                "StringLike": {
                    "iam:AWSServiceName": "ipam.amazonaws.com"
                }
            }
        }
    ]
}
```

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 selengkapnya, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Nama	Default	Dapat disesuaikan
Blok CIDR publik bersebelahan yang disediakan Amazon IPv4	2	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
CIDR publik bersebelahan yang disediakan Amazon panjang netmask blok IPv4	/29	Ukuran yang dapat diterima adalah antara/29 dan /30. Untuk meminta kenaikan, hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
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 IPv6 CIDR yang disediakan Amazon per kolam Regional	1	Ya. Hubungi AWS Support Center seperti yang dijelaska

Nama	Default	Dapat disesuaikan
		n dalam kuota AWS layanan di. Referensi Umum AWS
Autonomous System Numbers (ASNs) yang dapat Anda bawa ke IPAM	5	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
CIDRs per kolam	50	Ya
Target yang diaktifkan per kebijakan IPAM	100	Ya. Untuk meminta penyesuaian kuota, hubungi Pusat AWS Dukungan seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
Administrator IPAM per organisasi	1	Tidak
IPAMs per Wilayah	1	Tidak
Kebijakan IPAM per IPAM	10	Ya. Untuk meminta penyesuaian kuota, hubungi Pusat AWS Dukungan seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS

Nama	Default	Dapat disesuaikan
Aturan alokasi kebijakan IPAM per pasangan sumber daya-lokal*	10	Ya. Untuk meminta penyesuaian kuota, hubungi Pusat AWS Dukungan seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
Pengecualian unit organisasi per penemuan sumber daya	10	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
Kedalaman kolam (jumlah kolam di dalam kolam)	10	Ya
Kolam per lingkup	50	Ya
Penyelesai daftar awalan per IPAM	10	Ya
Target penyelesai daftar awalan per resolver daftar awalan	50	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
Aturan per resolver daftar awalan	100	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS

Nama	Default	Dapat disesuaikan
Entri CIDR per versi resolver daftar awalan	1000	Ya. Hubungi AWS Support Center seperti yang dijelaskan dalam kuota AWS layanan di. Referensi Umum AWS
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
Lingkup 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.

* Pasangan sumber daya lokal: Saat menyetel aturan alokasi, Anda harus menentukan jenis sumber daya (sumber daya seperti EIPs, ALBs, atau kluster RDS) dan lokal (AWS Wilayah atau Zona Lokal tempat aturan berlaku). AWS Aturan alokasi dicakup untuk jenis sumber daya dan kombinasi lokal ini.

Misalnya, jika Anda menetapkan kebijakan untuk EIPs di us-east-1, Anda dapat mengatur hingga 10 aturan untuk pasangan lokal sumber daya tertentu*.

Harga untuk IPAM

Amazon VPC IP Address Manager (IPAM) adalah layanan yang membantu Anda mengelola ruang alamat IP di seluruh AWS sumber daya dan jaringan lokal. IPAM menyediakan cara terpusat untuk merencanakan, memantau, dan mengontrol alamat IP yang digunakan oleh sumber daya Anda AWS dan lokal.

Bagian ini menjelaskan cara melihat informasi terkait harga dan biaya IPAM Anda saat ini.

Daftar Isi

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/rumah.
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- IPAddress Manajer-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

Meskipun situs dokumentasi AWS teknis adalah sumber daya yang komprehensif, ada banyak tempat lain untuk menemukan informasi tentang AWS layanan. AWS blog, whitepaper, studi kasus, dan forum komunitas dapat memberikan wawasan berharga, contoh dunia nyata, dan perspektif alternatif di luar rincian teknis resmi. Menjelajahi beragam sumber ini dapat memberi Anda pemahaman yang lebih menyeluruh tentang AWS penawaran.

Sumber daya terkait berikut dapat membantu Anda saat Anda bekerja dengan Amazon VPC IP Address Manager:

- Praktik Terbaik Manajer Alamat IP VPC Amazon: AWS Blog tentang praktik terbaik untuk merencanakan dan membuat skema alamat yang dapat diskalakan dengan Manajer Alamat IP VPC Amazon.
- Manajemen Alamat Jaringan dan Audit pada Skala dengan Amazon VPC IP Address Manager: Blog AWS yang memperkenalkan Amazon VPC IP Address Manager dan menunjukkan cara menggunakan layanan di konsol. AWS
- Konfigurasikan akses berbutir halus ke sumber daya yang Anda bagikan menggunakan AWS Resource Access Manager: AWS Blog yang menjelaskan cara berbagi kumpulan IPAM dengan akun di unit organisasi Organizations AWS .
- Visualisasikan manajemen dan perencanaan alamat IP perusahaan dengan peta CIDR: AWS Blog yang menjelaskan cara memvisualisasikan keseluruhan IPv4 dan IPv6 lanskap Anda menggunakan peta CIDR IPAM di konsol IPAM.

Riwayat dokumen untuk IPAM

Tabel berikut menjelaskan rilis untuk IPAM.

Fitur	Deskripsi	Tanggal Rilis
Bawa IP Anda sendiri untuk CloudFront menggunakan IPAM	Gunakan IPAM untuk mengelola BYOIP Anda CIDRs untuk layanan AWS global, dimulai dengan CloudFront layanan anycast.	November 21, 2025
Tentukan strategi IPv4 alokasi publik dengan kebijakan IPAM	Anda sekarang dapat menggunakan kebijakan IPAM untuk menentukan aturan yang memetakan AWS layanan ke kumpulan IPAM tertentu, membantu menentukan strategi IPv4 alokasi publik.	November 19, 2025
Integrasikan IPAM dengan infrastruktur Infoblox	Anda sekarang dapat mengintegrasikan IPAM dengan infrastruktur Infoblox, memungkinkan Anda mengelola alamat AWS IP melalui alur kerja Infoblox yang ada sambil mendapatkan kemampuan cloud-native. AWS Integrasi ini tersedia untuk cakupan pribadi dan membutuhk an Tingkat Lanjut IPAM.	November 7, 2025
Otomatiskan pembaruan daftar awalan	Anda sekarang dapat menggunakan resolver daftar awalan IPAM untuk mengotomatiskan pembaruan daftar awalan berdasarkan kumpulan IPAM. CIDRs	Oktober 31, 2025
Kelola alarm dari konsol IPAM	Anda sekarang dapat membuat dan mengelola CloudWatch alarm Amazon langsung dari konsol IPAM. Alarm terkait IPAM akan muncul sebagai bilah peringatan dan indikator visual saat dalam status INSUFFICIENT_DATA atau ALARM.	Agustus 21, 2025
Aktifkan distribusi biaya	Ketika Anda mengaktifkan distribusi biaya, Anda mendistribusikan biaya untuk alamat	1 Mei 2025

Fitur	Deskripsi	Tanggal Rilis
	IP aktif ke akun menggunakan alamat IP daripada ke pemilik IPAM. Ini berguna untuk organisasi besar di mana admin IPAM yang didelegasikan mengelola alamat IP secara terpusat menggunakan IPAM dan setiap akun bertanggung jawab atas penggunaa nnya sendiri, menghilangkan kebutuhan untuk perhitungan penagihan manual.	
Kecualikan unit organisasi dari IPAM	Jika IPAM Anda terintegrasi dengan AWS Organizations, Anda sekarang dapat mengecualikan unit organisasi dari IPAM. IPAM tidak akan mengelola alamat IP dalam akun dalam pengecualian unit organisasi.	November 21, 2024
AWS pembaruan kebijakan terkelola - Pembaruan ke kebijakan yang ada	Ada AWSIPAMService RolePolicy diperbarui.	November 21, 2024
Alokasikan alamat IP Elastis berurutan dari kolam IPAM	IPAM sekarang memungkinkan Anda untuk menyediakan IPv4 blok publik milik Amazon ke kolam IPAM dan mengalokasikan alamat IP Elastis berurutan dari kumpulan tersebut ke sumber daya. AWS Alamat IP Elastis Berurutan memungkinkan Anda untuk menyederhanakan jaringan dan kebutuhan daftar keamanan yang memungkinkan Anda.	Agustus 28, 2024
IPv6 GUA pribadi dan ULAs	Anda sekarang dapat menyediakan rentang IPv6 GUA dan ULA pribadi ke kolam IPAM dalam lingkup pribadi. IPv6 Alamat pribadi hanya tersedia di IPAM. Untuk informasi selengkapnya tentang IPv6 pengalamatan pribadi, lihat IPv6 Alamat pribadi di Panduan Pengguna Amazon VPC.	Agustus 8, 2024

Fitur	Deskripsi	Tanggal Rilis
IPAM Tingkatan Gratis dan Tingkat Lanjut	Anda sekarang dapat memilih antara Tingkat Gratis dan Tingkat Lanjut untuk IPAM Anda.	17 November 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.	17 November 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.	17 November 2023
Bawa ASN Anda sendiri (BYOASN)	Anda sekarang dapat membawa nomor sistem otonom Anda sendiri (ASN) ke AWS.	17 November 2023
AWS pembaruan kebijakan terkelola - Pembaruan ke kebijakan yang ada	Ada AWSIPAMService RolePolicy diperbarui.	17 November 2023
AWS pembaruan kebijakan terkelola - Pembaruan ke kebijakan yang ada	Ada AWSIPAMService RolePolicy diperbarui.	1 November 2023
Metrik pemanfaatan sumber daya	IPAM sekarang menerbitkan metrik pemanfaat an IP untuk sumber daya yang dipantau IPAM ke Amazon. CloudWatch	2 Agustus 2023

Fitur	Deskripsi	Tanggal Rilis
Wawasan IP publik	Wawasan IP publik menunjukkan kepada Anda semua IPv4 alamat publik yang digunakan oleh layanan di Wilayah ini di akun Anda. Anda dapat menggunakan wawasan ini untuk mengidentifikasi penggunaan IPv4 alamat publik dan melihat rekomendasi untuk merilis alamat IP Elastis yang tidak digunakan.	28 Juli 2023
AWS pembaruan kebijakan terkelola - Pembaruan ke kebijakan yang ada	Ada AWSIPAMService RolePolicy diperbarui.	Januari 25, 2023
Integrasikan IPAM dengan akun di luar organisasi Anda	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 IPv6 bersebelahan yang disediakan Amazon untuk kolam IPAM	Saat Anda membuat kolam IPAM di ruang lingkup publik, Anda sekarang dapat menyediakan blok CIDR IPv6 bersebelahan yang disediakan Amazon ke kolam. Untuk informasi selengkapnya, lihat Buat kumpulan IPv6 alamat di IPAM Anda.	Januari 25, 2023
Rilis awal	Rilis ini memperkenalkan Amazon VPC IP Address Manager.	2 Desember 2021

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.