



IP 주소 관리자

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: IP 주소 관리자

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

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon 계열사, 관련 업체 또는 Amazon의 지원 업체 여부에 상관없이 해당 소유자의 자산입니다.

Table of Contents

IPAM이란?	1
IPAM 작동 방식	2
IPAM 시작하기	4
IPAM 액세스	4
IPAM에 대한 권한 구성	5
AWS Organization에서 계정과 IPAM 통합	5
IPAM을 조직 외부 계정과 통합	8
단일 계정을 통해 IPAM 사용	10
IPAM 생성	10
IP 주소 프로비저닝 계획	13
IPAM 풀 계획의 예	14
IPv4 풀 생성	16
IPv6 풀 생성	25
CIDR 할당	31
IPAM 풀 CIDR을 사용하는 VPC 생성	32
CIDR을 풀에 수동으로 할당하여 IP 주소 공간을 예약합니다.	32
IPAM에서 IP 주소 공간 관리	34
VPC 생성에 IPAM 사용 적용	34
VPC를 생성할 때 IPAM 적용	35
VPC를 생성할 때 IPAM 풀 적용	35
지정된 OU 목록을 제외한 모든 OU에 IPAM 적용	36
AWS RAM을 사용하여 IPAM 풀 공유	37
풀에 CIDR 프로비저닝	39
풀에서 CIDR 프로비저닝 해제	40
풀 편집	41
풀 삭제	42
리소스 검색 작업	43
리소스 검색 생성	44
리소스 검색 세부 정보 보기	45
리소스 검색 공유	47
리소스 검색을 IPAM과 연결	49
리소스 검색 연결 해제	50
리소스 검색 삭제	51
추가 범위 생성	51

범위 간에 VPC CIDR 이동	53
VPC CIDR의 모니터링 상태 변경	54
범위 삭제	55
할당 해제	56
IPAM 수정	58
IPAMM 티어 수정	58
IPAM 운영 리전 수정	60
IPAM 삭제	60
IPAM에서 IP 주소 사용량 추적	63
IPAM 대시보드를 사용하여 CIDR 사용량 모니터링	63
리소스별 CIDR 사용량 모니터링	65
Amazon CloudWatch를 사용하여 IPAM 모니터링	69
IPAM 풀 및 범위 지표	69
리소스 사용률 지표	71
IP 주소 기록 보기	76
퍼블릭 IP 인사이트 보기	79
튜토리얼	84
콘솔을 사용하여 IPAM 및 풀 생성	84
필수 조건	85
AWS Organizations가 IPAM과 통합되는 방식	85
1단계: IPAM 관리자 위임	86
2단계: IPAM 생성	87
3단계: 최상위 IPAM 풀 생성	90
4단계: 리전 IPAM 풀 생성	95
5단계: 사전 프로덕션 개발 풀 생성	99
6단계: IPAM 풀 공유	103
7단계: IPAM 풀에서 할당된 CIDR을 사용하여 VPC 생성	108
8단계: 정리	112
AWS CLI를 사용하여 IPAM 및 풀 생성	113
1단계: 조직에서 IPAM 사용 설정	114
2단계: IPAM 생성	115
3단계: IPv4 주소 풀 생성	117
4단계: 최상위 풀에 CIDR 프로비저닝	119
5단계: 최상위 풀에서 소싱된 CIDR을 사용하여 리전 풀 생성	120
6단계: 리전 풀에 CIDR 프로비저닝	122
7단계: 계정 간 IP 할당을 사용 설정하기 위한 RAM 공유 생성	123

8단계. VPC 생성	124
9단계. 정리	125
AWS CLI를 사용하여 IP 주소 기록 보기	125
개요	126
시나리오	126
IPAM으로 ASN 가져오기	134
ASN에 대한 온보딩 사전 조건	135
자습서 단계	135
IPAM으로 IP 주소 가져오기	139
AWS 콘솔 및 CLI	140
AWS CLI 전용	163
IPAM으로 BYOIP IPv4 CIDR 전송	205
1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성	206
2단계: IPAM의 퍼블릭 범위 ID 가져오기	206
3단계: IPAM 풀 생성	207
4단계: AWS RAM을 사용하여 IPAM 풀 공유	209
5단계: IPAM으로 기존 BYOIP IPv4 CIDR 전송	211
6단계: IPAM에서 CIDR 보기	214
7단계: 정리	214
서브넷 IP 할당을 위한 VPC IP 주소 공간 계획	218
1단계: VPC 생성	219
2단계: 리소스 계획 풀 생성	220
3단계: 서브넷 풀 생성	220
4단계: 서브넷 생성	221
5단계: 정리	222
IPAM의 자격 증명 및 액세스 관리	223
IPAM의 서비스 연결 역할	223
서비스 연결 역할에 부여된 권한	223
서비스 연결 역할 생성	224
서비스 연결 역할 편집	225
서비스 연결 역할 삭제	225
IPAM에 대한 관리형 정책	225
AWS 관리형 정책으로 업데이트	227
예제 정책	228
할당량	231
요금	233

요금 정보 보기	233
AWS Cost Explorer을(를) 사용하여 현재 비용 및 사용량 확인	233
관련 정보	234
사용 설명서 기록	235

IPAM이란?

Amazon VPC IP 주소 관리자(IPAM)는 AWS 워크로드의 IP 주소를 보다 쉽게 계획, 추적 및 모니터링할 수 있게 해주는 VPC 기능입니다. IPAM의 자동화된 워크플로우를 사용하여 IP 주소를 보다 효율적으로 관리할 수 있습니다.

IPAM을 사용하여 다음을 수행할 수 있습니다.

- IP 주소 공간을 라우팅 및 보안 도메인으로 구성
- 사용 중인 IP 주소 공간 모니터링 및 비즈니스 규칙을 위반하여 공간을 사용하는 리소스 모니터링
- 조직의 IP 주소 할당 기록 보기
- 특정 비즈니스 규칙을 사용하여 VPC에 CIDR 자동 할당
- 네트워크 연결 문제 해결
- BYOIP(Bring Your Own IP) 주소의 리전 간 및 계정 간 공유 사용 설정
- Amazon에서 제공한 연속 IPv6 CIDR 블록을 VPC 생성을 위한 풀에 프로비저닝

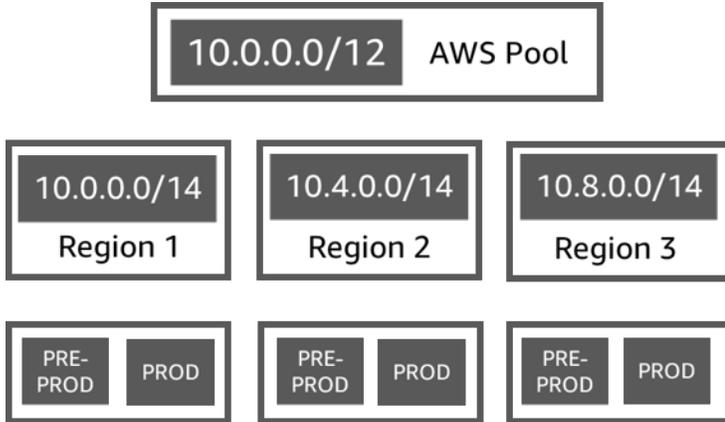
이 가이드는 다음 섹션을 포함하고 있습니다.

- [IPAM 작동 방식](#): IPAM의 개념 및 용어입니다.
- [IPAM 시작하기](#): AWS Organizations를 사용하여 전사적 IP 주소 관리를 사용 설정하고, IPAM을 생성하고, IP 주소 사용을 계획하는 단계입니다.
- [IPAM에서 IP 주소 공간 관리](#): IPAM, 범위, 풀 및 할당을 관리하는 단계입니다.
- [IPAM에서 IP 주소 사용량 추적](#): IPAM을 사용하여 IP 주소 사용을 모니터링하고 추적하는 단계입니다.
- [Amazon VPC IP Address Manager 자습서](#): IPAM 및 풀 생성, VPC CIDR 할당, 고유 퍼블릭 IP 주소 CIDR을 IPAM으로 가져오기에 대한 자세한 단계별 자습서입니다.

IPAM 작동 방식

IPAM을 시작하는 데 도움이 되도록 이번 주제에서는 몇 가지 주요 개념을 설명합니다.

다음 다이어그램은 최상위 IPAM 풀 내에서 여러 AWS 리전에 대한 IPAM 풀 계층을 보여줍니다. 각 AWS 리전 풀에는 IPAM 개발 풀 2개(사전 프로덕션 풀 1개와 풀 프로덕션 리소스 1개)가 있습니다. IPAM 개념에 대한 자세한 내용은 다이어그램 아래의 설명을 참조하세요.



Amazon VPC IP 주소 관리자를 사용하려면 먼저 IPAM을 생성해야 합니다.

IPAM을 생성하는 경우 IPAM을 만들 AWS 리전을 선택할 수 있습니다. IPAM을 생성하는 경우 AWS VPC IPAM은 IPAM에 대한 2개의 범위를 자동으로 생성합니다. 풀 및 할당과 함께 범위는 IPAM의 핵심 구성 요소입니다.

- 범위는 IPAM 내에서 가장 높은 수준의 컨테이너입니다. IPAM에는 2개의 기본 범위가 포함되어 있습니다. 각 범위는 단일 네트워크의 IP 공간을 나타냅니다. 프라이빗 범위(private scope)는 모든 프라이빗 공간을 위한 것입니다. 퍼블릭 범위(public scope)는 모든 퍼블릭 공간을 위한 것입니다. 범위를 사용하면 IP 주소가 중복되거나 충돌하지 않고 연결되지 않은 여러 네트워크에서 IP 주소를 재사용할 수 있습니다. 범위 내에서 IPAM 풀을 생성합니다.
- 풀(pool)은 연속 IP 주소 범위(또는 CIDR)의 모음입니다. IPAM 풀을 사용하면 라우팅 및 보안 요구 사항에 따라 IP 주소를 구성할 수 있습니다. 최상위 풀 내에 여러 개의 풀이 있을 수 있습니다. 예를 들어 개발 및 프로덕션 애플리케이션에 별도의 라우팅 및 보안 요구 사항이 있는 경우 각각에 대한 풀을 생성할 수 있습니다. IPAM 풀 내에서 CIDR을 AWS 리소스에 할당할 수 있습니다.
- 할당(allocation)은 IPAM 풀에서 다른 리소스 또는 IPAM 풀로 CIDR을 할당하는 것입니다. VPC를 생성하고 VPC의 CIDR에 대한 IPAM 풀을 선택하면 CIDR이 IPAM 풀에 프로비저닝된 CIDR에서 할당됩니다. IPAM을 사용하여 할당을 모니터링하고 관리할 수 있습니다.

IPAM은 소유한 프라이빗 IPv4 CIDR, 퍼블릭 IPv4/IPv6 CIDR, Amazon 소유 퍼블릭 IPv6 공간을 관리하고 모니터링할 수 있습니다.

IPAM을 생성하고 시작하려면 [IPAM 시작하기](#) 섹션을 참조하세요.

IPAM 시작하기

IPAM을 시작하려면 이 섹션의 단계를 따르세요. 먼저 IPAM에 액세스하여 IPAM 계정을 위임할지 여부를 결정합니다. 이 섹션을 마치면 IPAM을 생성하고, IP 주소 풀을 여러 개 생성하고, 풀의 CIDR을 VPC 할당할 수 있습니다.

내용

- [IPAM 액세스](#)
- [IPAM에 대한 권한 구성](#)
- [IPAM 생성](#)
- [IP 주소 프로비저닝 계획](#)
- [CIDR 할당](#)

IPAM 액세스

다른 AWS 서비스와 마찬가지로 다음 방법을 사용하여 IPAM을 생성하고, 액세스하고, 관리할 수 있습니다.

- AWS Management Console: IPAM을 생성하고 관리할 때 사용할 수 있는 웹 인터페이스를 제공합니다. <https://console.aws.amazon.com/ipam/>을 참조하세요.
- AWS Command Line Interface(AWS CLI): Amazon VPC를 비롯한 다양한 AWS 서비스에 대한 명령을 제공합니다. AWS CLI는 Windows, macOS, Linux에서 지원됩니다. AWS CLI를 가져오려면 [AWS Command Line Interface](#)를 참조하세요.
- AWS SDK: 언어별 API를 제공합니다. AWS SDK는 서명 계산, 요청 재시도 처리 및 오류 처리와 같은 많은 연결 세부 정보를 관리합니다. 자세한 정보는 [AWS SDK](#)를 참조하세요.
- 쿼리 API(Query API): HTTPS 요청을 사용하여 호출하는 하위 수준의 API 작업을 제공합니다. 쿼리 API 사용은 IPAM에 액세스할 수 있는 가장 직접적인 방법입니다. 하지만 이를 사용하려면 애플리케이션에서 요청에 서명할 해시 생성 및 오류 처리와 같은 하위 수준의 세부 정보를 처리해야 합니다. 자세한 내용은 [Amazon EC2 API 참조](#)의 Amazon IPAM 작업을 참조하세요.

이 가이드에서는 IPAM을 생성하고, 액세스하고, 관리할 수 있는 AWS 관리 콘솔을 사용하는 방법에 중점을 둡니다. 콘솔에서 프로세스를 완료하는 방법에 대한 각 설명에는 AWS CLI를 사용하여 동일한 작업을 수행하는 방법을 보여주는 AWS CLI 문서에 대한 링크가 포함됩니다.

IPAM을 처음 사용하시는 경우 [IPAM 작동 방식](#) 섹션을 참조하여 Amazon VPC에서 IPAM의 역할에 대해 알아본 후 [IPAM에 대한 권한 구성](#) 섹션의 지침을 따라 계속 진행합니다.

IPAM에 대한 권한 구성

IPAM을 사용하기 전에 IPAM이 EC2 네트워킹 리소스와 연결된 CIDR을 모니터링하고 지표를 저장하도록 하려면 이 섹션의 옵션 중 하나를 선택해야 합니다.

- IPAM과 AWS Organizations를 통합하여 Amazon VPC IPAM 서비스가 모든 AWS Organizations 멤버 계정에서 생성한 네트워킹 리소스를 관리하고 모니터링할 수 있도록 하려면 [AWS Organization에서 계정과 IPAM 통합](#)을 참조하세요.
- AWS Organizations와 통합한 후 IPAM을 조직 외부 계정과 통합하려면 [IPAM을 조직 외부 계정과 통합](#)을 참조하세요.
- IPAM을 통해 단일 AWS 계정을 사용하고 Amazon VPC IPAM 서비스가 단일 계정을 통해 생성한 네트워킹 리소스를 관리 및 모니터링할 수 있도록 하려면, [단일 계정을 통해 IPAM 사용](#) 섹션을 참조하세요.

이러한 옵션 중 하나를 선택하지 않는 경우 풀과 같은 IPAM 리소스를 만들 수는 있지만 대시보드에 지표가 표시되지 않으므로 리소스 상태를 모니터링할 수 없습니다.

내용

- [AWS Organization에서 계정과 IPAM 통합](#)
- [IPAM을 조직 외부 계정과 통합](#)
- [단일 계정을 통해 IPAM 사용](#)

AWS Organization에서 계정과 IPAM 통합

선택적으로 이 섹션의 단계에 따르면 IPAM을 AWS Organizations와 통합하고 멤버 계정을 IPAM 계정으로 위임할 수 있습니다.

IPAM 계정은 IPAM을 생성하고 이를 사용하여 IP 주소 사용을 관리 및 모니터링하는 일을 담당합니다.

AWS Organizations와 IPAM을 통합하고 IPAM 관리자를 위임하면 다음과 같은 장점이 있습니다.

- IPAM 풀을 조직과 공유: IPAM 계정을 위임하면 IPAM에서 조직의 다른 AWS Organizations 멤버 계정이 AWS RAM(Resource Access Manager)을 사용하여 공유되는 IPAM 풀의 CIDR을 할

당하도록 허용합니다. 조직 설정에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [AWS Organizations란 무엇인가요?](#)를 참조하세요.

- 조직의 IP 주소 사용량 모니터링: IPAM 계정을 위임하면 모든 계정에서 IP 사용량을 모니터링할 수 있는 권한을 IPAM에 부여합니다. 그러면 IPAM은 다른 AWS Organizations 멤버 계정에서 기존 VPC가 사용하는 CIDR을 IPAM으로 가져옵니다.

AWS Organizations 멤버 계정을 IPAM 계정으로 위임하지 않은 경우 IPAM은 IPAM을 생성하는 데 사용하는 AWS 계정의 리소스만 모니터링합니다.

Important

- AWS 관리 콘솔에서 IPAM을 사용하거나 [enable-ipam-organization-admin-account](#) AWS CLI 명령을 사용하여 AWS Organizations와의 통합을 사용 설정해야 합니다. 이렇게 하면 AWSServiceRoleForIPAM 서비스 연결 역할이 생성됩니다. AWS Organizations 콘솔 또는 [register-delegated-administrator](#) AWS CLI 명령을 사용하여 AWS Organizations에 대한 신뢰할 수 있는 액세스를 사용 설정하면 AWSServiceRoleForIPAM 서비스 연결 역할이 생성되지 않으며 조직 내 리소스를 관리하거나 모니터링할 수 없습니다.

Note

AWS Organizations와 통합하는 경우

- IPAM은 조직의 멤버 계정에서 모니터링하는 각 활성 IP 주소에 대해 요금을 청구합니다. 요금에 대한 자세한 내용은 [IPAM 요금](#)을 참조하세요.
- AWS Organizations의 계정 및 관리 계정이 1개 이상의 멤버 계정으로 설정되어 있어야 합니다. 계정 유형에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [용어 및 개념](#)을 참조하세요. 조직 설정에 대한 자세한 내용은 [AWS Organizations 시작하기](#)를 참조하세요.
- IPAM 계정은 AWS Organizations 멤버 계정이어야 합니다. AWS Organizations 관리 계정을 IPAM 계정으로 사용할 수 없습니다.
- IPAM 계정은 iam:CreateServiceLinkedRole 작업을 허용하는 IAM 정책이 연결된 IAM 역할을 사용해야 합니다. IPAM을 생성할 경우 AWSServiceRoleForIPAM 서비스 연결 역할이 자동으로 생성됩니다.
- AWS Organizations 관리 계정과 연결된 사용자는 다음과 같은 IAM 정책 작업이 연결된 IAM 역할을 사용해야 합니다.

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

IAM 역할 생성에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 사용자에게 권한을 위임하는 역할 생성](#)을 참조하세요.

- AWS Organizations 관리 계정과 연결된 사용자는 현재 AWS Orgs 위임 관리자 (`organizations:ListDelegatedAdministrators`)가 나열되는 다음과 같은 IAM 정책 작업이 연결되어 있는 IAM 역할을 사용할 수 있습니다.

AWS Management Console

IPAM 계정을 선택하려면

1. AWS Organizations 관리 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. AWS 관리 콘솔에서 IPAM에서 작업하려는 AWS 리전을 선택합니다.
3. 탐색 창에서 조직 설정을 선택합니다.
4. 위임 옵션은 콘솔에 AWS 조직 마스터 계정으로 로그인한 경우에만 사용할 수 있습니다. 위임을 선택합니다.
5. IPAM 계정에 AWS 계정 ID를 입력합니다. IPAM 관리자는 AWS Organizations 멤버 계정이어야 합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

- AWS CLI를 사용하여 IPAM 관리자 계정을 위임하려면 [enable-ipam-organization-admin-account](#)와 같은 명령을 사용합니다.

Organizations 멤버 계정을 IPAM 계정으로 위임하면 IPAM은 조직의 모든 멤버 계정에서 서비스 연결 IAM 역할을 자동으로 생성합니다. IPAM은 각 멤버 계정에서 서비스 연결 IAM 역할을 맡고, 리소스 및

해당 CIDR을 검색하고, IPAM과 통합하여 이러한 계정의 IP 주소 사용량을 모니터링합니다. 모든 멤버 계정 내의 리소스는 조직 단위에 관계없이 IPAM에서 검색할 수 있습니다. 예를 들어 VPC를 생성한 멤버 계정이 있는 경우 IPAM 콘솔의 리소스 섹션에 VPC와 해당 CIDR이 표시됩니다.

Important

IPAM 관리자를 위임한 AWS Organizations 관리 계정이 이제 완료되었습니다. IPAM을 계속 사용하려면 IPAM 관리자 계정이 Amazon VPC IPAM에 로그인하여 IPAM을 생성해야 합니다.

IPAM을 조직 외부 계정과 통합

이 섹션에서는 IPAM을 조직 외부 AWS 계정과 통합하는 방법을 설명합니다. 이 섹션의 단계를 완료하려면 [AWS Organization에서 계정과 IPAM 통합](#)의 단계를 이미 완료하고 IPAM 계정을 위임했어야 합니다.

IPAM을 조직 외부의 AWS 계정과 통합하면 다음과 같은 작업을 수행할 수 있습니다.

- 한 IPAM 계정에서 조직 외부의 IP 주소를 관리합니다.
- 다른 AWS Organizations의 다른 AWS 계정에서 호스팅하는 타사 서비스와 IPAM 풀을 공유합니다.

IPAM을 조직 외부의 AWS 계정과 통합한 후에는 IPAM 풀을 다른 조직의 원하는 계정과 직접 공유할 수 있습니다.

내용

- [고려 사항 및 제한](#)
- [프로세스 개요](#)

고려 사항 및 제한

이 섹션에는 IPAM을 조직 외부 계정과 통합할 때의 고려 사항 및 제한 사항이 포함되어 있습니다.

- 리소스 검색을 다른 계정과 공유할 때 교환되는 데이터는 IP 주소 및 계정 상태 모니터링 데이터뿐입니다. 공유하기 전에 [get-ipam-Discovered-resource-cidrs](#)과 [get-ipam-discovered-accounts](#) CLI 명령 또는 [GetIPAM DiscoveredResourceCidrs](#)과 [GetIPAM DiscoveredAccounts](#) API를 사용하여 이 데이터를 공유할 수 있습니다. 조직 전체의 리소스를 모니터링하는 리소스 검색의 경우 조직 데이터(예: 조직의 조직 단위 이름)는 공유되지 않습니다.

- 리소스 검색을 생성하면 리소스 검색은 소유자 계정에 표시되는 모든 리소스를 모니터링합니다. 소유자 계정이 여러 고객을 위한 리소스를 생성하는 타사 서비스 AWS 계정인 경우 리소스 검색을 통해 해당 리소스가 검색됩니다. 타사 AWS 서비스 계정이 최종 사용자 AWS 계정과 리소스 검색을 공유하는 경우 최종 사용자는 타사 AWS 서비스의 다른 고객의 리소스를 볼 수 있습니다. 따라서 타사 AWS 서비스에서는 리소스 검색 생성 및 공유에 주의를 기울이거나 각 고객에 대해 별도의 AWS 계정을 사용해야 합니다.

프로세스 개요

이 섹션에서는 IPAM을 조직 외부의 AWS 계정과 통합하는 방법을 설명합니다. 이 가이드의 다른 섹션의 주제를 참조합니다. 이 페이지를 계속 표시하고 아래에 링크된 주제를 새 창에서 열면 이 페이지로 돌아와 지침을 확인할 수 있습니다.

IPAM을 조직 외부의 AWS 계정과 통합하는 경우 프로세스에는 4개의 AWS 계정이 포함됩니다.

- 기본 조직 소유자 - 조직 1의 AWS Organizations 관리 계정입니다.
- 기본 조직 IPAM 계정 - 조직 1의 IPAM 위임된 관리자 계정입니다.
- 보조 조직 소유자 - 조직 2의 AWS Organizations 관리 계정입니다.
- 보조 조직 관리자 계정 - 조직 2의 IPAM 위임된 관리자 계정입니다.

단계

1. 기본 조직 소유자는 조직의 구성원을 기본 조직 IPAM 계정으로 위임합니다([AWS Organization에서 계정과 IPAM 통합](#) 참조).
2. 기본 조직 IPAM 계정은 IPAM을 생성합니다([IPAM 생성](#) 참조).
3. 보조 조직 소유자는 조직의 구성원을 보조 조직 관리자 계정으로 위임합니다([AWS Organization에서 계정과 IPAM 통합](#) 참조).
4. 보조 조직 관리자 계정은 리소스 검색을 생성하고 AWS RAM을 사용하여 기본 조직 IPAM 계정과 공유합니다([리소스 검색 생성](#) 및 [리소스 검색 공유](#) 참조). 리소스 검색은 기본 조직 IPAM과 동일한 홈 리전에 생성해야 합니다.
5. 기본 조직 IPAM 계정은 AWS RAM을 사용하여 리소스 공유 초대를 수락합니다(AWS RAM 사용 설명서의 [리소스 공유 초대 수락 및 거부](#) 참조).
6. 기본 조직 IPAM 계정은 리소스 검색을 해당 IPAM과 연결합니다([리소스 검색을 IPAM과 연결](#) 참조).

7. 기본 조직 IPAM 계정은 이제 보조 조직의 계정으로 생성된 IPAM 리소스를 모니터링 및/또는 관리할 수 있습니다.
8. (선택 사항) 기본 조직 IPAM 계정은 보조 조직의 구성원 계정과 IPAM 풀을 공유합니다([AWS RAM을 사용하여 IPAM 풀 공유](#) 참조).
9. (선택 사항) 기본 조직 IPAM 계정에서 보조 조직의 리소스 검색을 중지하려는 경우 IPAM에서 리소스 검색을 분리할 수 있습니다([리소스 검색 연결 해제](#) 참조).
10. (선택 사항) 보조 조직 관리자 계정이 기본 조직의 IPAM에 참여하지 않으려는 경우 공유 리소스 검색의 공유를 취소하거나(AWS RAM 사용 설명서의 [AWS RAM에서 리소스 공유 업데이트](#) 참조) 리소스 검색을 삭제할 수 있습니다([리소스 검색 삭제](#) 참조).

단일 계정을 통해 IPAM 사용

[AWS Organization에서 계정과 IPAM 통합](#)을 선택하지 않는 경우 단일 AWS 계정을 통해 IPAM을 사용할 수 있습니다.

다음 섹션에서 IPAM을 생성할 경우 AWS Identity and Access Management의 Amazon VPC IPAM 서비스에 대해 서비스 연결 역할이 자동으로 생성됩니다. IPAM은 서비스 연결 역할을 사용하여 EC2 네트워킹 리소스와 연결된 CIDR에 대한 지표를 모니터링하고 저장합니다. 서비스 연결 역할 및 IPAM이 이를 사용하는 방법에 대한 자세한 내용은 [IPAM의 서비스 연결 역할](#) 섹션을 참조하세요.

Important

단일 AWS 계정을 사용하여 IPAM을 사용하는 경우 IPAM을 생성하는 데 사용하는 AWS 계정은 iam:CreateServiceLinkedRole 작업을 허용하는 정책이 연결된 IAM 역할을 사용해야 합니다. IPAM을 생성할 경우 AWSServiceRoleForIPAM 서비스 연결 역할이 자동으로 생성됩니다. IAM 정책 관리에 대한 자세한 내용은 [IAM 사용 설명서](#)의 IAM 정책 편집을 참조하세요.

단일 AWS 계정에 IPAM 서비스 연결 역할을 생성할 수 있는 권한이 있을 경우 [IPAM 생성](#)(으)로 이동합니다.

IPAM 생성

이 섹션의 단계를 따르면 IPAM을 생성할 수 있습니다. IPAM 관리자를 위임한 경우 IPAM 계정에서 이러한 단계를 완료해야 합니다.

⚠ Important

IPAM을 생성하는 경우 IPAM이 소스 계정의 데이터를 IPAM 위임 계정으로 복제하도록 허용하라는 메시지가 표시됩니다. AWS Organizations 및 IPAM을 통합하려면 IPAM에는 계정(멤버 계정에서 위임된 IPAM 멤버 계정으로) 및 AWS 리전(운영 리전에서 IPAM의 홈 리전으로) 전체에서 리소스 및 IP 사용 세부 정보를 복제할 수 있는 권한이 필요합니다. 단일 계정 IPAM 사용자의 경우 IPAM에는 운영 리전 전체에서 리소스 및 IP 사용 세부 정보를 IPAM의 홈 리전으로 복제할 수 있는 권한이 필요합니다.

IPAM을 생성하는 경우 IPAM에서 IP 주소 CIDR을 관리할 수 있는 AWS 리전을 선택합니다. 이러한 AWS 리전을 운영 리전이라고 합니다. IPAM은 운영 리전으로 선택한 AWS 리전에서만 리소스를 검색하고 모니터링합니다. IPAM은 선택한 운영 리전 외부에는 어떠한 데이터도 저장하지 않습니다.

다음의 예 계층에서는 IPAM을 생성할 때 할당하는 AWS 리전이 나중에 생성하는 풀에 사용할 수 있는 리전에 영향을 미치는 방법을 보여줍니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 프라이빗 범위
 - 최상위 IPAM 풀
 - AWS 리전 2의 리전 IPAM 풀
 - 개발 풀
 - AWS 리전 2에서 VPC 할당

IPAM 하나만 생성할 수 있습니다. IPAM과 관련된 할당량 증가에 대한 자세한 내용은 [IPAM의 할당량](#) 섹션을 참조하세요.

AWS Management Console

IPAM을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. AWS 관리 콘솔에서 IPAM을 생성하려는 AWS 리전을 선택합니다. 기본 작업 리전에서 IPAM을 생성합니다.
3. 서비스 홈 페이지에서 IPAM 생성(Create IPAM)을 선택합니다.

4. Amazon VPC IP 주소 관리자가 소스 계정의 데이터를 IPAM 위임 계정으로 복제하도록 허용 (Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account)을 선택합니다. 이 옵션을 선택하지 않은 경우 IPAM을 생성할 수 없습니다.
5. IPAM 티어를 선택합니다. 각 티어에서 사용할 수 있는 기능 및 티어 관련 비용에 대한 자세한 내용은 [Amazon VPC 요금 페이지](#)의 IPAM 탭을 참조하세요.
6. 운영 리전(Operating regions)에서 이 IPAM이 리소스를 관리하고 검색할 수 있는 AWS 리전을 선택합니다. IPAM을 생성하는 AWS 리전은 기본적으로 운영 리전 중 하나로 선택됩니다. 예를 들어 AWS 리전 us-east-1에서 이 IPAM을 생성하지만 나중에 us-west-2의 VPC에 CIDR을 제공하는 리전 IPAM 풀을 생성하려는 경우 여기에서 us-west-2를 선택합니다. 운영 리전을 잊어버린 경우 나중에 다시 돌아와서 IPAM 설정을 편집할 수 있습니다.

 Note

프리 티어에서 IPAM을 생성하는 경우 IPAM에 대해 여러 운영 리전을 선택할 수 있지만 운영 리전 전체에서 사용할 수 있는 유일한 IPAM 기능은 [퍼블릭 IP 인사이트](#)입니다. IPAM 운영 리전 전체에서 BYOIP와 같은 프리 티어의 다른 기능을 사용할 수 없습니다. IPAM의 홈 리전에서만 사용할 수 있습니다. 운영 리전 전체에서 모든 IPAM 기능을 사용하려면 [고급 티어에서 IPAM을 생성](#)하세요.

7. IPAM 생성(Create IPAM)을 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음의 AWS CLI 명령을 사용하여 IPAM과 관련된 세부 정보를 생성, 수정 및 확인할 수 있습니다.

1. IPAM 생성: [create-ipam](#)
2. 생성한 IPAM 확인: [describe-ipams](#)
3. 자동으로 생성되는 범위 확인: [describe-ipam-scopes](#)
4. 기존 IPAM 수정: [modify-ipam](#)

이러한 단계가 완료되면 IPAM이 다음을 수행합니다.

- IPAM을 생성했습니다. 콘솔의 왼쪽 탐색 창에서 IPAM을 선택하면 IPAM 및 현재 선택한 운영 리전을 확인할 수 있습니다.
- 하나의 프라이빗 범위와 하나의 퍼블릭 범위를 생성했습니다. 탐색 창에서 범위(Scopes)를 선택하면 범위를 확인할 수 있습니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.

IP 주소 프로비저닝 계획

이 섹션의 단계를 따르면 IPAM 풀을 사용하여 IP 주소 프로비저닝 계획을 세울 수 있습니다. IPAM 계정을 구성한 경우 해당 계정에서 이러한 단계를 완료해야 합니다. 풀 생성 프로세스는 퍼블릭 및 프라이빗 범위의 풀에 따라 다릅니다. 이 섹션에는 프라이빗 범위에서 지역 풀을 만드는 단계가 포함되어 있습니다. BYOIP 및 BYOASN 자습서는 [튜토리얼](#)을 참조하십시오.

Important

AWS 계정에서 IPAM 풀을 사용하려면 IPAM과 AWS Organizations를 통합해야 합니다. 그렇지 않으면 일부 기능이 올바르게 작동하지 않을 수 있습니다. 자세한 내용은 [AWS Organization에서 계정과 IPAM 통합](#) 섹션을 참조하세요.

IPAM에서 풀은 연속 IP 주소 범위(또는 CIDR)의 모음입니다. 풀을 사용하면 라우팅 및 보안 요구 사항에 따라 IP 주소를 구성할 수 있습니다. IPAM 리전 이외의 AWS 리전에 대한 풀을 생성할 수 있습니다. 예를 들어 개발 및 프로덕션 애플리케이션에 별도의 라우팅 및 보안 요구 사항이 있는 경우 각각에 대한 풀을 생성할 수 있습니다.

이 섹션의 첫 번째 단계에서는 최상위 풀을 만듭니다. 그런 다음 최상위 풀 내에 리전 풀을 생성합니다. 리전 풀 내에서 필요에 따라 프로덕션 풀 및 개발 환경 풀과 같은 추가 풀을 생성할 수 있습니다. 기본적으로 최대 깊이 10까지의 풀을 생성할 수 있습니다. IPAM 할당량에 대한 자세한 내용은 [IPAM의 할당량](#) 섹션을 참조하세요.

Note

프로비저닝 및 할당 용어가 이 사용 설명서 및 IPAM 콘솔 전체에서 사용됩니다. 프로비저닝은 IPAM 풀에 CIDR을 추가할 때 사용됩니다. 할당은 IPAM 풀의 CIDR을 리소스와 연결할 때 사용됩니다.

다음은 이 섹션의 단계를 완료하면 생성할 수 있는 풀 구조의 계층에 대한 예입니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 프라이빗 범위
 - 최상위 풀
 - AWS 리전 1의 리전 풀
 - 개발 풀
 - VPC 대한 할당

이 구조는 IPAM을 사용할 수 있는 방법의 예로 사용되지만 IPAM을 사용하여 조직의 요구 사항에 맞출 수 있습니다. 모범 사례에 대한 자세한 내용은 [Amazon VPC IP 주소 관리자 모범 사례](#)를 참조하세요.

단일 IPAM 풀을 생성하는 경우 [최상위 IPv4 풀 생성](#)의 단계를 완료한 다음, [CIDR 할당](#) 섹션으로 이동합니다.

내용

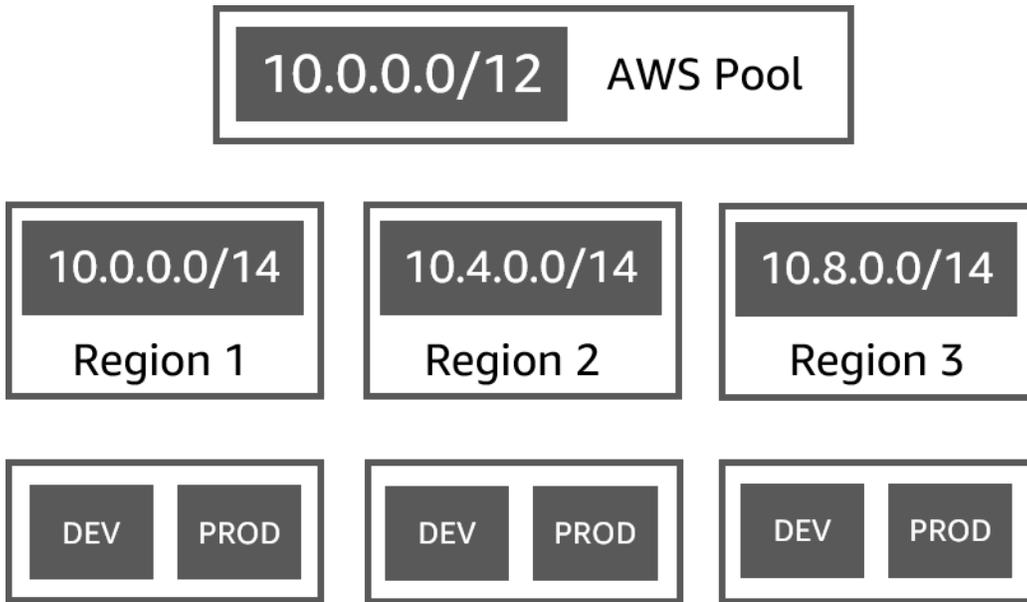
- [IPAM 풀 계획의 예](#)
- [IPv4 풀 생성](#)
- [IPv6 풀 생성](#)

IPAM 풀 계획의 예

IPAM을 사용하여 조직의 필요를 충족할 수 있습니다. 이 섹션에서는 IP 주소를 구성하는 방법에 대한 예가 제공됩니다.

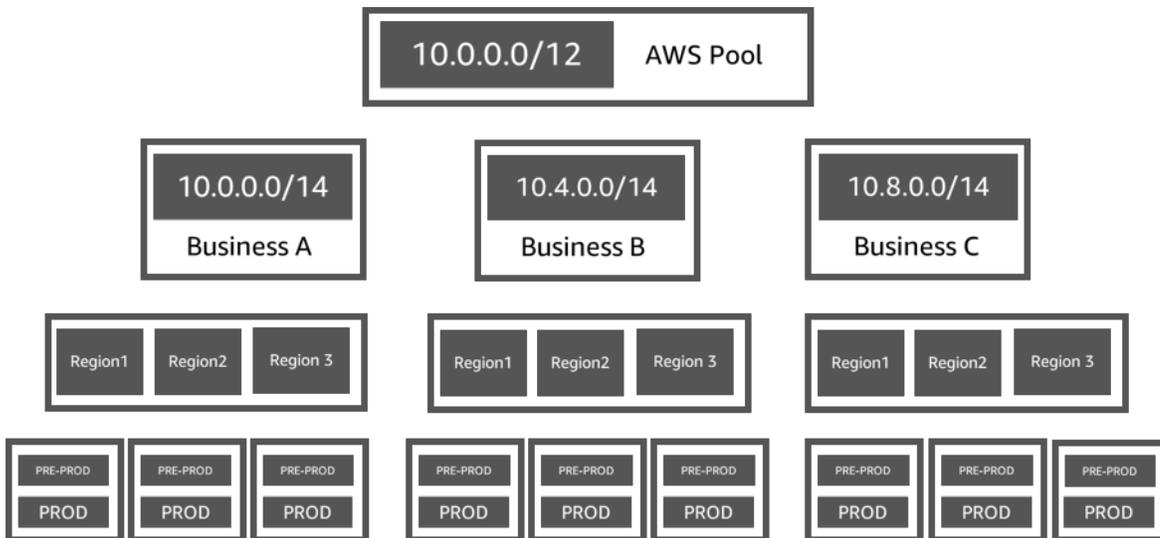
여러 AWS 리전의 IPv4 풀

다음 예는 최상위 풀 내의 여러 AWS 리전에 대한 IPAM 풀 계층을 보여줍니다. 각 AWS 리전 풀에는 IPAM 개발 풀 2개(개발 리소스의 풀 1개와 프로덕션 리소스의 풀 1개)가 있습니다.



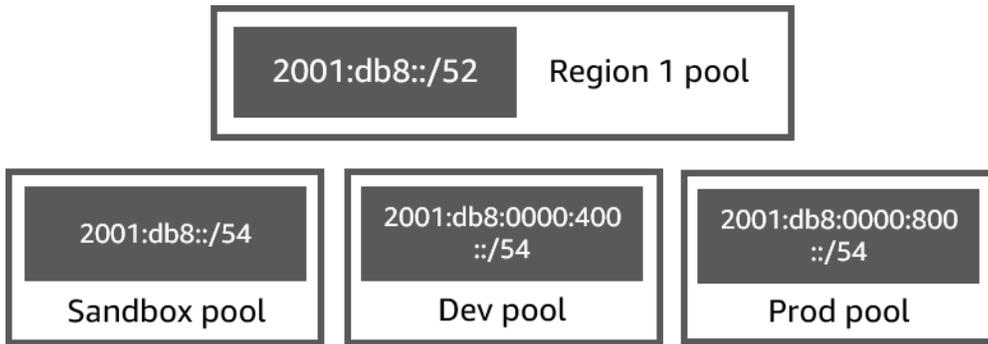
여러 LOB(Line of Business)에 대한 IPv4 풀

다음 예는 최상위 풀 내의 여러 LOB(Line of Business)에 대한 IPAM 풀 계층을 보여줍니다. 각 LOB(Line of Business)의 각 풀에는 3개의 AWS 리전 풀이 포함되어 있습니다. 각 리전 풀에는 IPAM 개발 풀 2개(사전 프로덕션 리소스의 풀 1개와 프로덕션 리소스의 풀 1개)가 있습니다.



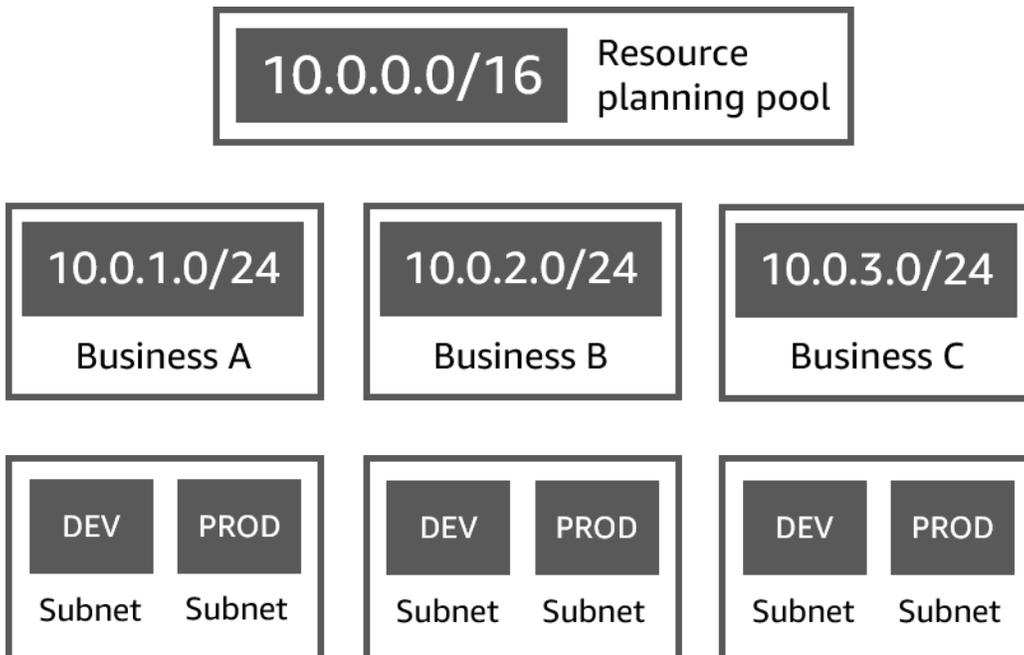
AWS 리전의 IPv6 풀

다음 예는 리전 풀 내의 여러 LOB(Line of Business)에 대한 IPAM IPv6 풀 계층을 보여줍니다. 각 리전 풀에는 IPAM 풀 3개(샌드박스 리소스의 풀 1개, 개발 리소스의 풀 1개, 프로덕션 리소스의 풀 1개)가 있습니다.



여러 LOB(Line of Business)에 대한 서브넷 풀

다음 예에서는 여러 사업 부분과 dev/prod 서브넷 풀에 대한 리소스 계획 풀 계층 구조를 보여줍니다. IPAM을 사용한 서브넷 IP 주소 공간 계획에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.



IPv4 풀 생성

이 섹션의 단계를 따르면 IPv4 IPAM 풀 계층을 생성할 수 있습니다.

다음 예에서는 이 설명서의 지침에 따라 생성할 수 있는 풀 구조의 계층을 보여줍니다. 이 섹션에서는 IPv4 IPAM 풀 계층을 생성합니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 프라이빗 범위

- 최상위 풀(10.0.0.0/8)
 - AWS 리전 2의 리전 풀(10.0.0.0/16)
 - 개발 풀(10.0.0.0/24)
 - VPC에 할당(10.0.0.0/25)

위 예에서 사용된 CIDR은 예에 불과합니다. 최상위 풀 내의 각 풀이 최상위 CIDR의 일부로 프로비저닝됨을 보여줍니다.

내용

- [최상위 IPv4 풀 생성](#)
- [리전 IPv4 풀 생성](#)
- [개발 IPv4 풀 생성](#)

최상위 IPv4 풀 생성

이 섹션의 단계를 따르면 IPv4 최상위 IPAM 풀을 생성할 수 있습니다. 풀을 생성하는 경우 풀이 사용할 CIDR을 프로비저닝합니다. 그런 다음 해당 공간을 할당에 할당합니다. 할당은 IPAM 풀에서 다른 IPAM 풀이나 리소스로 CIDR을 할당하는 것입니다.

다음 예에서는 이 설명서의 지침에 따라 생성할 수 있는 풀 구조의 계층을 보여줍니다. 이 단계에서는 최상위 IPAM 풀을 생성하고 있습니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 프라이빗 범위
 - 최상위 풀(10.0.0.0/8)
 - AWS 리전 1의 리전 풀(10.0.0.0/16)
 - 비프로덕션 VPC의 개발 풀(10.0.0.0/24)
 - VPC에 할당(10.0.0.0/25)

위 예에서 사용된 CIDR은 예에 불과합니다. 최상위 풀 내의 각 풀이 최상위 CIDR의 일부로 프로비저닝됨을 보여줍니다.

IPAM 풀을 생성하는 경우 IPAM 풀 내에서 이뤄지는 할당에 대한 규칙을 구성할 수 있습니다.

할당 규칙을 사용하면 다음을 구성할 수 있습니다.

- IPAM이 이 풀의 CIDR 범위 내에서 CIDR을 발견하는 경우 IPAM이 자동으로 IPAM 풀로 해당 CIDR을 가져와야 하는지 여부
- 풀 내 할당에 필요한 넷마스크 길이
- 풀 내 리소스에 필요한 태그
- 풀 내 리소스에 필요한 로컬 로컬은 IPAM 풀을 할당에 사용할 수 있는 AWS 리전입니다.

할당 규칙은 리소스가 규정을 준수하는지 여부를 결정합니다. 규정 준수에 대한 추가적인 내용은 [리소스별 CIDR 사용량 모니터링](#) 섹션을 참조하세요.

Important

할당 규칙에 표시되지 않는 암시적 규칙이 추가로 있습니다. 리소스가 AWS RAM(Resource Access Manager)의 공유 리소스인 IPAM 풀에 있는 경우 리소스 소유자를 AWS RAM의 보안 주체로 구성해야 합니다. RAM과 풀 공유에 대한 자세한 내용은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요.

다음 예에서는 할당 규칙을 사용하여 IPAM 풀에 대한 액세스를 제어하는 방법을 보여줍니다.

Example

라우팅 및 보안 요구 사항에 따라 풀을 생성하는 경우 특정 리소스만 풀을 사용하도록 허용할 수 있습니다. 이러한 경우 이 풀의 CIDR을 원하는 모든 리소스에 할당 규칙 태그 요구 사항과 일치하는 태그가 있어야 한다는 할당 규칙을 설정할 수 있습니다. 예를 들어 태그 프로덕션이 있는 VPC만 IPAM 풀에서 CIDR을 가져올 수 있는 할당 규칙을 설정할 수 있습니다. 이 풀에서 할당된 CIDR이 /24보다 커서는 안 된다는 할당 규칙을 설정할 수도 있습니다. 이 경우 공간을 사용할 수 있으면 이 풀에서 /24보다 큰 CIDR을 사용하여 리소스를 생성할 수 있습니다. 그러나 이렇게 하면 풀의 할당 규칙을 위반하므로 IPAM은 이 리소스에 비준수라는 플래그를 지정합니다.

Important

이 주제에서는 AWS에서 제공하는 IP 주소 범위를 사용하여 최상위 IPv4 풀을 만드는 방법을 설명합니다. 기존 보유 IPv4 주소 범위를 AWS로 가져오려면(BYOIP) 사전 조건이 있습니다. 자세한 내용은 [자습서: IPAM으로 IP 주소 가져오기](#) 단원을 참조하십시오.

AWS Management Console

풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 풀 생성을 선택합니다.
4. IPAM 범위에서 사용할 프라이빗 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.

기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 프라이빗 범위의 풀은 IPv4 풀이어야 합니다. 퍼블릭 범위의 풀은 IPv4 풀 또는 IPv6 풀일 수 있습니다. 퍼블릭 범위(public scope)는 모든 퍼블릭 공간을 위한 것입니다.

5. (선택 사항) 풀에 대해 이름 태그(Name tag) 및 풀에 대한 자세한 내용을 추가합니다.
6. 소스에서 IPAM 범위를 선택합니다.
7. 주소 패밀리(Address family)에서 IPv4를 선택합니다.
8. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
9. 로캘(Locale)의 경우 없음(None)을 선택합니다. 리전 풀에서 로캘을 설정합니다.

로캘은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를 들어 VPC의 리전과 로캘을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로캘을 선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로캘이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다.

10. (선택 사항) CIDR 없이도 풀을 생성할 수 있지만 CIDR을 프로비저닝하기 전까지는 할당에 대해 풀을 사용할 수 없습니다. CIDR을 프로비저닝하려면 새 CIDR 추가를 선택합니다. 풀에 대해 프로비저닝할 IPv4 CIDR을 입력합니다. 기존 보유 IPv4 또는 IPv6 IP 주소 범위를 AWS로 가져오려면 사전 조건이 있습니다. 자세한 내용은 [자습서: IPAM으로 IP 주소 가져오기](#) 단원을 참조하십시오.
11. 이 풀에 대한 선택적 할당 규칙을 선택합니다.
 - 검색된 리소스 자동으로 가져오기(Automatically import discovered resources): 이 옵션은 로캘(Locale)이 없음(None)으로 설정된 경우 사용할 수 없습니다. 이 옵션을 선택하면 IPAM은 이 풀의 CIDR 범위 내에 있는 리소스를 지속적으로 찾아서 자동으로 IPAM에 할당으로 가져옵니다. 유념할 사항:

- 가져오기가 성공하려면 이러한 리소스에 할당될 CIDR이 아직 다른 리소스에 할당되지 않아야 합니다.
- IPAM은 풀의 할당 규칙 관련 규정 준수 여부에 관계없이 CIDR을 가져오므로 리소스를 가져온 다음 비준수로 표시될 수 있습니다.
- IPAM이 겹치는 여러 CIDR을 검색하는 경우 IPAM은 가장 큰 CIDR만 가져옵니다.
- IPAM이 일치하는 CIDR이 있는 여러 개의 CIDR을 검색하는 경우 IPAM은 그중 하나만 임의로 가져옵니다.

Warning

- IPAM을 생성한 후 VPC를 생성할 때 IPAM에서 할당된 CIDR 블록 옵션을 선택합니다. 선택하지 않으면 VPC에 대해 선택한 CIDR이 IPAM CIDR 할당과 겹칠 수 있습니다.
 - IPAM 풀에 VPC가 이미 할당되어 있는 경우 CIDR이 겹치는 VPC를 자동으로 가져올 수 없습니다. 예를 들어 IPAM 풀에 10.0.0.0/26 CIDR이 할당된 VPC가 있는 경우 10.0.0.0/23 CIDR(10.0.0.0/26 CIDR 를 포함함)이 있는 VPC를 가져올 수 없습니다.
 - 기존 VPC CIDR 할당을 IPAM으로 자동으로 가져오는 데는 다소 시간이 걸립니다.
- **최소 넷마스크 길이(Minimum netmask length):** 준수할 이 IPAM 풀의 CIDR 할당에 필요한 최소 넷마스크 길이 및 풀에서 할당할 수 있는 최대 크기의 CIDR 블록입니다. 최소 넷마스크 길이는 최대 넷마스크 길이보다 작아야 합니다. IPv4 주소에 사용할 수 있는 넷마스크 길이는 0~32입니다. IPv6 주소에 사용할 수 있는 넷마스크 길이는 0~128입니다.
 - **기본 넷마스크 길이(Default netmask length):** 이 풀에 추가된 할당의 기본 넷마스크 길이입니다. 예를 들어 이 풀에 프로비저닝된 CIDR이 **10.0.0.0/8**이고 여기에 **16**를 입력하는 경우 이 풀에 있는 모든 새 할당은 기본적으로 넷마스크 길이가 /16으로 설정됩니다.
 - **최대 넷마스크 길이(Maximum netmask length):** 이 풀의 CIDR 할당에 필요한 최대 넷마스크 길이입니다. 이 값은 풀에서 할당할 수 있는 가장 작은 크기의 CIDR 블록을 지정합니다.
 - **태그 지정 요구 사항(Tagging requirements):** 리소스가 풀에서 공간을 할당하는 데 필요한 태그입니다. 리소스가 공간을 할당한 후 태그를 변경하거나 할당 태그 지정 규칙이 풀에서 변경된 경우 리소스를 비준수로 표시할 수 있습니다.
 - **로캘(Locale):** 이 풀의 CIDR을 사용하는 리소스에 필요한 로캘입니다. 자동으로 가져온 리소스에 이 로캘이 없는 경우 비준수로 표시됩니다. 풀로 자동으로 가져오지 않은 리소스는 이 로캘에 있지 않으면 풀에서 공간을 할당할 수 없습니다.

12. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.

13. 풀 생성을 선택합니다.
14. [리전 IPv4 풀 생성](#) 섹션을 참조하세요.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 IPAM에서 최상위 풀을 생성하거나 편집합니다.

1. 풀 생성: [create-ipam-pool](#)
2. 풀을 생성한 후 편집하여 할당 규칙 수정: [modify-ipam-pool](#).

리전 IPv4 풀 생성

이 섹션의 단계를 따르면 최상위 풀 내에 리전 풀을 생성할 수 있습니다. 최상위 풀만 필요하고 추가적인 리전 및 개발 풀은 필요하지 않은 경우 [CIDR 할당](#) 섹션으로 이동하세요.

Note

풀 생성 프로세스는 퍼블릭 및 프라이빗 범위의 풀에 따라 다릅니다. 이 섹션에는 프라이빗 범위에서 지역 풀을 만드는 단계가 포함되어 있습니다. BYOIP 및 BYOASN 자습서는 [튜토리얼](#)을 참조하십시오.

다음 예에서는 이 설명서의 지침에 따라 생성할 수 있는 풀 구조의 계층을 보여줍니다. 이 단계에서는 리전 IPAM 풀을 생성하고 있습니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 프라이빗 범위
 - 최상위 풀(10.0.0.0/8)
 - AWS 리전 1의 리전 풀(10.0.0.0/16)
 - 비프로덕션 VPC의 개발 풀(10.0.0.0/24)
 - VPC에 할당(10.0.0.0/25)

위 예에서 사용된 CIDR은 예에 불과합니다. 최상위 풀 내의 각 풀이 최상위 CIDR의 일부로 프로비저닝됨을 보여줍니다.

AWS Management Console

최상위 풀 내에 리전 풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 풀 생성을 선택합니다.
4. IPAM 범위에서 최상위 풀을 생성할 때 사용했던 것과 동일한 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
5. (선택 사항) 풀에 대해 이름 태그(Name tag) 및 풀에 대한 자세한 내용을 추가합니다.
6. 소스에서 IPAM 풀을 선택합니다. 그런 다음 이전 섹션에서 생성한 최상위 풀을 선택합니다.
7. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
8. 풀의 로컬을 선택합니다. 로컬을 선택하면 풀 및 풀에서 할당되는 리소스 간에 교차 리전 종속성이 없어집니다. 사용할 수 있는 옵션은 IPAM을 생성할 때 선택한 운영 리전에서 비롯된 것입니다.

로컬은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를 들어 VPC의 리전과 로컬을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로컬을 선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로컬이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다.

 Note

프리 티어에서 풀을 생성하는 경우 IPAM의 홈 리전과 일치하는 로케일만 선택할 수 있습니다. 로케일에서 모든 IPAM 기능을 사용하려면 [고급 티어로 업그레이드](#)하세요.

9. (선택 사항) 풀에 대해 프로비저닝할 CIDR을 선택합니다. CIDR 없이도 풀을 생성할 수 있지만 CIDR을 프로비저닝하기 전까지는 할당에 대해 풀을 사용할 수 없습니다. 풀을 편집하여 언제든지 풀에 CIDR을 추가할 수 있습니다.
10. 최상위 풀을 생성할 때와 동일한 할당 규칙 옵션이 여기에 적용됩니다. 풀을 생성할 때 사용할 수 있는 옵션에 대한 설명은 [최상위 IPv4 풀 생성](#) 섹션을 참조하세요. 리전 풀에 대한 할당 규칙은 최상위 풀에서 상속되지 않습니다. 여기에 규칙을 적용하지 않으면 풀에 대한 설정된 할당 규칙이 없어집니다.
11. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.

12. 풀 구성을 마쳤으면 풀 생성(Create pool)을 선택합니다.
13. [개발 IPv4 풀 생성](#) 섹션을 참조하세요.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 IPAM에서 리전 풀을 생성합니다.

1. [describe-ipam-scopes](#)에서 풀을 생성하려는 범위의 ID를 가져옵니다.
2. [describe-ipam-pools](#)에서 풀을 생성하려는 풀의 ID를 가져옵니다.
3. 풀 생성: [create-ipam-pool](#)
4. 새 풀 보기: [describe-ipam-pools](#)

필요에 따라 최상위 풀 내에 추가 개발 풀을 생성하려면 이러한 단계를 반복합니다.

개발 IPv4 풀 생성

이 섹션의 단계를 따르면 리전 풀 내에 개발 풀을 생성할 수 있습니다. 최상위 풀 및 리전 풀만 필요하고 개발 풀은 필요하지 않은 경우 [CIDR 할당](#) 섹션으로 이동하세요.

다음 예에서는 이 설명서의 지침에 따라 생성할 수 있는 풀 구조의 계층을 보여줍니다. 이 단계에서는 개발 IPAM 풀을 생성하고 있습니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 프라이빗 범위
 - 최상위 풀(10.0.0.0/8)
 - AWS 리전 1의 리전 풀(10.0.0.0/16)
 - 비프로덕션 VPC의 개발 풀(10.0.0.0/24)
 - VPC에 할당(10.0.1.0/25)

위 예에서 사용된 CIDR은 예에 불과합니다. 최상위 풀 내의 각 풀이 최상위 CIDR의 일부로 프로비저닝됨을 보여줍니다.

AWS Management Console

리전 풀 내에 개발 풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 풀 생성을 선택합니다.
4. IPAM 범위에서 최상위 및 리전 풀을 생성할 때 사용했던 것과 동일한 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
5. (선택 사항) 풀에 대해 이름 태그(Name tag) 및 풀에 대한 자세한 내용을 추가합니다.
6. 소스에서 IPAM 풀을 선택합니다. 그런 다음 리전 풀을 선택합니다.
7. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 듭니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
8. (선택 사항) 풀에 대해 프로비저닝할 CIDR을 선택합니다. 최상위 풀에 프로비저닝된 CIDR만 프로비저닝할 수 있습니다. CIDR 없이도 풀을 생성할 수 있지만 CIDR을 프로비저닝하기 전까지는 할당에 대해 풀을 사용할 수 없습니다. 풀을 편집하여 언제든지 풀에 CIDR을 추가할 수 있습니다.
9. 최상위 풀 및 리전 풀을 생성할 때와 동일한 할당 규칙 옵션이 여기에 적용됩니다. 풀을 생성할 때 사용할 수 있는 옵션에 대한 설명은 [최상위 IPv4 풀 생성](#) 섹션을 참조하세요. 풀에 대한 할당 규칙은 계층에서 상위에 있는 풀에서 상속되지 않습니다. 여기에 규칙을 적용하지 않으면 풀에 대한 할당 규칙이 설정되지 않습니다.
10. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.
11. 풀 구성을 마쳤으면 풀 생성(Create pool)을 선택합니다.
12. [CIDR 할당](#) 섹션을 참조하세요.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 IPAM에서 리전 풀을 생성합니다.

1. [describe-ipam-scopes](#)에서 풀을 생성하려는 범위의 ID를 가져옵니다.
2. [describe-ipam-pools](#)에서 풀을 생성하려는 풀의 ID를 가져옵니다.

3. 풀 생성: [create-ipam-pool](#)
4. 새 풀 보기: [describe-ipam-pools](#)

필요에 따라 리전 풀 내에 추가 개발 풀을 생성하려면 이 단계를 반복합니다.

IPv6 풀 생성

이 섹션의 단계를 따르면 IPAM IPv6 풀 계층을 생성할 수 있습니다. 풀을 생성하는 경우 풀이 사용할 CIDR을 프로비저닝할 수 있습니다. 풀은 해당 CIDR 내의 공간을 풀 내 할당에 할당합니다. 할당은 IPAM 풀에서 다른 리소스 또는 IPAM 풀로 CIDR을 할당하는 것입니다.

다음 예에서는 이 설명서의 지침에 따라 생성할 수 있는 풀 구조의 계층을 보여줍니다. 이 섹션에서는 IPv6 IPAM 풀 계층을 생성합니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 퍼블릭 범위
 - AWS 리전 1의 리전 풀(2001:db8::/52)
 - 개발 풀(2001:db8::/54)
 - VPC에 할당(2001:db8::/56)

내용

- [리전 IPv6 풀 생성](#)
- [개발 IPv6 풀 생성](#)

리전 IPv6 풀 생성

이 섹션의 단계를 따르면 IPv6 리전 IPAM 풀을 생성할 수 있습니다. Amazon에서 제공한 IPv6 CIDR 블록을 풀에 프로비저닝할 때는 로컬(AWS 리전)을 선택한 상태로 풀에 프로비저닝해야 합니다. 풀을 생성하는 경우 풀이 사용할 CIDR을 프로비저닝하거나 나중에 추가할 수 있습니다. 그런 다음 해당 공간을 할당에 할당합니다. 할당은 IPAM 풀에서 다른 IPAM 풀이나 리소스로 CIDR을 할당하는 것입니다.

다음 예에서는 이 설명서의 지침에 따라 생성할 수 있는 풀 구조의 계층을 보여줍니다. 이 단계에서는 IPv6 리전 IPAM 풀을 생성합니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 퍼블릭 범위

- AWS 리전 1의 리전 풀(2001:db8::/52)
- 개발 풀(2001:db8::/54)
 - VPC에 할당(2001:db8::/56)

위 예에서 사용된 CIDR은 예에 불과합니다. IPv6 리전 풀 내의 각 풀이 IPv6 리전 CIDR의 일부로 프로 비저닝됨을 보여줍니다.

IPAM 풀을 생성하는 경우 IPAM 풀 내에서 이뤄지는 할당에 대한 규칙을 구성할 수 있습니다.

할당 규칙을 사용하면 다음을 구성할 수 있습니다.

- 풀 내 할당에 필요한 넷마스크 길이
- 풀 내 리소스에 필요한 태그
- 풀 내 리소스에 필요한 로컬 로컬은 IPAM 풀을 할당에 사용할 수 있는 AWS 리전입니다.

할당 규칙은 리소스가 규정을 준수하는지 여부를 결정합니다. 규정 준수에 대한 추가적인 내용은 [리소 스별 CIDR 사용량 모니터링](#) 섹션을 참조하세요.

Important

할당 규칙에 표시되지 않는 암시적 규칙이 추가로 있습니다. 리소스가 AWS RAM(Resource Access Manager)의 공유 리소스인 IPAM 풀에 있는 경우 리소스 소유자를 AWS RAM의 보안 주체로 구성해야 합니다. RAM과 풀 공유에 대한 자세한 내용은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요.

다음 예에서는 할당 규칙을 사용하여 IPAM 풀에 대한 액세스를 제어하는 방법을 보여줍니다.

Example

라우팅 및 보안 요구 사항에 따라 풀을 생성하는 경우 특정 리소스만 풀을 사용하도록 허용할 수 있습 니다. 이러한 경우 이 풀의 CIDR을 원하는 모든 리소스에 할당 규칙 태그 요구 사항과 일치하는 태그가 있어야 한다는 할당 규칙을 설정할 수 있습니다. 예를 들어 태그 프로덕션이 있는 VPC만 IPAM 풀에서 CIDR을 가져올 수 있는 할당 규칙을 설정할 수 있습니다.

⚠ Important

이 주제에서는 AWS에서 제공하는 IP 주소 범위 중 하나를 사용하여 IPv6 리전 풀을 만드는 방법을 설명합니다. 기존 보유 IPv4 또는 IPv6 IP 주소 범위(BYOIP)를 AWS로 가져오려면 사전 조건이 있습니다. 자세한 내용은 [자습서: IPAM으로 IP 주소 가져오기](#) 단원을 참조하십시오.

AWS Management Console

풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 풀 생성을 선택합니다.
4. IPAM 범위에서 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.

기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 프라이빗 범위의 풀은 IPv4 풀이어야 합니다. 퍼블릭 범위의 풀은 IPv4 풀 또는 IPv6 풀일 수 있습니다. 퍼블릭 범위는 AWS가 인터넷에 광고할 수 있거나 현재 광고하고 있는 모든 공간이 대상입니다.

5. (선택 사항) 풀에 대해 이름 태그(Name tag) 및 풀에 대한 자세한 내용을 추가합니다.
6. 소스에서 IPAM 범위를 선택합니다.
7. 주소 패밀리에서 IPv6를 선택합니다. 풀의 CIDR을 공개적으로 광고 가능하도록 허용 토글이 나타납니다. 기본으로 이 풀의 모든 CIDR은 공개적으로 광고될 수 있습니다. 이 옵션은 활성화하거나 비활성화할 수 없습니다.
8. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
9. 풀의 로컬을 선택합니다. Amazon에서 제공한 IPv6 CIDR 블록을 풀에 프로비저닝할 때는 로컬(AWS 리전)을 선택한 상태로 풀에 프로비저닝해야 합니다. 로컬을 선택하면 풀 및 풀에서 할당되는 리소스 간에 교차 리전 종속성이 없어집니다. 사용할 수 있는 옵션은 IPAM을 생성할 때 선택한 운영 리전에서 비롯된 것입니다. 언제든지 운영 리전을 추가할 수 있습니다.

로컬은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를 들어 VPC의 리전과 로컬을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로컬을

선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로케일이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다.

Note

프리 티어에서 풀을 생성하는 경우 IPAM의 홈 리전과 일치하는 로케일만 선택할 수 있습니다. 로케일에서 모든 IPAM 기능을 사용하려면 [고급 티어로 업그레이드](#)하세요.

10. 서비스(Service)에서 EC2(EIP/VPC)를 선택합니다. 선택한 서비스에 따라 CIDR이 알릴 AWS 서비스가 결정됩니다. 현재, 유일한 옵션은 EC2(EIP/VPC)입니다. 즉, 이 풀에서 할당된 CIDR은 Amazon EC2 서비스(탄력적 IP 주소용) 및 Amazon VPC 서비스(VPC에 연결된 CIDR용)에 대해 알릴 수 있음을 의미합니다.
11. 퍼블릭 IP 소스 옵션에서 Amazon 소유를 선택하여 AWS가 풀에 대한 IPv6 주소 범위를 제공하도록 합니다. 이 페이지 상단에서 설명한 것처럼 이 주제에서는 AWS에서 제공하는 IP 주소 범위로 IPv6 리전 풀을 만드는 방법을 설명합니다. 기존 보유 IPv4 또는 IPv6 주소 범위를 AWS로 가져오려면(BYOIP) 사전 조건이 있습니다. 자세한 내용은 [자습서: IPAM으로 IP 주소 가져오기](#) 단원을 참조하십시오.
12. 퍼블릭 IP 소스 BYOIP를 사용하는 퍼블릭 범위의 풀의 경우 이 풀의 CIDR을 공개적으로 광고할 수 있도록 허용을 사용하여 AWS가 이 풀의 CIDR을 공개적으로 광고할 수 있는지 여부를 제어할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다. AWS가 이 풀에서 CIDR을 공개적으로 광고하는 것을 허용하지 않으려면 이 옵션을 비활성화하세요.
13. (선택 사항) CIDR 없이도 풀을 생성할 수 있지만 CIDR을 프로비저닝하기 전까지는 할당에 대해 풀을 사용할 수 없습니다. CIDR을 프로비저닝하려면 Amazon 소유 CIDR 추가를 선택하고 CIDR의 넷마스크 크기를 /40 ~ /52 사이에서 선택합니다.

Note

유념할 사항:

- 기본적으로 Amazon 제공 IPv6 CIDR 블록을 리전 풀에 추가할 수 있습니다. 기본 제한 증가에 대한 자세한 내용은 [IPAM의 할당량](#)을 참조하세요.
- 드롭다운 메뉴에서 넷마스크 길이를 선택하면 넷마스크 길이와 넷마스크가 나타내는 /56 CIDR 수가 표시됩니다.

14. 이 풀에 대한 선택적 할당 규칙을 선택합니다.

- **최소 넷마스크 길이(Minimum netmask length):** 준수할 이 IPAM 풀의 CIDR 할당에 필요한 최소 넷마스크 길이 및 풀에서 할당할 수 있는 최대 크기의 CIDR 블록입니다. 최소 넷마스크 길이는 최대 넷마스크 길이보다 작아야 합니다. IPv6 주소에 사용할 수 있는 넷마스크 길이는 0~128입니다.
- **기본 넷마스크 길이(Default netmask length):** 이 풀에 추가된 할당의 기본 넷마스크 길이입니다. 예를 들어 이 풀에 프로비저닝된 CIDR이 `2001:db8::/52`이고 여기에 56을 입력하는 경우 이 풀에 있는 모든 새 할당은 기본적으로 넷마스크 길이가 /56으로 설정됩니다.
- **최대 넷마스크 길이(Maximum netmask length):** 이 풀의 CIDR 할당에 필요한 최대 넷마스크 길이입니다. 이 값은 풀에서 할당할 수 있는 가장 작은 크기의 CIDR 블록을 지정합니다. 예를 들어 여기에 /56을 입력하면 이 풀의 CIDR에 할당할 수 있는 최소 넷마스크 길이는 /56입니다.
- **태그 지정 요구 사항(Tagging requirements):** 리소스가 풀에서 공간을 할당하는 데 필요한 태그입니다. 리소스가 공간을 할당한 후 태그를 변경하거나 할당 태그 지정 규칙이 풀에서 변경된 경우 리소스를 비준수로 표시할 수 있습니다.
- **로캘(Locale):** 이 풀의 CIDR을 사용하는 리소스에 필요한 로캘입니다. 자동으로 가져온 리소스에 이 로캘이 없는 경우 비준수로 표시됩니다. 풀로 자동으로 가져오지 않은 리소스는 이 로캘에 있지 않으면 풀에서 공간을 할당할 수 없습니다.

15. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.

16. 풀 생성을 선택합니다.

17. [개발 IPv6 풀 생성](#) 섹션을 참조하세요.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 IPAM에서 IPv6 리전 풀을 생성합니다.

1. 풀 생성: [create-ipam-pool](#)
2. 풀을 생성한 후 편집하여 할당 규칙 수정: [modify-ipam-pool](#).

개발 IPv6 풀 생성

이 섹션의 단계를 따르면 IPv6 리전 풀 내에 개발 풀을 생성할 수 있습니다. 리전 풀만 필요하고 개발 풀은 필요하지 않은 경우 [CIDR 할당](#)으로 건너뛰세요.

다음 예에서는 이 설명서의 지침에 따라 생성할 수 있는 풀 구조의 계층을 보여줍니다. 이 단계에서는 개발 IPAM 풀을 생성하고 있습니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM
 - 퍼블릭 범위
 - AWS 리전 1의 리전 풀(2001:db8::/52)
 - 개발 풀(2001:db8::/54)
 - VPC에 할당(2001:db8::/56)

위 예에서 사용된 CIDR은 예에 불과합니다. 최상위 풀 내의 각 풀이 최상위 CIDR의 일부로 프로비저닝됨을 보여줍니다.

AWS Management Console

IPv6 리전 풀 내에 개발 풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 풀 생성을 선택합니다.
4. IPAM 범위에서 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.

기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 프라이빗 범위의 풀은 IPv4 풀이어야 합니다. 퍼블릭 범위의 풀은 IPv4 풀 또는 IPv6 풀일 수 있습니다. 퍼블릭 범위는 AWS가 인터넷에 광고할 수 있거나 현재 광고하고 있는 모든 공간이 대상입니다.

5. (선택 사항) 풀에 대해 이름 태그(Name tag) 및 풀에 대한 자세한 내용을 추가합니다.
6. 소스에서 IPAM 풀을 선택합니다. 그런 다음 소스 풀에서 IPv6 리전 풀을 선택합니다.
7. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
8. (선택 사항) 풀에 대해 프로비저닝할 CIDR을 선택합니다. 최상위 풀에 프로비저닝된 CIDR만 프로비저닝할 수 있습니다. CIDR 없이도 풀을 생성할 수 있지만 CIDR을 프로비저닝하기 전까지는 할당에 대해 풀을 사용할 수 없습니다. 풀을 편집하여 언제든지 풀에 CIDR을 추가할 수 있습니다.

9. IPv6 리전 풀을 생성할 때와 동일한 할당 규칙 옵션이 여기에 적용됩니다. 풀을 생성할 때 사용할 수 있는 옵션에 대한 설명은 [리전 IPv6 풀 생성](#) 섹션을 참조하세요. 풀에 대한 할당 규칙은 계층에서 상위에 있는 풀에서 상속되지 않습니다. 여기에 규칙을 적용하지 않으면 풀에 대한 할당 규칙이 설정되지 않습니다.
10. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.
11. 풀 구성을 마쳤으면 풀 생성(Create pool)을 선택합니다.
12. [CIDR 할당](#) 섹션을 참조하세요.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 IPv6 IPAM에서 리전 풀을 생성합니다.

1. [describe-ipam-scopes](#)에서 풀을 생성하려는 범위의 ID를 가져옵니다.
2. [describe-ipam-pools](#)에서 풀을 생성하려는 풀의 ID를 가져옵니다.
3. 풀 생성: [create-ipam-pool](#)
4. 새 풀 보기: [describe-ipam-pools](#)

필요에 따라 IPv6 리전 풀 내에 추가 개발 풀을 생성하려면 이 단계를 반복합니다.

CIDR 할당

이번 섹션의 단계를 따르면 IPAM 풀의 CIDR을 리소스에 할당할 수 있습니다.

Note

프로비전 및 할당 용어가 이 사용 설명서 및 IPAM 콘솔 전체에서 사용됩니다. 프로비저닝은 IPAM 풀에 CIDR을 추가할 때 사용됩니다. 할당은 IPAM 풀의 CIDR을 리소스와 연결할 때 사용됩니다.

다음과 같은 방법으로 IPAM 풀의 CIDR을 할당할 수 있습니다.

- Amazon VPC와 같은 IPAM과 통합된 AWS 서비스를 사용하고 CIDR에 대해 IPAM 풀을 사용하는 옵션을 선택합니다. IPAM은 자동으로 풀에서 할당을 생성합니다.

- IPAM 풀 내에서 CIDR을 수동으로 할당하여 Amazon VPC와 같은 IPAM과 통합된 AWS 서비스를 통해 나중에 사용할 수 있도록 예약합니다.

이 섹션에서는 IPAM과 통합된 AWS 서비스를 사용하여 IPAM 풀 CIDR을 프로비저닝하는 방법 및 IP 주소 공간을 수동으로 예약하는 방법의 두 옵션을 모두 살펴보겠습니다.

내용

- [IPAM 풀 CIDR을 사용하는 VPC 생성](#)
- [CIDR을 풀에 수동으로 할당하여 IP 주소 공간을 예약합니다.](#)

IPAM 풀 CIDR을 사용하는 VPC 생성

Amazon VPC 사용 설명서의 [VPC 생성](#) 단계를 따르세요. VPC 대한 CIDR을 선택하는 단계를 완료하면 IPAM 풀의 CIDR을 사용할 수 있는 옵션이 제공됩니다.

VPC 생성할 때 IPAM 풀을 사용하는 옵션을 선택한 경우 AWS는 IPAM 풀에서 CIDR을 할당합니다. IPAM 콘솔의 콘텐츠 창에서 풀을 선택하고 풀의 리소스 탭을 보면 IPAM에서 할당을 확인할 수 있습니다.

Note

VPC 생성을 포함하여 AWS CLI를 사용하는 전체 지침은 [Amazon VPC IP Address Manager 자습서](#) 섹션을 참조하세요.

CIDR을 풀에 수동으로 할당하여 IP 주소 공간을 예약합니다.

이번 섹션의 단계를 따르면 CIDR을 풀에 수동으로 할당할 수 있습니다. 나중에 사용할 수 있도록 IPAM 풀 내에서 CIDR을 예약하려면 이 작업을 수행해야 합니다. 또한 IPAM 풀에 공간을 예약하여 온프레미스 네트워크를 나타낼 수 있습니다. IPAM은 해당 예약을 관리하며, CIDR이 온프레미스 IP 공간과 겹치는지 여부를 표시합니다.

AWS Management Console

CIDR을 수동으로 할당하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.

3. 기본적으로 기본 프라이빗 범위가 선택되어 있습니다. 기본 개인 범위를 사용하지 않으려는 경우 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 콘텐츠 창에서 풀을 선택합니다.
5. 작업(Actions) > 사용자 지정 할당 생성(Create custom allocation)을 선택합니다.
6. 할당할 특정 CIDR을 추가할지(예: IPv4의 경우 10.0.0.0/24, IPv6의 경우 2001:db8::/52), 넷마스크 길이만 선택하여 크기별로 CIDR을 추가할지(예: IPv4의 경우 /24, IPv6의 경우 /52) 선택합니다.
7. 할당(Allocate)을 선택합니다.
8. 탐색 창에서 풀(Pools)을 선택하고 풀에 대한 할당(Allocations) 탭을 보면 IPAM에서 할당을 확인할 수 있습니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 수동으로 CIDR을 풀에 할당합니다.

1. [describe-ipam-pools](#)에서 할당을 생성하고자 하는 IPAM 풀의 ID를 가져옵니다.
2. 할당 생성: [allocate-ipam-pool-cidr](#).
3. 할당 보기: [get-ipam-pool-allocations](#).

수동으로 할당된 CIDR을 릴리스하려면 [할당 해제](#) 섹션을 참조하세요.

IPAM에서 IP 주소 공간 관리

이 섹션의 작업은 선택 사항입니다. 이 섹션의 작업을 완료하고 IPAM 계정을 위임한 경우에는 IPAM 관리자가 작업을 완료해야 합니다.

IPAM에서 IP 주소 공간을 관리하려면 이 섹션의 단계를 따르세요.

내용

- [VPC 생성에 IPAM 사용 적용](#)
- [AWS RAM을 사용하여 IPAM 풀 공유](#)
- [풀에 CIDR 프로비저닝](#)
- [풀에서 CIDR 프로비저닝 해제](#)
- [풀 편집](#)
- [풀 삭제](#)
- [리소스 검색 작업](#)
- [추가 범위 생성](#)
- [범위 간에 VPC CIDR 이동](#)
- [VPC CIDR의 모니터링 상태 변경](#)
- [범위 삭제](#)
- [할당 해제](#)
- [IPAM 수정](#)
- [IPAM 삭제](#)

VPC 생성에 IPAM 사용 적용

Note

이 섹션은 IPAM이 AWS Organizations를 통합하도록 설정한 경우에만 적용할 수 있습니다. 자세한 내용은 [AWS Organization에서 계정과 IPAM 통합](#) 단원을 참조하십시오.

이 섹션에서는 AWS Organizations에서 조직의 구성원이 VPC를 생성할 때 IPAM을 사용하도록 요구하는 서비스 제어 정책을 생성하는 방법을 설명합니다. 서비스 제어 정책(SCP)은 조직의 권한을 관리하

도록 하는 조직의 정책 유형입니다. 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책을 참조](#)하세요.

VPC를 생성할 때 IPAM 적용

이 섹션의 단계에 따라 조직의 구성원이 VPC를 생성할 때 IPAM을 사용하도록 요구합니다.

SCP를 생성하고 VPC 생성을 IPAM으로 제한하려면

1. AWS Organizations 사용 설명서의 [SCP 생성](#)에서 설명하는 단계를 따르고 JSON 편집기에 다음 텍스트를 입력합니다.

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

2. 조직의 하나 이상의 조직 단위에 정책을 연결합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책 연결 및 분리](#)를 참조하십시오.

VPC를 생성할 때 IPAM 풀 적용

이 섹션의 단계에 따라 조직의 구성원이 VPC를 생성할 때 특정 IPAM 풀을 사용하도록 요구합니다.

SCP를 생성하고 VPC 생성을 IPAM 풀로 제한하려면

1. AWS Organizations 사용 설명서의 [SCP 생성](#)에서 설명하는 단계를 따르고 JSON 편집기에 다음 텍스트를 입력합니다.

```
{
  "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. ipam-pool-0123456789abcdefg 예의 값을 사용자를 제한하려는 IPv4 풀 ID로 변경합니다.
3. 조직의 하나 이상의 조직 단위에 정책을 연결합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책 연결 및 분리](#)를 참조하십시오.

지정된 OU 목록을 제외한 모든 OU에 IPAM 적용

이 섹션의 단계에 따라 지정된 조직 단위(OU) 목록을 제외한 모든 OU에 IPAM을 적용하세요. 이 섹션에서 설명하는 정책을 수행하려면 aws:PrincipalOrgPaths에서 지정한 OU를 제외한 조직 내 OU가 IPAM을 사용하여 VPC를 생성하고 확장해야 합니다. 나열된 OU는 VPC를 생성할 때 IPAM을 사용하거나 IP 주소 범위를 수동으로 지정할 수 있습니다.

SCP 생성 및 지정된 OU 목록을 제외한 모든 OU에 IPAM 적용

1. AWS Organizations 사용 설명서의 [SCP 생성](#)에서 설명하는 단계를 따르고 JSON 편집기에 다음 텍스트를 입력합니다.

```

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

```

```

    ]
  }
}
}]
}

```

- 예제 값(예: o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/)을 제거하고, IPAM을 사용하는 옵션(필수는 아님)을 원하는 OU의 AWS Organizations 엔터티 경로를 추가합니다. 엔터티 경로에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [AWS Organizations 엔터티 경로 이해](#)와 [aws:PrincipalOrgPaths](#)를 참조하세요.
- 정책을 조직 루트에 연결합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책 연결 및 분리](#)를 참조하십시오.

AWS RAM을 사용하여 IPAM 풀 공유

이 섹션의 단계에 따라 AWS RAM(Resource Access Manager)을 사용하여 IPAM 풀을 공유합니다. RAM과 IPAM 풀을 공유하는 경우 “보안 주체”는 풀의 CIDR을 해당 계정에서 AWS 리소스(예: VPC)에 할당할 수 있습니다. 보안 주체란 AWS 계정, IAM 역할 또는 AWS Organizations의 조직 단위를 뜻하는 RAM의 개념입니다. 자세한 내용은 AWS RAM 사용 설명서의 [AWS 리소스 공유](#)를 참조하세요.

Note

- IPAM을 AWS Organizations와 통합한 경우 AWS RAM과 IPAM 풀만 공유할 수 있습니다. 자세한 내용은 [AWS Organization에서 계정과 IPAM 통합](#) 단원을 참조하십시오. 단일 계정 IPAM 사용자인 경우 IPAM 풀을 AWS RAM과 공유할 수 없습니다.
- AWS RAM에서 AWS Organizations와의 리소스 공유를 사용 설정해야 합니다. 자세한 내용은 AWS RAM 사용 설명서의 [내 리소스 공유 활성화AWS Organizations](#)를 참조하세요.
- RAM 공유는 IPAM의 홈 AWS 리전에서만 사용할 수 있습니다. IPAM 풀의 리전이 아닌 IPAM이 있는 AWS 리전에서 공유를 생성해야 합니다.
- IPAM 풀 리소스 공유를 생성 및 삭제하는 계정에는 해당 IAM 역할에 연결된 IAM 정책에 다음과 같은 권한이 있어야 합니다.
 - ec2:PutResourcePolicy
 - ec2>DeleteResourcePolicy
- RAM 공유에 여러 IPAM 풀을 추가할 수 있습니다.

AWS Management Console

RAM을 사용하여 IPAM 풀을 공유하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 기본 프라이빗 범위가 선택되어 있습니다. 기본 개인 범위를 사용하지 않으려는 경우 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 콘텐츠 창에서 공유하려는 풀을 선택한 다음, 작업(Actions) > 세부 정보 보기(View details)를 선택합니다.
5. 리소스 공유(Resource sharing)에서 리소스 공유 생성(Create resource share)을 선택합니다. 그러면 AWS RAM 콘솔이 열립니다. AWS RAM에서 공유 풀을 생성합니다.
6. 리소스 공유 생성(Create a resource share)을 선택합니다.
7. 공유 리소스에 이름을 추가합니다.
8. 리소스 유형 선택(Select resource type)에서 IPAM 풀을 선택하고 하나 이상의 IPAM 풀을 선택합니다.
9. 다음(Next)을 선택합니다.
10. 리소스 공유에 대한 권한 중 하나를 선택합니다.
 - `AWSRAMDefaultPermissionsIpamPool`: 이 권한을 선택하여 보안 주체가 공유 IPAM 풀에서 CIDR 및 할당을 확인하고 풀에서 CIDR을 할당/해제할 수 있도록 합니다.
 - `AWSRAMPermissionIpamPoolByoipCidrImport`: 이 권한을 선택하여 보안 주체가 BYOIP CIDR을 공유 IPAM 풀로 가져올 수 있도록 합니다. 기존 BYOIP CIDR이 있고 이를 IPAM으로 가져와 보안 주체와 공유하려는 경우에만 이 권한이 필요합니다. IPAM에 대한 BYOIP CIDR의 자세한 정보는 [자습서: IPAM으로 BYOIP IPv4 CIDR 전송](#) 섹션을 참조하세요.
11. 이 리소스에 액세스할 수 있는 보안 주체를 선택합니다. 보안 주체가 기존 BYOIP CIDR을 이 공유 IPAM 풀로 가져올 경우 BYOIP CIDR 소유자 계정을 보안 주체로 추가합니다.
12. 리소스 공유 옵션 및 공유할 보안 주체를 검토하고 생성(Create)을 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 여기에서 볼 수 있습니다.

RAM을 사용하여 IPAM 풀을 공유하려면 다음 AWS CLI 명령을 사용합니다.

1. IPAM의 ARN 가져오기: [describe-ipam-pools](#)
2. 리소스 공유 생성: [create-resource-share](#)
3. 리소스 공유 확인: [get-resource-shares](#)

RAM에서 리소스 공유를 만든 결과로 다른 보안 주체는 이제 IPAM 풀을 사용하여 리소스에 CIDR을 할당할 수 있습니다. 보안 주체가 생성한 리소스 모니터링에 대한 자세한 내용은 [리소스별 CIDR 사용량 모니터링](#) 섹션을 참조하세요. VPC를 생성하고 공유 IPAM 풀의 CIDR을 할당하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 생성](#)을 참조하세요.

풀에 CIDR 프로비저닝

이 섹션의 단계를 따르면 풀에 CIDR을 프로비저닝할 수 있습니다. 풀을 만들 때 CIDR을 이미 프로비저닝한 경우 풀이 할당을 거의 완료한 경우 추가 CIDR을 프로비저닝해야 할 수 있습니다. 풀 사용량을 모니터링하려면 [IPAM 대시보드를 사용하여 CIDR 사용량 모니터링](#) 섹션을 참조하세요.

Note

프로비저닝 및 할당 용어가 이 사용 설명서 및 IPAM 콘솔 전체에서 사용됩니다. 프로비저닝은 IPAM 풀에 CIDR을 추가할 때 사용됩니다. 할당은 IPAM 풀의 CIDR을 VPC 또는 탄력적 IP 주소와 연결할 때 사용됩니다.

AWS Management Console

풀에 CIDR을 프로비저닝하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 기본 프라이빗 범위가 선택되어 있습니다. 기본 개인 범위를 사용하지 않으려는 경우 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 콘텐츠 창에서 CIDR을 추가하려는 풀을 선택합니다.
5. 작업(Actions) > CIDR 프로비저닝(Provision CIDRs)을 선택합니다.
6. 추가하려는 CIDR을 입력한 다음 추가 CIDR에 대해 새 CIDR 추가(Add new CIDR)를 선택합니다.

Note

- 기본적으로 Amazon 제공 IPv6 CIDR 블록을 리전 풀에 추가할 수 있습니다. 기본 제한 증가에 대한 자세한 내용은 [IPAM의 할당량](#)을 참조하세요.
- 프로비저닝하려는 CIDR은 범위 내에서 사용할 수 있어야 합니다.
- 풀 내에서 풀에 CIDR을 프로비저닝하는 경우 프로비저닝할 CIDR 공간을 풀에서 사용할 수 있어야 합니다.

7. 프로비저닝 요청(Request provisioning)을 선택합니다.
8. 탐색 창에서 풀(Pools)을 선택하고, 풀에 대한 CIDR 탭을 보면 IPAM에서 CIDR을 확인할 수 있습니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 풀에 CIDR을 프로비저닝합니다.

1. IPAM 풀 ID 가져오기: [describe-ipam-pools](#)
2. 풀에 프로비저닝된 CIDR 가져오기: [get-ipam-pool-cidrs](#)
3. 풀에 새 CIDR 프로비저닝: [provision-ipam-pool-cidr](#)
4. 풀에 프로비저닝된 CIDR 가져오기 및 새 CIDR 보기: [get-ipam-pool-cidrs](#)

풀에서 CIDR 프로비저닝 해제

이 섹션의 단계를 따르면 IPAM 풀의 CIDR을 프로비저닝 해제할 수 있습니다. 모든 풀 CIDR을 프로비저닝 해제하면 풀을 할당에 더 이상 사용할 수 없습니다. 할당에 풀을 사용하려면 먼저 풀에 새 CIDR을 프로비저닝해야 합니다.

Important

풀에 할당이 있는 경우 CIDR을 프로비저닝 해제할 수 없습니다. 할당을 제거하려면 [할당 해제](#) 섹션을 참조하세요.

AWS Management Console

풀 CIDR을 프로비저닝 해제하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 콘텐츠 창에서 프로비저닝 해제하려는 CIDR이 있는 풀을 선택합니다.
5. CIDR 탭을 선택합니다.
6. 하나 이상의 CIDR을 선택하고 CIDR 프로비저닝 해제(Deprovision CIDR)를 선택합니다.
7. CIDR 프로비저닝 해제(Deprovision CIDR)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 풀 CIDR을 프로비저닝 해제합니다.

1. IPAM 풀 ID 가져오기: [describe-ipam-pools](#)
2. 풀에 대한 현재 CIDR 확인: [get-ipam-pool-cidrs](#)
3. CIDR 프로비저닝 해제: [deprovision-ipam-pool-cidr](#)
4. 업데이트된 CIDR 확인: [get-ipam-pool-cidrs](#)

풀에 새 CIDR을 프로비저닝하려면 [풀에서 CIDR 프로비저닝 해제](#) 섹션을 참조하세요. 풀을 삭제하려면 [풀 삭제](#) 섹션을 참조하세요.

풀 편집

이 섹션의 단계를 따르면 IPAM 풀을 편집할 수 있습니다. 풀을 편집하여 풀에서 할당 규칙을 변경할 수 있습니다. 할당 규칙에 대한 자세한 내용은 [최상위 IPv4 풀 생성](#) 섹션을 참조하세요.

AWS Management Console

풀을 편집하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 기본 프라이빗 범위가 선택되어 있습니다. 기본 개인 범위를 사용하지 않으려는 경우 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 콘텐츠 창에서 편집하려는 CIDR이 있는 풀을 선택합니다.
5. 작업(Actions) > 편집(Edit)을 선택합니다.
6. 풀에 필요한 사항을 변경합니다. 풀 구성 옵션에 대한 자세한 내용은 [최상위 IPv4 풀 생성](#) 섹션을 참조하세요.
7. 업데이트를 선택합니다.

Command line

다음 AWS CLI 명령을 사용하여 풀을 편집합니다.

1. IPAM 풀 ID 가져오기: [describe-ipam-pools](#)
2. 풀 수정: [modify-ipam-pool](#)

풀 삭제

이 섹션의 단계를 따르면 IPAM 풀을 삭제할 수 있습니다.

Important

IP 주소 풀에 할당이 있는 경우 IP 주소 풀을 삭제할 수 없습니다. 먼저 할당 및 [풀에서 CIDR 프로비저닝 해제](#)을 해제해야만 풀을 삭제할 수 있습니다.

AWS Management Console

풀을 삭제하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.

2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 콘텐츠 창에서 삭제하려는 CIDR이 있는 풀을 선택합니다.
5. 작업(Actions) > 풀 삭제>Delete pool)를 선택합니다.
6. **delete**을 입력한 다음 삭제>Delete)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 풀을 삭제합니다.

1. 풀 보기 및 IPAM 풀 ID 가져오기: [describe-ipam-pools](#)
2. 풀 삭제: [delete-ipam-pool](#)
3. 풀 보기: [describe-ipam-pools](#)

새 풀을 삭제하려면 [최상위 IPv4 풀 생성](#) 섹션을 참조하세요.

리소스 검색 작업

리소스 검색은 IPAM이 소유 계정에 속한 리소스를 관리하고 모니터링할 수 있도록 하는 IPAM 구성 요소입니다. 리소스 검색은 IPAM을 생성할 때 기본적으로 생성됩니다. 또한 IPAM과 독립적으로 리소스 검색을 생성하여 다른 계정 또는 조직에서 소유한 IPAM과 통합할 수 있습니다. 리소스 검색 소유자가 조직의 위임된 관리자인 경우 IPAM은 조직의 모든 구성원에 대한 리소스를 모니터링합니다.

Note

리소스 검색 생성, 공유 및 연결은 IPAM을 조직 외부 계정과 통합하는 프로세스의 일부입니다 ([IPAM을 조직 외부 계정과 통합](#) 참조). IPAM을 생성하여 조직 외부 계정과 통합하지 않는 경우에는 리소스 검색을 생성, 공유 또는 연결할 필요가 없습니다.

내용

- [리소스 검색 생성](#)

- [리소스 검색 세부 정보 보기](#)
- [리소스 검색 공유](#)
- [리소스 검색을 IPAM과 연결](#)
- [리소스 검색 연결 해제](#)
- [리소스 검색 삭제](#)

리소스 검색 생성

이 섹션에서는 리소스 검색을 생성하는 방법을 설명합니다. 리소스 검색은 IPAM을 생성할 때 기본적으로 생성됩니다. 리전당 리소스 검색의 기본 할당량은 1입니다. IPAM 할당량에 대한 자세한 내용은 [IPAM의 할당량](#)을 참조하세요.

Note

리소스 검색 생성, 공유 및 연결은 IPAM을 조직 외부 계정과 통합하는 프로세스의 일부입니다 ([IPAM을 조직 외부 계정과 통합](#) 참조). IPAM을 생성하여 조직 외부 계정과 통합하지 않는 경우에는 리소스 검색을 생성, 공유 또는 연결할 필요가 없습니다.

IPAM을 조직 외부 계정과 통합하는 경우 이 단계는 보조 조직 관리자 계정에서 완료해야 하는 필수 단계입니다. 이 프로세스와 관련된 역할에 대한 자세한 내용은 [프로세스 개요](#)를 참조하세요.

AWS Management Console

리소스 검색을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 리소스 검색을 선택합니다.
3. 리소스 검색 생성을 선택합니다.
4. Amazon VPC IP 주소 관리자가 소스 계정의 데이터를 IPAM 위임 계정으로 복제하도록 허용 (Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account)을 선택합니다. 이 옵션을 선택하지 않으면 리소스 검색을 생성할 수 없습니다.
5. (선택 사항) 리소스 검색에 이름 태그를 추가합니다. 태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 값(선택 사항)으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

6. (선택 사항) 설명을 추가합니다.
7. 운영 리전에서 리소스를 검색할 AWS 리전을 선택합니다. 현재 리전은 운영 리전 중 하나로 자동 설정됩니다. 운영 리전 us-east-1의 IPAM과 공유할 수 있도록 리소스 검색을 생성하는 경우 여기에서 us-east-1를 선택해야 합니다. 운영 리전을 잊어버린 경우 나중에 다시 돌아와서 리소스 검색 설정을 편집할 수 있습니다.

Note

대부분의 경우 리소스 검색의 운영 리전은 IPAM과 동일해야 합니다. 그렇지 않으면 해당 리전에서만 리소스 검색이 가능합니다.

8. (선택 사항) 풀에 대한 태그를 선택합니다.
9. 생성(Create)을 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

- 리소스 검색 생성: [create-ipam-resource-discovery](#)

리소스 검색 세부 정보 보기

이 섹션에서는 리소스 검색의 세부 정보를 보는 방법을 설명합니다. 여기에는 리소스 CIDR 및 리소스 검색에서 모니터링되는 계정의 검색 상태가 포함됩니다.

AWS Management Console

리소스 검색 세부 정보를 보려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 리소스 검색을 선택합니다.
3. 리소스 검색을 선택합니다.
4. 리소스 검색 세부 정보에서 리소스 검색이 기본값인지 여부를 나타내는 기본값과 같은 리소스 검색 관련 세부 정보를 봅니다. 기본 리소스 검색은 IPAM을 생성할 때 자동으로 생성되는 리소스 검색입니다.
5. 탭에서 리소스 검색의 세부 정보를 봅니다.

- 검색된 리소스 - 리소스 검색에서 모니터링되는 리소스입니다. IPAM은 VPC, 퍼블릭 IPv4 풀, VPC 서브넷 및 탄력적 IP 주소와 같은 리소스 유형에서 CIDR을 모니터링합니다.
- 이름(리소스 ID) - 리소스 검색 ID입니다.
- IP 사용량: 사용 중인 IP 주소 공간의 백분율입니다. 소수를 백분율로 변환하려면 소수에 100을 곱합니다. 다음을 참조하세요.
 - VPC인 리소스의 경우 이는 서브넷 CIDR이 차지하는 VPC 내 IP 주소 공간의 백분율입니다.
 - 서브넷인 리소스의 경우 서브넷에 IPv4 CIDR이 프로비저닝된 경우 서브넷에서 사용 중인 IPv4 주소 공간 백분율입니다. 서브넷에 프로비저닝된 IPv6 CIDR이 있는 경우 사용 중인 IPv6 주소 공간 백분율은 표시되지 않습니다. 현재 사용 중인 IPv6 주소 공간의 백분율을 계산할 수 없습니다.
 - 퍼블릭 IPv4 풀인 리소스의 경우 이는 탄력적 IP 주소(EIP)에 할당된 풀 내 IP 주소 공간의 백분율입니다.
- CIDR - 리소스 CIDR입니다.
- 리전 - 리소스 리전입니다.
- 소유자 ID - 리소스 소유자 ID입니다.
- 샘플 시간 - 마지막으로 성공한 리소스 검색 시간입니다.
- 검색된 계정: 리소스 검색에서 모니터링 중인 AWS 계정입니다. IPAM을 AWS Organizations와 통합한 경우 조직의 모든 계정은 검색된 계정입니다.
 - 계정 ID - 계정 ID입니다.
 - 리전 - 계정 정보가 반환되는 AWS 리전입니다.
 - 마지막으로 시도한 검색 시간 - 마지막으로 시도한 리소스 검색 시간입니다.
 - 마지막으로 성공한 검색 시간 - 마지막으로 성공한 리소스 검색 시간입니다.
 - 상태 - 리소스 검색 실패 이유입니다.
- 운영 리전 - 리소스 검색의 운영 리전입니다.
- 리소스 공유 - 리소스 검색이 공유된 경우 리소스 공유 ARN이 나열됩니다.
 - 리소스 공유 ARN - 리소스 공유 ARN입니다.
 - 상태 - 리소스 공유의 현재 상태입니다. 가능한 값은 다음과 같습니다.
 - 활성화 - 리소스 공유가 활성화되어 사용할 수 있습니다.
 - 삭제됨 - 리소스 공유가 삭제되어 더 이상 사용할 수 없습니다.
 - 대기 중 - 리소스 공유를 수락하라는 초대기 응답을 기다리고 있습니다.

- 생성 날짜 - 리소스 공유가 생성된 시간입니다.
- 태그 - 태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 값(선택 사항)으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

- 리소스 검색 세부 정보 보기: [describe-ipam-resource-discovery](#)

리소스 검색 공유

이 섹션의 단계를 따르면 AWS Resource Access Manager를 사용하여 리소스 검색을 공유할 수 있습니다. AWS RAM에 대한 자세한 내용은 AWS RAM 사용 설명서의 [AWS 리소스 공유](#)를 참조하세요.

Note

리소스 검색 생성, 공유 및 연결은 IPAM을 조직 외부 계정과 통합하는 프로세스의 일부입니다 ([IPAM을 조직 외부 계정과 통합](#) 참조). IPAM을 생성하여 조직 외부 계정과 통합하지 않는 경우에는 리소스 검색을 생성, 공유 또는 연결할 필요가 없습니다.

조직 외부 계정을 모니터링하는 IPAM을 생성하면 보조 조직 관리자 계정은 AWS RAM을 사용하여 기본 조직 IPAM 계정과 리소스 검색을 공유합니다. 기본 조직 IPAM 계정에서 리소스 검색을 해당 IPAM과 연결하려면 먼저 기본 조직 IPAM 계정과 리소스 검색을 공유해야 합니다. 이 프로세스와 관련된 역할에 대한 자세한 내용은 [프로세스 개요](#)를 참조하세요.

Note

- 리소스 검색을 공유하기 위해 AWS RAM을 사용하여 리소스 공유를 생성하는 경우 기본 조직 IPAM의 홈 리전에 리소스 공유를 생성해야 합니다.
- 리소스 검색 위해 리소스 공유를 생성 및 삭제하는 계정은 IAM 정책에서 다음과 같은 권한이 있어야 합니다.
 - ec2:PutResourcePolicy

- ec2:DeleteResourcePolicy

IPAM을 조직 외부 계정과 통합하는 경우 이 단계는 보조 조직 관리자 계정에서 완료해야 하는 필수 단계입니다.

AWS Management Console

리소스 검색을 공유하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 리소스 검색을 선택합니다.
3. 리소스 공유 탭을 선택합니다.
4. 리소스 공유 생성을 선택합니다. 리소스 공유를 생성할 수 있는 AWS RAM 콘솔이 열립니다.
5. AWS RAM 콘솔에서 설정을 선택합니다.
6. AWS Organizations와 공유 활성화를 선택한 다음 설정 저장을 선택합니다.
7. 리소스 공유 생성(Create a resource share)을 선택합니다.
8. 공유 리소스에 이름을 추가합니다.
9. 리소스 유형 선택에서 IPAM 리소스 검색을 선택하고 리소스 검색을 선택합니다.
10. 다음을 선택합니다.
11. 권한 연결에서 이 리소스 공유에 대한 액세스 권한이 부여된 보안 주체에 대해 활성화되는 기본 권한을 볼 수 있습니다.
 - AWSRAMPermissionIpamResourceDiscovery
 - 이 권한으로 허용되는 작업:
 - ec2:AssociateIpamResourceDiscovery
 - ec2:GetIpamDiscoveredAccounts
 - ec2:GetIpamDiscoveredPublicAddresses
 - ec2:GetIpamDiscoveredResourceCidrs
12. 공유된 리소스에 액세스할 수 있는 보안 주체를 지정합니다. 보안 주체에서 기본 조직 IPAM 계정을 선택한 다음 추가를 선택합니다.
13. 다음을 선택합니다.
14. 리소스 공유 옵션 및 공유할 보안 주체를 검토합니다. 그런 다음 리소스 공유 생성을 선택합니다.

15. 리소스 검색을 공유한 후에는 기본 조직 IPAM 계정에서 리소스 검색을 수락한 다음 기본 조직 IPAM 계정을 통해 IPAM과 연결해야 합니다. 자세한 내용은 [리소스 검색을 IPAM과 연결](#) 단원을 참조하십시오.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

1. 리소스 공유 생성: [create-resource-share](#)
2. 리소스 공유 확인: [get-resource-shares](#)

리소스 검색을 IPAM과 연결

이 섹션에서는 리소스 검색을 IPAM과 연결하는 방법을 설명합니다. 리소스 검색을 IPAM과 연결하면 IPAM은 리소스 검색에서 검색된 모든 리소스 CIDR 및 계정을 모니터링합니다. IPAM을 생성하면 IPAM에 대한 기본 리소스 검색이 생성되고 IPAM에 자동으로 연결됩니다.

리소스 검색 연결의 기본 할당량은 5입니다. 자세한 내용(이 할당량 조정 방법 포함)은 [IPAM의 할당량](#)을 참조하세요.

Note

리소스 검색 생성, 공유 및 연결은 IPAM을 조직 외부 계정과 통합하는 프로세스의 일부입니다 ([IPAM을 조직 외부 계정과 통합](#) 참조). IPAM을 생성하여 조직 외부 계정과 통합하지 않는 경우에는 리소스 검색을 생성, 공유 또는 연결할 필요가 없습니다.

IPAM을 조직 외부 계정과 통합하는 경우 이 단계는 기본 조직 IPAM 계정에서 완료해야 하는 필수 단계입니다. 이 프로세스와 관련된 역할에 대한 자세한 내용은 [프로세스 개요](#)를 참조하세요.

AWS Management Console

리소스 검색을 연결하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 IPAM을 선택합니다.
3. 연결된 검색을 선택한 다음 리소스 검색 연결을 선택합니다.

4. IPAM 리소스 검색에서 보조 조직 관리자 계정이 공유한 리소스 검색을 선택합니다.
5. Associate(연결)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

- 리소스 검색 연결: [associate-ipam-resource-discovery](#)

리소스 검색 연결 해제

이 섹션에서는 IPAM에서 리소스 검색을 연결 해제하는 방법을 설명합니다. IPAM에서 리소스 검색을 연결 해제하면 IPAM은 리소스 검색에서 검색된 모든 리소스 CIDR 및 계정을 더 이상 모니터링하지 않습니다.

Note

기본 리소스 검색 연결은 연결 해제할 수 없습니다. 기본 리소스 검색 연결은 IPAM을 생성할 때 자동으로 생성되는 연결입니다. 그러나 IPAM을 삭제하면 기본 리소스 검색 연결이 삭제됩니다.

이 단계는 기본 조직 IPAM 계정에서 완료해야 합니다. 이 프로세스와 관련된 역할에 대한 자세한 내용은 [프로세스 개요](#)를 참조하세요.

AWS Management Console

리소스 검색 연결을 해제하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 IPAM을 선택합니다.
3. 연결된 검색을 선택한 다음 리소스 검색 연결 해제를 선택합니다.
4. IPAM 리소스 검색에서 보조 조직 관리자 계정이 공유한 리소스 검색을 선택합니다.
5. 연결 해제를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

- 리소스 검색 연결 해제: [disassociate-ipam-resource-discovery](#)

리소스 검색 삭제

이 섹션에서는 리소스 검색을 삭제하는 방법을 설명합니다.

Note

기본 리소스 검색은 삭제할 수 없습니다. 기본 리소스 검색은 IPAM을 생성할 때 자동으로 생성되는 리소스 검색입니다. 그러나 IPAM을 삭제하면 기본 리소스 검색이 삭제됩니다.

이 단계는 보조 조직 관리자 계정에서 완료해야 합니다. 이 프로세스와 관련된 역할에 대한 자세한 내용은 [프로세스 개요](#)를 참조하세요.

AWS Management Console

리소스 검색 삭제 방법

- <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
- 탐색 창에서 리소스 검색을 선택합니다.
- 리소스 검색을 선택하고 작업 > 리소스 검색 삭제를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

- 리소스 검색 삭제: [delete-ipam-resource-discovery](#)

추가 범위 생성

이 섹션의 단계를 따르면 추가 범위를 생성할 수 있습니다.

범위는 IPAM 내에서 가장 높은 수준의 컨테이너입니다. IPAM을 생성하는 경우 IPAM은 2개의 기본 범위를 대신 생성합니다. 각 범위는 단일 네트워크의 IP 공간을 나타냅니다. 프라이빗 범위(private scope)는 모든 프라이빗 공간을 위한 것입니다. 퍼블릭 범위(public scope)는 모든 퍼블릭 공간을 위한 것입니다. 범위를 사용하면 IP 주소가 중복되거나 충돌하지 않고 연결되지 않은 여러 네트워크에서 IP 주소를 재사용할 수 있습니다.

IPAM을 생성하면 기본 범위(프라이빗 범위 하나 및 퍼블릭 범위 하나)가 대신 생성됩니다. 프라이빗 범위를 추가로 생성할 수 있습니다. 프라이빗 범위를 추가로 생성할 수 없습니다.

연결이 끊긴 여러 프라이빗 네트워크에 대한 지원이 필요한 경우 추가 프라이빗 범위를 만들 수 있습니다. 추가 프라이빗 범위를 사용하면 동일한 IP 공간을 사용하는 풀을 만들고 리소스를 관리할 수 있습니다.

Important

IPAM이 프라이빗 IPv4 CIDR이 있는 리소스를 검색하면 리소스 CIDR을 기본 프라이빗 범위로 가져와 생성한 추가 프라이빗 범위에는 나타나지 않습니다. CIDR을 기본 프라이빗 범위에서 다른 프라이빗 범위로 이동할 수 있습니다. 자세한 내용은 [범위 간에 VPC CIDR 이동](#) 섹션을 참조하세요.

AWS Management Console

프라이빗 서브넷을 추가로 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 범위(Scopes)를 선택합니다.
3. 범위 생성(Create scope)을 선택합니다.
4. 범위를 추가할 IPAM을 선택합니다.
5. 범위에 대한 설명을 추가합니다.
6. 범위 생성(Create scope)을 선택합니다.
7. 탐색 창에서 범위(Scopes)를 선택하면 IPAM에서 범위를 확인할 수 있습니다.

Command line

이 섹션의 명령은 AWS CLI 참조 문서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 프라이빗 범위를 추가로 생성합니다.

1. 현재 범위 확인: [describe-ipam-scopes](#)
2. 새 프라이빗 범위 생성: [create-ipam-scope](#)
3. 새 범위를 보려면 현재 범위 확인: [describe-ipam-scopes](#)

범위 간에 VPC CIDR 이동

이번 섹션의 단계를 따르면 VPC CIDR을 한 범위에서 다른 범위로 이동할 수 있습니다.

Important

- VPC CIDR만 이동할 수 있습니다. VPC CIDR을 이동하면 VPC의 서브넷 CIDR도 자동으로 이동합니다.
- VPC CIDR은 한 프라이빗 범위에서 다른 프라이빗 범위로만 이동할 수 있습니다. VPC CIDR은 퍼블릭 범위에서 프라이빗 범위로 이동하거나 프라이빗 범위에서 퍼블릭 범위로 이동할 수 없습니다.
- 동일한 AWS 계정은 두 범위를 모두 소유해야 합니다.
- VPC CIDR이 프라이빗 범위의 풀에서 현재 할당된 경우 이동 요청은 성공하지만 현재 풀에서 VPC CIDR 할당을 해제할 때까지 VPC CIDR은 이동하지 않습니다. 할당 해제에 대한 자세한 내용은 [할당 해제](#)를 참조하세요.

AWS Management Console

VPC에 할당된 CIDR 이동

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 리소스(Resources)를 선택합니다.
3. 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다.
4. 콘텐츠 창에서 VPC를 선택하고 VPC의 세부 정보를 봅니다.
5. VPC CIDRs에서 리소스에 할당된 CIDR 중 하나를 선택하고 작업(Actions) > CIDR을 다른 범위로 이동(Move CIDR to different scope)을 선택합니다.
6. VPC CIDR을 이동하려는 범위를 선택합니다.
7. CIDR을 다른 범위로 이동(Move CIDR to different scope)을 선택합니다.

Command line

다음 AWS CLI 명령을 사용하여 VPC CIDR을 이동합니다.

1. 현재 범위의 VPC CIDR 가져오기: [get-ipam-resource-cidrs](#)
2. 리소스 CIDR 이동: [modify-ipam-resource-cidr](#)
3. 다른 범위의 VPC CIDR 가져오기: [get-ipam-resource-cidrs](#)

VPC CIDR의 모니터링 상태 변경

이 섹션의 단계를 따르면 VPC CIDR의 모니터링 상태를 변경할 수 있습니다. IPAM이 VPC를 관리하거나 모니터링하지 않고 VPC에 할당된 CIDR을 사용할 수 있도록 하려면 VPC CIDR을 모니터링됨에서 무시됨으로 변경할 수 있습니다. IPAM이 VPC CIDR을 관리하거나 모니터링하려면 VPC CIDR을 무시됨에서 모니터링됨으로 변경할 수 있습니다.

Note

- 퍼블릭 범위의 VPC CIDR은 무시할 수 없습니다.
- CIDR이 무시되면 CIDR의 활성 IP 주소에 대한 요금이 계속 부과됩니다. 자세한 내용은 [IPAM 가격](#) 단원을 참조하십시오.
- CIDR이 무시되면 CIDR에서 IP 주소 기록을 볼 수 있습니다. 자세한 내용은 [IP 주소 기록 보기](#) 단원을 참조하십시오.

VPC CIDR의 모니터링 상태를 모니터링됨 또는 무시됨으로 변경할 수 있습니다.

- 모니터링됨(Monitored): IPAM에서 VPC CIDR이 감지되었으며 다른 CIDR 및 할당 규칙 관련 규정 준수와 겹치는지 여부가 모니터링되고 있습니다.
- 무시됨(Ignored): VPC CIDR이 모니터링에서 면제되도록 선택되었습니다. 무시된 VPC CIDR은 다른 CIDR 또는 할당 규칙 관련 규정 준수와 겹치는 것으로 평가되지 않습니다. VPC CIDR을 무시하도록 선택하면 IPAM 풀에서 해당 VPC CIDR에 할당된 공간이 풀로 반환되며, 자동 가져오기 할당 규칙이 풀에 설정된 경우 VPC CIDR을 다시 가져오지 않습니다.

AWS Management Console

VPC에 할당된 CIDR의 모니터링 상태 변경

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 리소스(Resources)를 선택합니다.
3. 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 프라이빗 범위를 선택합니다.
4. 콘텐츠 창에서 VPC를 선택하고 VPC의 세부 정보를 봅니다.
5. VPC CIDR에서 VPC에 할당된 CIDR 중 하나를 선택하고 작업 > 무시됨으로 표시 또는 무시됨으로 표시 해제를 선택합니다.
6. 무시됨으로 표시(Mark as ignored) 또는 무시됨으로 표시 해제(Unmark as ignored)를 선택합니다.

Command line

다음 AWS CLI 명령을 사용하여 VPC CIDR의 모니터링 상태를 변경할 수 있습니다.

1. 범위 ID 가져오기: [describe-ipam-scopes](#)
2. VPC CIDR에 대한 현재 모니터링 상태 보기: [get-ipam-resource-cidrs](#)
3. VPC CIDR의 상태 변경: [modify-ipam-resource-cidr](#)
4. VPC CIDR에 대한 새로운 모니터링 상태 보기: [get-ipam-resource-cidrs](#)

범위 삭제

이 섹션의 단계를 따르면 IPAM 범위를 삭제할 수 있습니다.

Important

다음 중 하나가 true인 경우 범위를 삭제할 수 없습니다.

- 범위는 기본 범위입니다. IPAM을 생성하는 경우 2개의 기본 범위(퍼블릭 1개, 프라이빗 1개)가 자동으로 생성되며 삭제할 수 없습니다. 범위가 기본 범위인지 확인하려면 범위의 세부 정보에서 범위 유형(Scope type)을 확인할 수 있습니다.
- 범위에 폴이 하나 이상 있습니다. 먼저 [폴 삭제](#)를 수행해야 범위를 삭제할 수 있습니다.

AWS Management Console

범위를 삭제하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 범위(Scopes)를 선택합니다.
3. 콘텐츠 창에서 삭제하려는 범위를 선택합니다.
4. 작업(Actions) > 범위 삭제>Delete scope를 선택합니다.
5. **delete**을 입력한 다음 삭제>Delete)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 범위를 삭제합니다.

1. 범위 확인: [describe-ipam-scopes](#)
2. 범위 삭제: [delete-ipam-scope](#)
3. 업데이트된 범위 확인: [describe-ipam-scopes](#)

새 범위를 생성하려면 [추가 범위 생성](#) 섹션을 참조하세요. IPAM을 삭제하려면 [IPAM 삭제](#) 섹션을 참조하세요.

할당 해제

이번 섹션의 단계를 따르면 IPAM 풀에서 CIDR 할당을 해제할 수 있습니다. 할당은 IPAM 풀에서 다른 리소스 또는 IPAM 풀로 CIDR을 할당하는 것입니다.

풀을 삭제하려는 경우 풀 할당을 해제해야 할 수 있습니다. 풀에 CIDR이 프로비저닝되어 있으면 해당 풀을 삭제할 수 없으며, CIDR이 리소스에 할당되어 있는 경우에는 CIDR의 프로비저닝을 해제할 수 없습니다.

Note

- 수동 할당을 해제하려면 이 섹션의 단계를 사용하거나 [ReleaseIpamPoolAllocation API](#)를 호출하세요.

- 프라이빗 범위에서 할당을 해제하려면 리소스 CIDR을 무시하거나 삭제해야 합니다. 자세한 내용은 [VPC CIDR의 모니터링 상태 변경](#) 단원을 참조하십시오. 잠시 후 Amazon VPC IPAM은 사용자를 대신하여 할당을 자동으로 해제합니다.

Example

예

VPC CIDR이 프라이빗 범위에 있는 경우 할당을 해제하기 위해서는 VPC CIDR을 무시하거나 삭제해야 합니다. 잠시 후 Amazon VPC IPAM은 VPC CIDR 할당을 IPAM에서 자동으로 해제합니다.

- 퍼블릭 범위에서 할당을 해제하려면 리소스 CIDR을 삭제해야 합니다. 퍼블릭 리소스 CIDR은 무시할 수 없습니다. 자세한 내용은 [AWS CLI만 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#)의 정리 또는 [AWS CLI만 사용하여 IPAM으로 고유 IPv6 CIDR 가져오기](#)의 정리를 참조하세요. 잠시 후 Amazon VPC IPAM은 사용자를 대신하여 할당을 자동으로 해제합니다.

Amazon VPC IPAM이 사용자를 대신하여 할당을 해제하기 위해서는 모든 계정 권한이 [단일 계정 사용](#) 또는 [복수 계정 사용](#)에 대해 올바르게 구성되어야 합니다.

IPAM에서 관리하는 CIDR을 해제하면 Amazon VPC IPAM은 CIDR을 다시 IPAM 풀로 재활용합니다. CIDR을 향후 할당에 사용할 수 있게 되는 데 몇 분 정도 걸립니다. 풀 및 할당에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.

AWS Management Console

풀 할당을 해제하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 콘텐츠 창에서 할당이 있는 풀을 선택합니다.
5. 할당(Allocations) 탭을 선택합니다.
6. 하나 이상의 할당을 선택합니다. 리소스 유형별로 할당을 식별할 수 있습니다.

- 사용자 지정(custom): 사용자 지정 할당입니다.
 - vpc: VPC 할당입니다.
 - ipam-pool: IPAM 풀 할당입니다.
 - ec2-public-ipv4-pool: 퍼블릭 IPv4 풀 할당입니다.
7. 작업(Actions) > 사용자 지정 할당 해제(Release custom allocation)를 선택합니다.
 8. CIDR 할당 취소(Deallocate CIDRs)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 풀 할당을 해제합니다.

1. IPAM 풀 ID 가져오기: [describe-ipam-pools](#)
2. 풀에서 현재 할당 보기: [get-ipam-pool-allocations](#)
3. 할당 해제: [release-ipam-pool-allocation](#)
4. 업데이트된 할당 보기: [get-ipam-pool-allocations](#).

새 할당을 추가하려면 [CIDR 할당](#) 섹션을 참조하세요. 할당을 해제한 후 풀을 삭제하려면 먼저 [풀에서 CIDR 프로비저닝 해제](#)를 수행해야 합니다.

IPAM 수정

이 섹션의 단계를 따르면 IPAM을 수정할 수 있습니다.

내용

- [IPAMM 티어 수정](#)
- [IPAM 운영 리전 수정](#)

IPAMM 티어 수정

IPAM 티어를 수정하려면 이 섹션의 단계를 따르세요. IPAM은 프리 티어와 고급 티어라는 두 가지 티어를 제공합니다. 프리 티어에서 사용할 수 있는 기능 및 고급 티어 관련 비용에 대한 자세한 내용은 [Amazon VPC 요금 페이지](#)의 IPAM 탭을 참조하세요.

⚠ Important

고급 티어에서 프리 티어로 전환하려면 먼저 다음을 수행해야 합니다.

- 프라이빗 스코프 풀을 삭제합니다.
- 기본이 아닌 프라이빗 범위를 삭제합니다.
- IPAM 홈 리전과 다른 로케일을 가진 풀을 삭제합니다.
- 기본이 아닌 리소스 검색 연결을 삭제합니다.
- IPAM 소유자가 아닌 계정에 대한 풀 할당을 삭제합니다.

AWS Management Console

IPAM 티어를 수정하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 IPAM을 선택합니다.
3. 콘텐츠 창에서 IPAM을 선택합니다.
4. 작업(Actions) > 편집(Edit)을 선택합니다.
5. IPAM에 사용하려는 IPAM 티어를 선택합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

IPAM 티어를 보고 수정하려면 다음 AWS CLI 명령을 사용하세요.

1. 현재 IPAM 확인: [describe-ipams](#)
2. IPAM 티어 수정: [modify-ipam](#)
3. 업데이트된 IPAM 확인: [describe-ipams](#)

IPAM 운영 리전 수정

IPAM 운영 리전을 수정하려면 이 섹션의 단계를 따르세요. 운영 리전은 IPAM이 IP 주소 CIDR을 관리할 수 있는 AWS 리전입니다. IPAM은 운영 리전으로 선택한 AWS 리전에서만 리소스를 검색하고 모니터링합니다.

AWS Management Console

IPAM 운영 리전을 수정하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 IPAM을 선택합니다.
3. 콘텐츠 창에서 IPAM을 선택합니다.
4. 작업(Actions) > 편집(Edit)을 선택합니다.
5. IPAM 설정에서 IPAM에 사용할 운영 리전을 선택합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

IPAM 운영 리전을 보고 수정하려면 다음 AWS CLI 명령을 사용하세요.

1. 현재 IPAM 확인: [describe-ipams](#)
2. IPAM 운영 리전 추가 또는 제거: [modify-ipam](#)
3. 업데이트된 IPAM 확인: [describe-ipams](#)

IPAM 삭제

이 섹션의 단계를 따르면 IPAM을 삭제할 수 있습니다. 기존 IPAM을 삭제하는 대신 보유할 수 있는 IPAM의 기본 수를 늘리는 방법에 대한 자세한 내용은 [IPAM의 할당량](#) 섹션을 참조하세요.

Important

IPAM을 삭제하면 CIDR에 대한 기록 데이터를 포함하여 IPAM과 연결된 모든 모니터링된 데이터가 제거됩니다.

AWS Management Console

IPAM을 삭제하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 IPAM을 선택합니다.
3. 콘텐츠 창에서 IPAM을 선택합니다.
4. 작업(Actions) > IPAM 삭제>Delete IPAM)를 선택합니다.
5. 다음 중 하나를 수행하십시오.
 - IPAM, 프라이빗 범위, 프라이빗 범위의 풀 및 프라이빗 범위의 풀에 있는 모든 할당을 삭제하려면 CASCADE 삭제(Cascade delete)를 선택합니다. 퍼블릭 범위에 풀이 있는 경우에는 이 옵션을 사용하여 IPAM을 삭제할 수 없습니다. 이 옵션을 사용하는 경우 IPAM은 다음을 수행합니다.
 - 프라이빗 범위의 풀에서 VPC 리소스(예: VPC)에 할당된 모든 CIDR 할당을 해제합니다.

 Note

이 옵션을 사용 설정한 결과 VPC 리소스가 삭제되지 않습니다. 리소스와 연결된 CIDR은 더 이상 IPAM 풀에서 할당되지 않지만 CIDR 자체는 변경되지 않습니다.

- 프라이빗 범위의 IPAM 풀에 프로비저닝된 모든 IPv4 CIDR의 프로비저닝을 해제합니다.
 - 프라이빗 범위의 모든 IPAM 풀을 삭제합니다.
 - IPAM에서 기본이 아닌 모든 프라이빗 범위를 삭제합니다.
 - 기본 퍼블릭 및 프라이빗 범위와 IPAM을 삭제합니다.
6. Cascade 삭제(Cascade delete)를 선택하지 않은 경우 IPAM을 삭제하기 전에 먼저 다음을 수행해야 합니다.
 - IPAM 풀 내에서 할당을 릴리스합니다. 자세한 내용은 [할당 해제](#) 섹션을 참조하세요.
 - IPAM 내의 풀에 프로비저닝된 CIDR 프로비전을 해제합니다. 자세한 내용은 [풀에서 CIDR 프로비저닝 해제](#) 단원을 참조하십시오.
 - 기본 범위가 아닌 추가 범위를 모두 삭제합니다. 자세한 내용은 [범위 삭제](#) 단원을 참조하십시오.
 - IPAM 풀을 삭제합니다. 자세한 내용은 [풀 삭제](#) 단원을 참조하십시오.
6. **delete**을 입력한 다음 삭제>Delete)를 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 IPAM을 삭제합니다.

1. 현재 IPAM 확인: [describe-ipams](#)
2. IPAM 삭제: [delete-ipam](#)
3. 업데이트된 IPAM 확인: [describe-ipams](#)

새 IPAM을 삭제하려면 [IPAM 생성](#) 섹션을 참조하세요.

IPAM에서 IP 주소 사용량 추적

이 섹션에서 설명하는 작업은 선택 사항입니다. 이 섹션의 작업을 완료하고 IPAM 계정을 위임한 경우에는 IPAM 계정이 작업을 완료해야 합니다.

이 섹션의 단계를 따라 IPAM을 통해 IP 주소 사용량을 추적합니다.

내용

- [IPAM 대시보드를 사용하여 CIDR 사용량 모니터링](#)
- [리소스별 CIDR 사용량 모니터링](#)
- [Amazon CloudWatch를 사용하여 IPAM 모니터링](#)
- [IP 주소 기록 보기](#)
- [퍼블릭 IP 인사이트 보기](#)

IPAM 대시보드를 사용하여 CIDR 사용량 모니터링

이 섹션의 단계를 따르면 IPAM 대시보드에 액세스하고 특정 IPAM 범위 내의 모든 CIDR 상태를 확인할 수 있습니다.

AWS Management Console

IPAM 대시보드를 사용하여 CIDR 사용량을 모니터링하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 대시보드(Dashboard)를 선택합니다.
3. 기본적으로 대시보드를 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 기본 개인 범위를 사용하지 않으려는 경우 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 대시보드는 범위 내의 IPAM 풀 및 CIDR에 대한 개요를 제공합니다. 위젯을 추가, 제거, 크기 조정 및 이동하여 대시보드를 사용자 정의할 수 있습니다.

- 범위: 이 범위의 세부 정보입니다. 범위는 IPAM 내에서 가장 높은 수준의 컨테이너입니다. IPAM에는 2개의 기본 범위(프라이빗 및 퍼블릭)가 포함되어 있습니다. 각 범위는 단일 네트워크의 IP 공간을 나타냅니다. 프라이빗 범위는 여러 개 있을 수 있지만 퍼블릭 범위는 한 개만 가질 수 있습니다.
- 범위 ID(Scope ID): 이 범위의 ID입니다.

- 범위 유형(Scope type): 범위 유형입니다.
- IPAM ID: 범위가 있는 IPAM의 ID입니다.
- 이 범위의 IPAM 풀: 범위가 있는 IPAM의 ID입니다.
- 이 범위의 네트워킹 리소스 보기: IPAM 콘솔의 리소스 섹션으로 이동합니다.
- 이 범위의 IP 주소 기록 검색: IPAM 콘솔의 IP 기록 검색 섹션으로 이동합니다.
- 리소스 CIDR 유형: 범위에 있는 리소스 CIDR의 유형입니다.
 - 서브넷: 서브넷의 CIDR 수입니다.
 - VPC: VPC의 CIDR 수입니다.
 - EIP: 엘라스틱 IP 주소의 CIDR 수입니다.
 - 퍼블릭 IPv4 풀: 퍼블릭 IPv4 풀의 CIDR 수입니다.
- 관리 상태: CIDR의 관리 상태입니다.
 - 비관리형 CIDR(Unmanaged CIDRs): 이 범위의 비관리형 리소스에 대한 리소스 CIDR 수입니다.
 - 무시된 CIDR(Ignored CIDRs): 범위의 IPAM을 사용하여 모니터링이 면제되도록 선택한 리소스 CIDR 수입니다. IPAM은 무시된 리소스를 범위 내의 겹침 또는 규정 준수로 평가하지 않습니다. 리소스를 무시하도록 선택하면 IPAM 풀에서 해당 리소스에 할당된 공간이 풀로 반환되며, 자동 가져오기를 통해(자동 가져오기 할당 규칙이 풀에 설정된 경우) 리소스를 다시 가져오지 않습니다.
 - 관리형 CIDR(Managed CIDRs): 범위의 IPAM 풀에서 할당된 관리 가능한 리소스(VPC 또는 퍼블릭 IPv4 풀)에 대한 리소스 CIDR 수입니다.
- 겹치는 리소스 CIDR: 겹치는 CIDR과 겹치지 않는 CIDR의 수입니다. CIDR이 겹치면 VPC에서 라우팅이 잘못될 수 있습니다.
 - 겹치는 CIDR(Overlapping CIDRs): 범위의 IPAM 풀 내에서 현재 겹치는 CIDR의 수입니다. CIDR이 겹치면 VPC에서 라우팅이 잘못될 수 있습니다.
 - 겹치지 않는 CIDR: 이 범위의 IPAM 풀 내에서 겹치지 않는 리소스 CIDR의 수입니다.
- 규정 준수 리소스 CIDR: 규정 준수 리소스 CIDR의 수입니다.
 - 규정 준수 CIDR(Compliant CIDRs): 범위의 IPAM 풀에 대한 할당 규칙을 준수하는 리소스 CIDR 수입니다.
 - 규정 미준수 CIDR(Noncompliant CIDRs): 범위의 IPAM 풀에 대한 할당 규칙을 준수하지 않는 리소스 CIDR 수입니다.
- 겹침 상태: 시간이 지남에 따라 겹치는 CIDR의 수입니다.

- **겹치는 리소스 CIDR:** 이 범위의 IPAM 풀 내에서 현재 겹치는 CIDR의 수입입니다. CIDR이 겹치면 VPC에서 라우팅이 잘못될 수 있습니다.
- **규정 준수 상태:** 시간이 지남에 따라 범위의 IPAM 풀에 대한 할당 규칙을 준수하지 않는 CIDR의 수입입니다.
- **규정 준수 리소스 CIDR:** 할당 규칙을 준수하는 리소스 CIDR의 수입입니다.
- **규정 미준수 리소스 CIDR:** 할당 규칙을 준수하지 않는 리소스 CIDR의 수입입니다.
- **VPC 사용률:** IP 사용률이 가장 높거나 가장 낮은 VPC(IPv4 및 IPv6)입니다. 이 정보를 사용하여 IP 사용률 임계값을 위반한 경우 Amazon CloudWatch 경보가 울리도록 구성할 수 있습니다. 자세한 내용은 [리소스 사용률 지표](#) 단원을 참조하십시오.
- **서브넷 사용률:** IP 사용률이 가장 높거나 가장 낮은 서브넷(IPv4만 해당)입니다. 이 정보를 사용하여 사용률이 낮은 리소스를 유지할지 또는 삭제할지 결정할 수 있습니다. 자세한 내용은 [리소스 사용률 지표](#) 단원을 참조하십시오.
- **할당된 IP가 가장 많은 VPC:** 서브넷에 할당된 IP 주소 공간 비율이 가장 높은 VPC입니다. 이는 VPC에 추가 IP 주소 공간을 프로비저닝해야 하는지를 보여 주는 데 유용합니다.
- **할당된 IP가 가장 많은 서브넷:** 리소스에 할당된 IP 주소 공간 비율이 가장 높은 서브넷입니다. 이는 서브넷에 추가 IP 주소 공간을 프로비저닝해야 하는지를 보여 주는 데 유용합니다.
- **풀 할당:** 시간이 지남에 따라 범위의 리소스 및 수동 할당에 할당된 IP 공간의 백분율입니다.
- **풀 할당:** 시간이 지남에 따라 범위의 다른 풀에 할당된 풀 IP 공간의 백분율입니다.

Command line

대시보드에 표시되는 정보는 Amazon CloudWatch에 저장된 지표에서 가져옵니다. Amazon CloudWatch에 저장된 지표에 대한 자세한 내용은 [Amazon CloudWatch를 사용하여 IPAM 모니터링](#) 섹션을 참조하세요. [AWS CLI 참조](#)에서 Amazon CloudWatch 옵션을 사용하여 IPAM 풀 및 범위의 할당에 대한 지표를 확인합니다.

풀에 대해 프로비저닝된 CIDR 할당이 거의 완료된 경우 추가로 CIDR을 프로비저닝해야 할 수 있습니다. 자세한 내용은 [풀에 CIDR 프로비저닝](#) 섹션을 참조하세요.

리소스별 CIDR 사용량 모니터링

IPAM에서 리소스는 IP 주소 또는 CIDR 블록이 할당된 AWS 서비스 엔터티입니다. IPAM은 일부 리소스를 관리하지만 다른 리소스는 모니터링만 합니다.

- 관리형 리소스(Managed resource): 관리형 리소스에는 IPAM 풀에서 할당된 CIDR이 있습니다. IPAM은 풀의 다른 CIDR과 IP 주소가 겹칠 가능성이 있는지 CIDR을 모니터링하고 CIDR이 풀의 할당 규칙을 준수하는지 모니터링합니다. IPAM은 다음과 같은 유형의 리소스 관리를 지원합니다.
 - VPC
 - 퍼블릭 IPv4 풀

Important

퍼블릭 IPv4 풀 및 IPAM 풀은 AWS의 고유한 리소스에 의해 관리됩니다. 퍼블릭 IPv4 풀은 공개 소유의 CIDR을 탄력적 IP 주소로 변환할 수 있는 단일 계정 리소스입니다. IPAM 풀을 사용하여 퍼블릭 공간을 퍼블릭 IPv4 풀에 할당할 수 있습니다.

- 모니터링된 리소스(Monitored resource): IPAM에서 리소스를 모니터링하는 경우 AWS CLI를 통해 `get-ipam-resource-cidrs`를 사용하거나 탐색 창에서 리소스(Resources)를 확인하면 IPAM에서 리소스를 감지하고 리소스의 CIDR에 대한 세부 정보를 확인할 수 있습니다. IPAM은 다음 리소스의 모니터링을 지원합니다.
 - VPC
 - 퍼블릭 IPv4 풀
 - VPC 서브넷
 - 탄력적 IP 주소

다음 단계에서는 리소스별 CIDR 사용량 및 할당 규칙 규정 준수를 모니터링하는 방법을 보여줍니다.

AWS Management Console

리소스별 CIDR 사용량을 모니터링하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 리소스(Resources)를 선택합니다.
3. 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 리소스 CIDR 맵을 사용하면 범위 내에서 사용 가능한 IP 주소 공간, 할당된 IP 주소 공간 및 겹치는 IP 주소 공간을 볼 수 있습니다.
 - 사용 가능: 할당할 수 있는 IP 주소 범위가 있습니다.
 - 규정 준수 및 비겹침: IPAM에서 관리하는 리소스에 IP 주소 범위가 할당되었습니다.

- 점유: IP 주소 범위가 리소스에 할당되었습니다.
- 겹침: IP 주소 범위가 여러 리소스에 할당되어 중첩됩니다.
- 규정 미준수: IP 주소 범위가 규정을 준수하지 않습니다. 풀에 설정된 할당 규칙을 준수하지 않는 IP 주소 범위를 사용하는 리소스가 있습니다.

CIDR 맵에서 맵 하단에 있는 IP 주소 블록을 선택하면 작은 CIDR 블록 단위로 리소스를 볼 수 있습니다. 맵 상단에서 IP 주소 블록을 선택하면 더 큰 CIDR 블록 단위로 리소스를 볼 수 있습니다.

5. 표에서 범위 내 리소스에 대해 다음과 같은 세부 정보를 볼 수 있습니다.

- 이름(리소스 ID): 리소스의 이름 및 리소스 ID입니다.
- CIDR: 리소스와 연결된 CIDR입니다.
- 관리 상태(Management state): 리소스의 상태입니다.
 - 관리형(Managed): 리소스에는 IPAM 풀에서 할당된 CIDR이 있으며 IPAM에서 잠재적 CIDR 겹침 및 풀 할당 규칙 관련 규정 준수에 대해 모니터링하고 있습니다.
 - 비관리형(Unmanaged): 리소스에는 IPAM 풀에서 할당된 CIDR이 있으며 IPAM에서 잠재적 CIDR 겹침 및 풀 할당 규칙 관련 규정 준수에 대해 모니터링하고 있지 않습니다. CIDR은 겹침에 대해 모니터링됩니다.
 - 무시됨(Ignored): 리소스가 모니터링에서 면제되도록 선택되었습니다. 무시된 리소스는 겹침 또는 할당 규칙 관련 규정 준수로 평가되지 않습니다. 리소스를 무시하도록 선택하면 IPAM 풀에서 해당 리소스에 할당된 공간이 풀로 반환되며, 자동 가져오기를 통해(자동 가져오기 할당 규칙이 풀에 설정된 경우) 리소스를 다시 가져오지 않습니다.
 - -: 이 리소스는 IPAM이 관리할 수 있는 리소스 유형 중 하나가 아닙니다.
- 규정 준수 상태(Compliance status): CIDR의 규정 준수 상태입니다.
 - 규정 준수(Compliant): 관리형 리소스는 IPAM 풀의 할당 규칙을 준수합니다.
 - 규정 미준수(Noncompliant): 리소스 CIDR은 IPAM 풀의 할당 규칙 하나 이상을 준수하지 않습니다.

Example

VPC에 IPAM 풀의 넷마스크 길이 파라미터를 충족하지 않는 CIDR이 있거나 리소스가 IPAM 풀과 동일한 AWS 리전에 있지 않은 경우 비준수 플래그로 지정됩니다.

- 비관리형(Unmanaged): 리소스에는 IPAM 풀에서 할당된 CIDR이 있으며 IPAM에서 잠재적 CIDR 겹침 및 풀 할당 규칙 관련 규정 준수에 대해 모니터링하고 있지 않습니다. CIDR은 겹침에 대해 모니터링됩니다.
 - 무시됨(Ignored): 리소스가 모니터링에서 면제되도록 선택되었습니다. 무시된 리소스는 겹침 또는 할당 규칙 관련 규정 준수로 평가되지 않습니다. 리소스를 무시하도록 선택하면 IPAM 풀에서 해당 리소스에 할당된 공간이 풀로 반환되며, 자동 가져오기를 통해(자동 가져오기 할당 규칙이 풀에 설정된 경우) 리소스를 다시 가져오지 않습니다.
 - -: 이 리소스는 IPAM이 관리할 수 있는 리소스 유형 중 하나가 아닙니다.
 - 겹침 상태(Overlap status): CIDR의 겹침 상태입니다.
 - 비겹침(Nonoverlapping): 리소스 CIDR이 동일한 범위의 다른 CIDR과 겹치지 않습니다.
 - 겹침(Overlapping): 리소스 CIDR이 동일한 범위의 다른 CIDR과 겹칩니다. 리소스 CIDR이 겹치는 경우 수동 할당과 겹칠 수 있습니다.
 - 무시됨(Ignored): 리소스가 모니터링에서 면제되도록 선택되었습니다. IPAM은 무시된 리소스를 겹침 또는 할당 규칙 관련 규정 준수로 평가하지 않습니다. 리소스를 무시하도록 선택하면 IPAM 풀에서 해당 리소스에 할당된 공간이 풀로 반환되며, 자동 가져오기를 통해(자동 가져오기 할당 규칙이 풀에 설정된 경우) 리소스를 다시 가져오지 않습니다.
 - -: 이 리소스는 IPAM이 관리할 수 있는 리소스 유형 중 하나가 아닙니다.
 - IP 사용량: VPC인 리소스의 경우 서브넷 CIDR이 차지하는 VPC의 IP 주소 공간 백분율입니다. 서브넷인 리소스의 경우 서브넷에 IPv4 CIDR이 프로비저닝된 경우 서브넷에서 사용 중인 IPv4 주소 공간 백분율입니다. 서브넷에 프로비저닝된 IPv6 CIDR이 있는 경우 사용 중인 IPv6 주소 공간 백분율은 표시되지 않습니다. 현재 사용 중인 IPv6 주소 공간의 백분율을 계산할 수 없습니다. 퍼블릭 IPv4 풀인 리소스의 경우 이는 탄력적 IP 주소(EIP)에 할당된 풀 내 IP 주소 공간의 백분율입니다.
 - 리전(Region): 리소스의 AWS 리전입니다.
 - 소유자 ID(Owner ID): 이 리소스를 만든 사람의 AWS 계정 ID입니다.
 - 리소스 유형: 리소스가 VPC, 서브넷, 탄력적 IP 주소 또는 퍼블릭 IPv4 풀인지 여부.
 - 풀 ID(Pool ID): 리소스가 있는 IPAM 풀의 ID입니다.
6. 리소스 필터링을 사용하여 리소스 테이블을 VPC ID나 규정 준수 상태와 같은 열 속성에 따라 필터링할 수 있습니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

다음 AWS CLI 명령을 사용하여 리소스별 CIDR 사용량을 모니터링합니다.

1. 범위 ID 가져오기: [describe-ipam-scopes](#)
2. 리소스 정보 요청: [get-ipam-resource-cidrs](#)

Amazon CloudWatch를 사용하여 IPAM 모니터링

IPAM은 IP 주소 사용량(예: IPAM 풀에서 사용 가능한 IP 주소 공간 및 할당 규칙을 준수하는 리소스 CIDR 수) 및 리소스 사용률과 관련된 메트릭을 IPAM의 홈 리전에 있는 AWS/IPAM [Amazon CloudWatch 네임스페이스](#)에 자동으로 저장합니다.

내용

- [IPAM 풀 및 범위 지표](#)
- [리소스 사용률 지표](#)

IPAM 풀 및 범위 지표

IPAM은 IPAM 풀 및 범위에 대한 데이터를 Amazon CloudWatch에 게시합니다. 이러한 지표로 IPAM 풀에 대한 경보를 생성하여 주소 풀이 거의 소진되거나 리소스가 풀에 설정된 할당 규칙을 준수하지 못하는 경우 이를 알릴 수 있습니다. Amazon CloudWatch를 사용한 경보 생성 및 알림 설정은 본 섹션의 범위를 벗어납니다. 자세한 내용은 [Amazon CloudWatch 사용 설명서](#)의 Amazon CloudWatch 경보 사용을 참조하세요.

IPAM에서 Amazon CloudWatch로 전송하는 지표와 차원은 아래에 나와 있습니다.

IPAM 풀 지표

지표 이름	설명
CompliantResourceCidrs	IPAM 풀의 할당 규칙을 준수하는 관리형 리소스 CIDR 수입니다. 할당 규칙에 대한 자세한 내용은 최상위 IPv4 풀 생성 섹션을 참조하세요.
NoncompliantResourceCidrs	IPAM 풀의 할당 규칙을 준수하지 않는 관리형 리소스 CIDR 수입니다. 할당 규칙에 대한 자세한 내용은 최상위 IPv4 풀 생성 섹션을 참조하세요.
PercentAllocated	다른 풀에 할당된 풀 IP 공간의 백분율입니다.

지표 이름	설명
PercentAssigned	수동 할당을 포함하여 리소스에 할당된 풀 IP 공간의 백분율입니다.
PercentAvailable	다른 풀 또는 리소스에 할당되지 않은 풀 IP 공간의 백분율입니다.

IPAM 범위 지표

지표 이름	설명
CompliantResourceCidrs	범위의 IPAM 풀에 대한 할당 규칙을 준수하는 리소스 CIDR 수입입니다.
ManagedResourceCidrs	범위의 IPAM 풀에서 할당된 관리 가능한 리소스(VPC 또는 퍼블릭 IPv4 풀)에 대한 리소스 CIDR 수입입니다.
NoncompliantResourceCidrs	범위의 IPAM 풀에 대한 할당 규칙을 준수하지 않는 리소스 CIDR 수입입니다.
OverlappingResourceCidrs	범위에서 겹치는 리소스 CIDR 수입입니다.
UnmanagedResourceCidrs	현재 관리 가능한 리소스와 연결되어 있지만 IPAM에서 관리하지 않는 범위의 리소스 CIDR 수입입니다.

다음은 IPAM 지표를 필터링하는 데 사용할 수 있는 차원입니다.

측정기준	설명
AddressFamily	리소스 CIDR(IPv4 또는 IPv6)의 IP 주소 패밀리입니다.
Locale	IPAM 풀을 할당에 사용할 수 있는 AWS 리전입니다.
PoolID	풀의 ID입니다.
ScopeID	범위의 ID입니다.

Amazon CloudWatch를 사용하여 VPC를 모니터링하는 방법에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 [VPC의 CloudWatch 지표](#)를 참조하세요.

리소스 사용률 지표

IPAM은 IPAM이 모니터링하는 리소스에 대한 IP 사용률 지표를 Amazon CloudWatch에 게시합니다. 이러한 리소스는 다음을 포함합니다.

- VPC(IPv4 및 IPv6)
- 서브넷(IPv4)
- 퍼블릭 IPv4 풀

IPAM은 IP 주소 패밀리(IPv4 또는 IPv6)별로 IP 사용률 지표를 별도로 계산하고 게시합니다. 리소스의 IP 사용률은 동일한 주소 패밀리의 모든 CIDR에 대해 계산됩니다.

각 리소스 유형 및 주소 패밀리 조합에 대해 IPAM은 세 가지 규칙을 사용하여 게시할 지표를 결정합니다.

- 최대 50개의 IP 사용률이 가장 높은 리소스. 이 정보를 사용하여 IP 사용률 임계값을 위반한 경우 경보가 울리도록 구성할 수 있습니다.
- 최대 50개의 IP 사용률이 가장 낮은 리소스. 이 정보를 사용하여 사용률이 낮은 리소스를 유지할지 또는 삭제할지 결정할 수 있습니다.
- 최대 50개의 기타 리소스. 이 정보를 사용하여 사용률이 높거나 낮은 그룹 내에서 캡처되지 않을 수 있는 리소스의 IP 사용률을 일관되게 추적할 수 있습니다.
 - IPAM 풀에서 할당된 CIDR을 포함하는 최대 50개의 VPC(총 CIDR 블록 크기에 따라 우선순위 지정).
 - VPC에 IPAM 풀에서 할당된 CIDR이 포함된 최대 50개의 서브넷(CIDR 블록의 총 크기에 따라 우선순위 지정).
 - IPAM 풀에서 할당된 CIDR을 포함하는 최대 50개의 퍼블릭 IPv4 풀(총 CIDR 블록 크기에 따라 우선순위 지정).

각 규칙을 적용한 후 지표는 각 리소스 유형에 대해 동일한 지표 이름으로 집계되고 게시됩니다. 지표 이름 및 차원에 대한 자세한 내용은 아래를 참조하세요.

⚠ Important

각 리소스 유형, 주소 패밀리, 규칙 조합에 대해 고유한 제한이 있습니다. 각 한도의 기본값은 50입니다. AWS 일반 참조의 [AWS 서비스 할당량](#)에 설명된 대로 AWS 지원 센터에 문의하여 이러한 한도를 조정할 수 있습니다.

Example 예

IPAM이 IPv4 및 IPv6 CIDR을 모두 사용하여 2,500개의 VPC와 10,000개의 서브넷을 모니터링한다고 가정해 보겠습니다. IPAM은 다음과 같은 IP 사용률 지표를 게시합니다.

- 다음을 포함하여 VPC IPv4 IP 사용률에 대한 최대 150개의 지표:
 - IPv4 IP 사용률이 가장 높은 50개의 VPC
 - IPv4 사용률이 가장 낮은 50개의 VPC
 - IPAM 풀에서 할당된 IPv4 CIDR을 포함하는 최대 50개의 VPC
- 다음을 포함하여 VPC IPv6 사용률에 대한 최대 150개의 지표:
 - IPv6 IP 사용률이 가장 높은 50개의 VPC
 - IPv6 사용률이 가장 낮은 50개의 VPC
 - IPAM 풀에서 할당된 IPv6 CIDR을 포함하는 최대 50개의 VPC
- 다음을 포함하여 서브넷 IPv4 사용률에 대한 최대 150개의 지표:
 - IPv4 IP 사용률이 가장 높은 50개의 서브넷
 - IPv4 IP 사용률이 가장 낮은 50개의 서브넷
 - VPC에 IPAM 풀에서 할당된 IPv4 CIDR이 포함된 최대 50개의 서브넷

VPC 지표

VPC 지표 이름과 설명은 다음과 같습니다.

지표 이름	설명
VpcIPUsage	VPC 서브넷의 CIDR이 적용되는 총 IP를 VPC의 CIDR이 적용되는 총 IP로 나눈 값입니다. 이는 동일한 IPAM 범위의 모든 VPC CIDR에서 계산되며 IPv4 및 IPv6 CIDR에 대해서는 별도로 계산됩니다.

다음은 VPC 지표를 필터링하는 데 사용할 수 있는 차원입니다.

측정기준	설명
AddressFamily	리소스 CIDR(IPv4 또는 IPv6)의 IP 주소 패밀리입니다.
OwnerId	VPC 소유자의 ID입니다.
지역	VPC가 있는 AWS 리전입니다.
ScopeID	VPC가 속한 IPAM 범위의 ID입니다.
VpcID	VPC의 ID입니다.

서브넷 지표

서브넷 지표 이름과 설명은 다음과 같습니다.

지표 이름	설명
SubnetIPUsage	활성 IP의 수를 서브넷의 IPv4 CIDR에 있는 총 IP로 나눈 값입니다.

다음은 서브넷 지표를 필터링하는 데 사용할 수 있는 차원입니다.

측정기준	설명
AddressFamily	리소스 CIDR의 IP 주소 패밀리입니다(IPv4만 해당).
OwnerId	서브넷 소유자의 ID입니다.
지역	서브넷이 있는 AWS 리전입니다.
ScopeID	서브넷이 속한 IPAM 범위의 ID입니다.
SubnetID	서브넷의 ID입니다.
VpcID	서브넷이 속한 VPC의 ID입니다.

퍼블릭 IPv4 풀 지표

퍼블릭 IPv4 풀 지표 이름과 설명은 다음과 같습니다.

지표 이름	설명
PublicIPv4PoolIPUsage	퍼블릭 IPv4 풀의 EIP 수를 풀의 총 IP로 나눈 값입니다.

다음은 퍼블릭 IPv4 풀 지표를 필터링하는 데 사용할 수 있는 차원입니다.

측정기준	설명
OwnerID	퍼블릭 IPv4 풀 소유자의 ID입니다.
PublicIPv4PoolID	퍼블릭 IPv4 풀의 ID입니다.
지역	퍼블릭 IPv4 풀이 있는 AWS 리전입니다.
ScopeID	퍼블릭 IPv4 풀이 속한 IPAM 범위의 ID입니다.

퍼블릭 IP 인사이트 지표

[퍼블릭 IP 인사이트](#) 지표 이름 및 설명은 다음과 같습니다.

지표 이름	설명
AmazonOwnedElasticIPs	AWS 계정의 리소스에 프로비저닝했거나 할당한 Amazon 소유 탄력적 IP 주소의 수입입니다.
AssociatedAmazonOwnedElasticIPs	AWS 계정의 리소스와 연결한 Amazon 소유 탄력적 IP 주소의 수입입니다.
AssociatedBringYourOwnIPs	고유 IP 주소 가져오기(BYOIP)를 사용하여 AWS로 가져오고 AWS 계정의 리소스와 연결한 퍼블릭 IPv4 주소의 수입입니다.
BringYourOwnIPs	고유 IP 주소 가져오기(BYOIP)를 사용하여 AWS로 가져온 퍼블릭 IPv4 주소의 수입입니다.

지표 이름	설명
EC2PublicIPs	인스턴스가 기본 서브넷 또는 퍼블릭 IPv4 주소를 자동으로 할당하도록 구성된 서브넷으로 시작될 때 EC2 인스턴스에 할당된 퍼블릭 IPv4 주소의 수입입니다.
ServiceManagedBringingYourOwnIPs	AWS 서비스에서 프로비저닝하고 관리하는 고유 IP 주소 가져오기(BYOIP)를 사용하여 AWS로 가져온 퍼블릭 IPv4 주소의 수입입니다.
ServiceManagedIPs	AWS 서비스에서 프로비저닝하고 관리하는 퍼블릭 IPv4 주소의 수입입니다.
UnassociatedAmazonOwnedElasticIPs	AWS 계정의 리소스와 연결되지 않은 Amazon 소유 탄력적 IP 주소의 수입입니다.
UnassociatedBringYourOwnIPs	고유 IP 주소 가져오기(BYOIP)를 사용하여 AWS로 가져왔지만 AWS 계정의 리소스와 연결되지 않은 퍼블릭 IPv4 주소의 수입입니다.

다음은 퍼블릭 IP 인사이트 지표를 필터링하는 데 사용할 수 있는 차원입니다.

측정기준	설명
IpamId	IP 주소가 속한 IPAM의 ID입니다.
지역	퍼블릭 IP 주소가 위치한 AWS 리전입니다.

경보 생성을 위한 간편 도움말

IP 주소 사용률이 높은 리소스에 대한 Amazon CloudWatch 경보를 빠르게 생성하려면 CloudWatch 콘솔을 열고 지표, 모든 지표를 선택하고 쿼리 탭을 선택하고 네임스페이스 AWS/IPAM > VPC IP Usage Metrics, AWS/IPAM > Subnet IP Usage Metrics 또는 AWS/IPAM > Public IPv4 Pool IP Usage Metrics를 선택하고 지표 이름 MAX(VpcIPUsage), MAX(SubnetIPUsage) 또는 MAX(PublicIPv4PoolIPUsage)를 클릭하고 경보 생성을 선택합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 [Create alarms on Metrics Insights queries](#)를 참조하세요.

IP 주소 기록 보기

이 섹션의 단계를 따르면 IPAM 범위에서 IP 주소 또는 CIDR 기록을 볼 수 있습니다. 기록 데이터를 사용하여 네트워크 보안 및 라우팅 정책을 분석하고 감사할 수 있습니다. IPAM은 IP 주소 모니터링 데이터를 최대 3년 동안 자동으로 유지합니다.

IP 기록 데이터를 사용하여 다음 리소스 유형에 대한 IP 주소 또는 CIDR의 상태 변경을 검색할 수 있습니다.

- VPC
- VPC 서브넷
- 탄력적 IP 주소
- EC2 인스턴스
- 인스턴스에 연결된 EC2 네트워크 인터페이스

Important

IPAM은 Amazon EC2 인스턴스 또는 인스턴스에 연결된 EC2 네트워크 인터페이스를 모니터링하지 않지만 IP 기록 검색 기능을 사용하여 EC2 인스턴스 및 네트워크 인터페이스 CIDR에서 기록 데이터를 검색할 수 있습니다.

Note

- 한 IPAM 범위에서 다른 IPAM 범위로 리소스를 이동하는 경우 이전 기록 레코드가 종료되고 새 범위 아래 새 기록 레코드가 생성됩니다. 자세한 내용은 [범위 간에 VPC CIDR 이동](#) 단원을 참조하십시오.
- 리소스를 삭제하거나 IPAM에서 모니터링하지 않는 AWS 계정으로 이전하면 리소스와 관련된 새 기록이 표시되지 않으며 IPAM에서 리소스를 모니터링하지 않습니다. 그러나 리소스의 IP 주소는 계속 검색할 수 있습니다.
- [IPAM을 조직 외부 계정과 통합](#)의 경우 해당 계정에서 소유하는 모든 리소스 CIDR의 IP 주소 기록을 IPAM 소유자가 볼 수 있습니다.

AWS Management Console

CIDR 기록을 보려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 IP 기록 검색을 선택합니다.
3. IPv4 또는 IPv6 IP 주소 또는 CIDR을 입력합니다. 리소스에 대한 특정 CIDR이어야 합니다.
4. IPAM 범위 ID를 선택합니다.
5. 날짜/시간 범위를 선택합니다.
6. 결과를 VPC별로 필터링하려면 VPC ID를 입력합니다. CIDR이 여러 VPC에 나타나는 경우 이 옵션을 사용합니다.
7. 검색(Search)을 선택합니다.

Command line

이 섹션의 명령은 AWS CLI 참조 설명서로 연결됩니다. 이 설명서에서는 명령을 실행할 때 사용할 수 있는 옵션에 대한 자세한 설명을 제공합니다.

- CIDR 기록 보기: [get-ipam-address-history](#)

AWS CLI를 사용하여 IP 주소 사용을 분석하고 감사하는 방법의 예를 보려면 [자습서: AWS CLI를 사용하여 IP 주소 기록 보기](#)를 참조하세요.

검색 결과는 다음 열로 구성됩니다.

- 샘플링된 종료 시간(Sampled end time): IPAM 범위 내에서 리소스와 CIDR 연결의 샘플링된 종료 시간입니다. 변경 사항은 주기적인 스냅샷에서 선택되므로 종료 시간이 이 특정 시간 이전에 발생했을 수 있습니다.
- 샘플링된 시작 시간(Sampled start time): IPAM 범위 내에서 리소스와 CIDR 연결의 샘플링된 시작 시간입니다. 변경 사항은 주기적인 스냅샷에서 선택되므로 시작 시간이 이 특정 시간 이전에 발생했을 수 있습니다.

Example

샘플링된 시작 시간 및 샘플링된 종료 시간 아래에 표시되는 시간을 설명할 수 있도록 사용 사례 예를 살펴보겠습니다.

오후 2시에 CIDR 10.0.0.0/16을 사용하여 VPC가 생성되었습니다. 오후 3시에 CIDR 10.0.0.0/8을 사용하여 IPAM 및 IPAM 풀을 생성하고, 자동 가져오기 옵션을 선택하여 IPAM이 10.0.0.0/8 IP 주소 범위에 속하는 모든 CIDR을 검색하고 가져올 수 있도록 합니다. IPAM은 주기적 스냅샷에서 CIDR에 대한 변경 사항을 선택하기 때문에 오후 3시 05분까지 기존 VPC CIDR을 검색하지 않습니다. IP 기록 검색 기능을 사용하여 이 VPC의 ID를 검색하는 경우 VPC의 샘플링된 시작 시간은 오후 3시 5분입니다. 이 시작 시간은 IPAM이 VPC를 생성한 시점인 오후 2시가 아니라 VPC를 검색한 시점입니다. 이제 오후 5시에 VPC를 삭제하기로 결정한다고 가정합니다. VPC가 삭제되면 VPC에 할당된 CIDR 10.0.0.0/16이 IPAM 풀로 다시 재활용됩니다. IPAM은 오후 5시 05분에 주기적인 스냅샷을 찍고 변경 사항을 선택합니다. IP 기록 검색에서 이 VPC의 ID를 검색하는 경우 오후 5시 5분은 VPC가 삭제된 시점인 오후 5시가 아니라 VPC CIDR의 샘플링된 종료 시간입니다.

- 리소스 ID(Resource ID): 리소스가 CIDR과 연결되었을 때 생성된 ID입니다.
- 이름(Name): 리소스의 이름입니다(해당하는 경우).
- 규정 준수 상태(Compliance status): CIDR의 규정 준수 상태입니다.
 - 규정 준수(Compliant): 관리형 리소스는 IPAM 풀의 할당 규칙을 준수합니다.
 - 규정 미준수(Noncompliant): 리소스 CIDR은 IPAM 풀의 할당 규칙 하나 이상을 준수하지 않습니다.

Example

VPC에 IPAM 풀의 넷마스크 길이 파라미터를 충족하지 않는 CIDR이 있거나 리소스가 IPAM 풀과 동일한 AWS 리전에 있지 않은 경우 비준수 플래그로 지정됩니다.

- 비관리형(Unmanaged): 리소스에는 IPAM 풀에서 할당된 CIDR이 있으며 IPAM에서 잠재적 CIDR 겹침 및 풀 할당 규칙 관련 규정 준수에 대해 모니터링하고 있지 않습니다. CIDR은 겹침에 대해 모니터링됩니다.
- 무시됨(Ignored): 관리형 리소스가 모니터링에서 면제되도록 선택되었습니다. 무시된 리소스는 겹침 또는 할당 규칙 관련 규정 준수로 평가되지 않습니다. 리소스를 무시하도록 선택하면 IPAM 풀에서 해당 리소스에 할당된 공간이 풀로 반환되며, 자동 가져오기를 통해(자동 가져오기 할당 규칙이 풀에 설정된 경우) 리소스를 다시 가져오지 않습니다.
- -: 이 리소스는 IPAM이 모니터링하거나 관리할 수 있는 리소스 유형 중 하나가 아닙니다.
- 겹침 상태(Overlap status): CIDR의 겹침 상태입니다.
 - 비겹침(Nonoverlapping): 리소스 CIDR이 동일한 범위의 다른 CIDR과 겹치지 않습니다.
 - 겹침(Overlapping): 리소스 CIDR이 동일한 범위의 다른 CIDR과 겹칩니다. 리소스 CIDR이 겹치는 경우 수동 할당과 겹칠 수 있습니다.

- 무시됨(Ignored): 관리형 리소스가 모니터링에서 면제되도록 선택되었습니다. IPAM은 무시된 리소스를 겹침 또는 할당 규칙 관련 규정 준수로 평가하지 않습니다. 리소스를 무시하도록 선택하면 IPAM 풀에서 해당 리소스에 할당된 공간이 풀로 반환되며, 자동 가져오기를 통해(자동 가져오기 할당 규칙이 풀에 설정된 경우) 리소스를 다시 가져오지 않습니다.
- -: 이 리소스는 IPAM이 모니터링하거나 관리할 수 있는 리소스 유형 중 하나가 아닙니다.
- 리소스 유형(Resource type)
 - vpc: CIDR은 VPC와 연결되어 있습니다.
 - 서브넷(subnet): CIDR은 VPC 서브넷과 연결되어 있습니다.
 - eip: CIDR은 탄력적 IP 주소와 연결되어 있습니다.
 - 인스턴스(instance): CIDR은 EC2 인스턴스와 연결되어 있습니다.
 - network-interface: CIDR은 네트워크 인터페이스와 연결되어 있습니다.
- VPC ID: 이 리소스가 속한 VPC ID입니다(해당하는 경우).
- 리전(Region): 이 리소스의 AWS 리전입니다.
- 소유자 ID(Owner ID): 이 리소스를 만든 사용자의 AWS 계정 ID입니다(해당하는 경우).

퍼블릭 IP 인사이트 보기

퍼블릭 IPv4 주소는 인터넷에서 라우팅할 수 있는 IPv4 주소입니다. 퍼블릭 IPv4 주소는 인터넷에서 IPv4를 통해 리소스에 직접 연결하는 데 필요합니다.

Note

AWS에서는 탄력적 IP 주소 및 실행 중인 인스턴스에 연결된 퍼블릭 IPv4 주소를 포함하여 모든 퍼블릭 IPv4 주소에 요금을 부과합니다. 자세한 내용은 [Amazon VPC 요금 페이지](#)의 퍼블릭 IPv4 주소 탭을 참조하세요.

다음 퍼블릭 IPv4 주소 유형에 대한 인사이트를 볼 수 있습니다.

- 탄력적 IP 주소(EIP): EC2 인스턴스, 탄력적 네트워크 인터페이스 또는 AWS 리소스와 연결할 수 있는 Amazon에서 제공하는 정적 퍼블릭 IPv4 주소입니다.
- EC2 퍼블릭 IPv4 주소: Amazon에서 EC2 인스턴스에 할당한 퍼블릭 IPv4 주소입니다(EC2 인스턴스가 기본 서브넷에서 시작되거나 인스턴스가 퍼블릭 IPv4 주소를 자동으로 할당하도록 구성된 서브넷에서 시작되는 경우).

- BYOIPv4 주소: [고유 IP 주소 가져오기\(BYOIP\)](#)를 사용하여 AWS로 가져온 IPv4 주소 범위의 퍼블릭 IPv4 주소입니다.
- 서비스 관리형 IPv4 주소: 퍼블릭 IPv4 주소는 AWS 리소스에 자동으로 프로비저닝되고 AWS 서비스에 의해 관리됩니다. 예를 들어 Amazon ECS, Amazon RDS 또는 Amazon WorkSpaces의 퍼블릭 IPv4 주소입니다.

퍼블릭 IP 인사이트를 사용하여 다음을 확인할 수 있습니다.

- IPAM이 [AWS Organization의 계정과 통합된 경우](#) 전체 AWS Organization에 대해 모든 AWS 리전에서 서비스 사용하는 모든 퍼블릭 IPv4 주소를 볼 수 있습니다.
- IPAM이 [단일 계정으로 통합된 경우](#) 계정의 모든 AWS 리전에서 서비스 사용하는 모든 퍼블릭 IPv4 주소를 볼 수 있습니다.

퍼블릭 IP 인사이트는 리전 전체의 서비스에서 사용되는 모든 퍼블릭 IPv4 주소를 보여 줍니다. 이러한 인사이트를 사용하여 퍼블릭 IPv4 주소 사용을 식별하고 사용하지 않는 탄력적 IP 주소를 해제하기 위한 권장 사항을 볼 수 있습니다.

- 퍼블릭 IP 유형: 유형별로 구성된 퍼블릭 IPv4 주소의 수입입니다.
 - Amazon 소유 EIP: 프로비저닝했거나 AWS 계정의 리소스에 할당된 탄력적 IP 주소입니다.
 - EC2 퍼블릭 IP: 인스턴스가 기본 서브넷 또는 퍼블릭 IPv4 주소를 자동으로 할당하도록 구성된 서브넷으로 시작될 때 EC2 인스턴스에 할당된 퍼블릭 IPv4 주소입니다.
 - BYOIP: 고유 IP 주소 가져오기(BYOIP)를 사용하여 AWS에 가져온 퍼블릭 IPv4 주소입니다.
 - 서비스 관리형 IP: AWS 서비스에서 프로비저닝하고 관리하는 퍼블릭 IPv4 주소입니다.
- EIP 사용량: 사용 방식에 따라 구성된 탄력적 IP 주소의 수입입니다.
 - 연결된 Amazon 소유 EIP: AWS 계정에서 프로비저닝하고 EC2 인스턴스, 네트워크 인터페이스 또는 AWS 리소스와 연결한 탄력적 IP 주소입니다.
 - 연결된 BYOIP: 네트워크 인터페이스와 연결한 BYOIP를 사용하여 AWS로 가져온 퍼블릭 IPv4 주소입니다.
 - 연결되지 않은 Amazon 소유 EIP: AWS 계정에 프로비저닝했지만 네트워크 인터페이스와 연결하지 않은 탄력적 IP 주소입니다.
 - 연결되지 않은 BYOIP: BYOIP를 사용하여 AWS로 가져왔지만 네트워크 인터페이스와 연결되지 않은 퍼블릭 IPv4 주소입니다.
- 퍼블릭 IP 주소: 퍼블릭 IPv4 주소 및 해당 속성의 표입니다.
 - IP 주소: 퍼블릭 IPv4 주소입니다.

- 연결됨: 주소가 EC2 인스턴스, 네트워크 인터페이스 또는 AWS 리소스와 연결되어 있는지 여부입니다.
- 연결됨: 퍼블릭 IPv4 주소는 EC2 인스턴스, 네트워크 인터페이스 또는 AWS 리소스와 연결되어 있습니다.
- 연결되지 않음: 퍼블릭 IPv4 주소가 어떤 리소스에도 연결되지 않았으며 AWS 계정에서 유휴 상태입니다.
- 주소 유형: IP 주소 유형입니다.
 - Amazon 소유 EIP: 퍼블릭 IPv4 주소는 탄력적 IP 주소입니다.
 - BYOIP: 퍼블릭 IPv4 주소는 BYOIP를 사용하여 AWS로 가져왔습니다.
 - EC2 퍼블릭 IP: 퍼블릭 IPv4 주소는 EC2 인스턴스에 자동으로 할당되었습니다.
 - 서비스 관리형 BYOIP: 고유 IP 주소 가져오기(BYOIP)를 사용하여 퍼블릭 IPv4 주소를 AWS로 가져왔습니다.
 - 서비스 관리형 IP: 퍼블릭 IPv4 주소가 프로비저닝되었으며 AWS 서비스에서 관리합니다.
- 서비스: IP 주소와 연결된 서비스입니다.
 - AGAAWS Global Accelerator: 입니다. [사용자 지정 라우팅 액셀러레이터](#)를 사용하는 경우에는 퍼블릭 IP가 목록에 표시되지 않습니다. 이러한 퍼블릭 IP를 보려면 [사용자 지정 라우팅 액셀러레이터 보기](#)를 참조하세요.
 - 데이터베이스 마이그레이션 서비스: AWS Database Migration Service(DMS) 복제 인스턴스입니다.
 - Redshift: Amazon Redshift 클러스터입니다.
 - RDS: Amazon 관계형 데이터베이스 서비스(RDS) 인스턴스입니다.
 - 로드 밸런서(EC2): Application Load Balancer 또는 Network Load Balancer입니다.
 - NAT 게이트웨이(VPC): Amazon VPC 퍼블릭 NAT 게이트웨이입니다.
 - 사이트 간 VPN: AWS Site-to-Site VPN 가상 프라이빗 게이트웨이입니다.
 - 기타: 현재 식별할 수 없는 기타 서비스입니다.
- 이름(EIP ID): 이 퍼블릭 IPv4 주소가 탄력적 IP 주소 할당인 경우 이는 EIP 할당의 이름 및 ID입니다.
- 네트워크 인터페이스 ID: 이 퍼블릭 IPv4 주소가 네트워크 인터페이스와 연결된 경우 이는 네트워크 인터페이스의 ID입니다.
- 인스턴스 ID: 이 퍼블릭 IPv4 주소가 EC2 인스턴스와 연결된 경우 이는 인스턴스 ID입니다.
- 보안 그룹: 이 퍼블릭 IPv4 주소가 EC2 인스턴스와 연결된 경우 이는 인스턴스에 할당된 보안 그룹의 이름 및 ID입니다.

- 퍼블릭 IPv4 풀: Amazon에서 소유하고 관리하는 IP 주소 풀의 탄력적 IP 주소인 경우 값은 "-"입니다. 사용자가 소유하고 있고 (BYOIP를 사용하여) Amazon으로 가져온 IP 주소 범위의 탄력적 IP 주소인 경우, 이 값은 공용 IPv4 풀 ID입니다.
- 네트워크 경계 그룹: IP 주소가 광고되는 경우 이는 IP 주소가 광고된 AWS 리전입니다.
- 소유자 ID: 리소스 소유자의 AWS 계정 번호입니다.
- 샘플 시간: 마지막으로 성공한 리소스 검색 시간입니다.
- 리소스 검색 ID: 이 퍼블릭 IPv4 주소를 검색한 리소스 검색의 ID입니다.
- 서비스 리소스: 리소스 ARN 또는 ID입니다.

탄력적 IP 주소가 계정에 할당되었지만 네트워크 인터페이스와 연결되지 않은 경우 계정에 연결되지 않은 EIP가 있으므로 해제해야 한다는 것을 알리는 배너가 나타납니다.

Important

퍼블릭 IP 인사이트는 최근에 업데이트되었습니다. `GetIpamDiscoveredPublicAddresses`를 호출할 권한이 없는 것과 관련된 오류가 표시되는 경우 사용자와 공유된 리소스 검색에 연결된 관리 권한을 업데이트해야 합니다. 리소스 검색을 생성한 사람에게 연락하여 관리 권한 `AWSRAMPermissionIpamResourceDiscovery`를 기본 버전으로 업데이트해 달라고 요청하세요. 자세한 내용은 AWS RAM 사용 설명서의 [리소스 공유 업데이트](#)를 참조하세요.

AWS Management Console

퍼블릭 IP 주소 인사이트를 보려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 퍼블릭 IP 인사이트를 선택합니다.
3. 퍼블릭 IP 주소에 대한 세부 정보를 보려면 IP 주소를 클릭하여 선택합니다.
4. IP 주소에 대한 다음 정보를 확인하세요.
 - 세부 정보: 주소 유형 및 서비스와 같은 기본 퍼블릭 IP 인사이트 창의 열에 표시되는 동일한 정보입니다.
 - 인바운드 보안 그룹 규칙: 이 IP 주소가 EC2 인스턴스와 연결된 경우 이는 인스턴스로의 인바운드 트래픽을 제어하는 보안 그룹 규칙입니다.
 - 아웃바운드 보안 그룹 규칙: 이 IP 주소가 EC2 인스턴스와 연결된 경우 이는 인스턴스에서 오는 아웃바운드 트래픽을 제어하는 보안 그룹 규칙입니다.

- 태그: AWS 리소스 구성을 위한 메타데이터 역할을 하는 키 및 값 쌍입니다.

Command line

다음 명령을 사용하여 IPAM에서 발견한 퍼블릭 IP 주소를 가져오세요. [get-ipam-discovered-public-address](#)

Amazon VPC IP Address Manager 자습서

다음 자습서는 AWS CLI를 사용하여 일반적인 IPAM 작업을 수행하는 방법을 보여줍니다. AWS CLI를 가져오려면 [IPAM 액세스](#) 섹션을 참조하세요. 이 자습서에서 언급한 IPAM 개념에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.

내용

- [자습서: 콘솔을 사용하여 IPAM 및 풀 생성](#)
- [자습서: AWS CLI를 사용하여 IPAM 및 풀 생성](#)
- [자습서: AWS CLI를 사용하여 IP 주소 기록 보기](#)
- [자습서: IPAM으로 ASN 가져오기](#)
- [자습서: IPAM으로 IP 주소 가져오기](#)
- [자습서: IPAM으로 BYOIP IPv4 CIDR 전송](#)
- [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)

자습서: 콘솔을 사용하여 IPAM 및 풀 생성

이 자습서에서는 IPAM을 생성하고, AWS Organizations와 통합하고, IP 주소 풀을 생성하고, IPAM 풀에서 CIDR을 사용하여 VPC를 생성합니다.

이 자습서에서는 IPAM을 사용하여 다양한 개발 요구 사항에 따라 IP 주소 스페이스를 구성하는 방법을 보여줍니다. 이 자습서를 완료하면 사전 프로덕션 리소스를 위한 IP 주소 풀을 하나 갖게 됩니다. 그런 다음 라우팅 및 보안 요구 사항에 따라 프로덕션 리소스를 위한 풀 등의 다른 풀을 생성할 수 있습니다.

IPAM을 단일 사용자로 사용할 수 있지만 AWS Organizations와 통합하면 조직 내 계정 전체의 IP 주소를 관리할 수 있습니다. 이 자습서에서는 IPAM을 조직의 계정과 통합하는 방법을 다룹니다. [IPAM을 조직 외부 계정과 통합](#) 방법은 다루지 않습니다.

Note

이 자습서에서는 특정 방식으로 IPAM 리소스의 이름을 지정하고, 특정 리전에서 IPAM 리소스를 생성하고, 풀에 특정 IP 주소 CIDR 범위를 사용하도록 지시합니다. 이는 IPAM에서 사용할 수 있는 선택 사항을 간소화하고 IPAM을 빠르게 시작할 수 있도록 하기 위한 것입니다. 이 자습서를 완료한 후에는 새 IPAM을 생성하고 다르게 구성할 수 있습니다.

내용

- [필수 조건](#)
- [AWS Organizations가 IPAM과 통합되는 방식](#)
- [1단계: IPAM 관리자 위임](#)
- [2단계: IPAM 생성](#)
- [3단계: 최상위 IPAM 풀 생성](#)
- [4단계: 리전 IPAM 풀 생성](#)
- [5단계: 사전 프로덕션 개발 풀 생성](#)
- [6단계: IPAM 풀 공유](#)
- [7단계: IPAM 풀에서 할당된 CIDR을 사용하여 VPC 생성](#)
- [8단계: 정리](#)

필수 조건

시작하기 전에 하나 이상의 멤버 계정으로 AWS Organizations 계정을 설정해야 합니다. 방법 지침은 [AWS Organizations 사용 설명서](#)의 조직 생성 및 관리를 참조하세요.

AWS Organizations가 IPAM과 통합되는 방식

이 섹션에서는 이 자습서에서 사용하는 AWS Organizations 계정의 예를 보여줍니다. 이 자습서에서 IPAM과 통합할 때 사용하는 조직에는 세 가지 계정이 있습니다.

- IPAM 콘솔에 로그인하고 IPAM 관리자를 위임하기 위한 관리 계정(다음 이미지에서는 example-management-account). 조직의 관리 계정을 IPAM 관리자로 사용할 수 없습니다.
- IPAM 관리자 계정인 멤버 계정(다음 이미지에서는 example-member-account-1). IPAM 관리자 계정은 IPAM을 생성하고 이를 사용하여 조직 전체의 IP 주소 사용을 관리하고 모니터링하는 일을 담당합니다. 조직의 모든 멤버 계정을 IPAM 관리자로 위임할 수 있습니다.
- 개발자 계정인 멤버 계정(다음 이미지에서는 example-member-account-2). 이 계정은 IPAM 풀에서 할당된 CIDR을 사용하여 VPC를 생성합니다.

The screenshot shows the AWS Organizations console interface. On the left is a navigation sidebar with 'AWS Organizations' and 'AWS accounts' selected. The main content area is titled 'AWS accounts' and includes an 'Add an AWS account' button. Below this is a search bar and a view toggle set to 'Hierarchy'. The 'Organizational structure' section shows a tree view: Root (r-fssg) contains Organizational-unit-1 (ou-fssg-ycy89843), which contains Organizational-unit-1a (ou-fssg-q5brfv9c). Under Organizational-unit-1a, there are three accounts: example-member-account-1, example-member-account-2, and example-management-account (management account). Each account entry shows its ID, email address, and the date it was joined (2022/12/28).

계정 외에도 개발자 계정으로 사용할 멤버 계정이 포함된 조직 구성 단위의 ID(앞의 이미지에서 ou-fssg-q5brfv9c)가 필요합니다. 이후 단계에서 IPAM 풀을 공유할 때 이 OU와 공유할 수 있도록 이 ID가 필요합니다.

Note

관리 계정과 멤버 계정 등의 AWS Organizations 계정 유형에 대한 자세한 내용은 [AWS Organizations 용어 및 개념](#)을 참조하세요.

1단계: IPAM 관리자 위임

이 단계에서는 AWS Organizations 멤버 계정을 IPAM 관리자로 위임합니다. IPAM 관리자를 위임하면 각 AWS Organizations 멤버 계정에 [서비스 연결 역할](#)이 자동으로 생성됩니다. IPAM은 각 멤버 계정에서 서비스 연결 역할을 수임하여 이러한 계정의 IP 주소 사용을 모니터링합니다. 그러면 조직 단위에 관계없이 리소스와 해당 CIDR을 검색할 수 있습니다.

필수 AWS Identity and Access Management(IAM) 권한이 없으면 이 단계를 완료할 수 없습니다. 자세한 내용은 [AWS Organization에서 계정과 IPAM 통합](#) 단원을 참조하십시오.

IPAM 관리자 계정 위임

1. AWS Organizations 관리 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. AWS 관리 콘솔에서 IPAM에서 작업하려는 AWS 리전을 선택합니다.
3. 탐색 창에서 조직 설정을 선택합니다.
4. 위임을 선택합니다. 위임 옵션은 콘솔에 AWS Organizations 관리 계정으로 로그인한 경우에만 사용할 수 있습니다.
5. 조직 멤버 계정의 AWS 계정 ID를 입력합니다. IPAM 관리자는 관리 계정이 아닌 AWS Organizations 멤버 계정이어야 합니다.

The screenshot shows the 'Settings' page for Amazon VPC IP Address Manager. The breadcrumb trail is 'Amazon VPC IP Address Manager > Settings > Edit'. The main heading is 'Settings' with an 'Info' link. Below this, there is a section titled 'Delegated administrator'. Under this section, there are two sub-sections: 'Delegated administrator account' and 'Service access'. The 'Delegated administrator account' section includes a text input field with the placeholder text 'Enter an account ID for the IPAM administrator'. The 'Service access' section includes a 'View details' button. At the bottom right of the settings area, there are two buttons: 'Cancel' and 'Save changes'.

6. Save changes(변경 사항 저장)를 선택합니다. 위임된 관리자 정보는 멤버 계정과 관련된 세부 정보로 채워집니다.

2단계: IPAM 생성

이 단계에서는 IPAM을 생성합니다. IPAM을 생성하면 IPAM이 자동으로 IPAM에 대한 두 가지 범위, 즉 모든 프라이빗 스페이스를 위한 프라이빗 범위와 모든 퍼블릭 스페이스를 위한 퍼블릭 범위를 생성합

니다. 풀 및 할당과 함께 범위는 IPAM의 핵심 구성 요소입니다. 자세한 내용은 [IPAM 작동 방식](#) 단원을 참조하십시오.

IPAM을 생성하려면

1. [이전 단계](#)에서 IPAM 관리자로 위임된 AWS Organizations 멤버 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. AWS 관리 콘솔에서 IPAM을 생성하려는 AWS 리전을 선택합니다. 기본 작업 리전에서 IPAM을 생성합니다.
3. 서비스 홈 페이지에서 IPAM 생성(Create IPAM)을 선택합니다.
4. Amazon VPC IP 주소 관리자가 소스 계정의 데이터를 IPAM 위임 계정으로 복제하도록 허용 (Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account)을 선택합니다. 이 옵션을 선택하지 않은 경우 IPAM을 생성할 수 없습니다.

Create IPAM Info

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

Allow data replication Info

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

Allow Amazon VPC IP Address Manager to replicate data from the member account(s) into the Amazon VPC IP Address Manager delegate account.
You must select this checkbox to continue to create an IPAM.

5. 운영 리전에서 이 IPAM이 리소스를 관리하고 검색할 수 있는 AWS 리전을 선택합니다. IPAM을 생성하는 AWS 리전은 자동으로 운영 리전 중 하나로 선택됩니다. 이 자습서에서는 IPAM의 홈 리전이 us-east-1이므로 추가 운영 리전으로 us-west-1과 us-west-2를 선택합니다. 운영 리전을 잊어버린 경우 나중에 IPAM 설정을 편집하고 리전을 추가하거나 편집할 수 있습니다.

IPAM settings [Info](#)**Name tag - optional**

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

Description - optional

Write a brief description for the IPAM.

Operating Regions

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

**Default resources will be created**

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

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

6. IPAM 생성(Create IPAM)을 선택합니다.

☑ Successfully created IPAM ipam-005f921c17ebd5107
✕

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

DemoIPAM (ipam-005f921c17ebd5107) Info

Edit Delete

IPAM details

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

Operating Regions

Associated discoveries

Tags

Operating Regions (3) Info

< 1 >

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

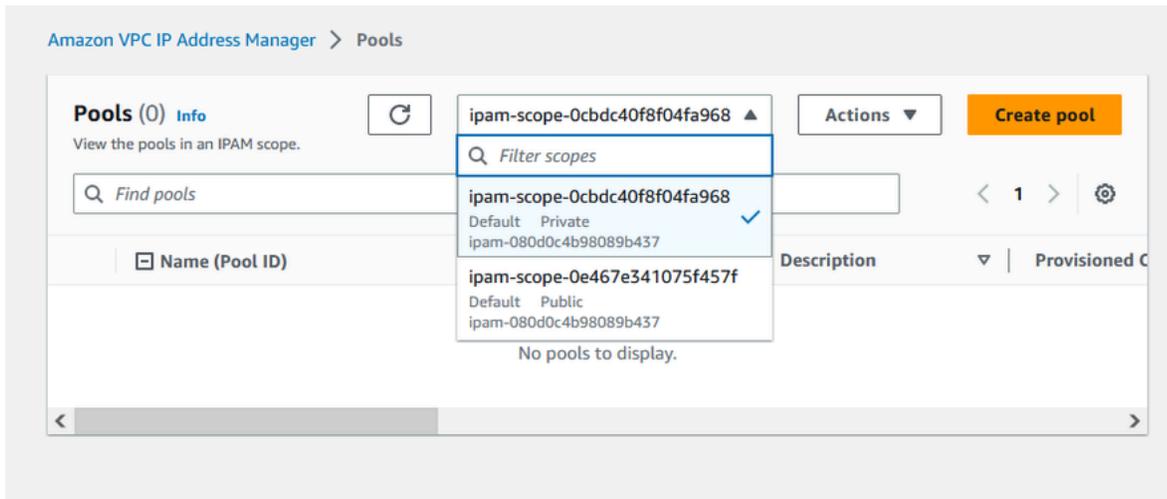
3단계: 최상위 IPAM 풀 생성

이 자습서에서는 최상위 IPAM 풀부터 시작하여 풀 계층 구조를 생성합니다. 이후 단계에서는 리전 풀 중 하나에 한 쌍의 리전 풀과 사전 프로덕션 개발 풀을 생성합니다.

IPAM으로 구축할 수 있는 풀 계층 구조에 대한 자세한 내용은 [IPAM 풀 계획의 예](#) 섹션을 참조하세요.

최상위 풀 생성

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택합니다.



4. 풀 생성을 선택합니다.
5. IPAM 범위에서 프라이빗 범위를 선택한 상태로 둡니다.
6. (선택 사항) 풀에 대한 이름 태그와 설명(예: 'Global pool')을 추가합니다.
7. 소스에서 IPAM 범위를 선택합니다. 최상위 풀이므로 소스 풀이 없습니다.
8. 주소 패밀리(Address family)에서 IPv4를 선택합니다.
9. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
10. 로캘(Locale)의 경우 없음(None)을 선택합니다. 로캘은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 이 자습서의 다음 섹션에서 생성할 리전 풀의 로캘을 설정합니다.

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

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

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

Description - optional
Write a brief description for the pool.

Pool hierarchy [Info](#)

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

Address family
Select the address family for this pool.

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

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

11. 풀에 대해 프로비저닝할 CIDR을 선택합니다. 이 예제에서는 10.0.0.0/16을 프로비저닝합니다.

CIDRs to provision [Info](#)

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

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/16	65K IPs	Remove
<input type="button" value="←"/> <input type="button" value="→"/> <input type="button" value="↑"/> <input type="button" value="↓"/>		

Add new CIDR

12. 이 풀의 할당 규칙 설정 구성을 비활성화된 상태로 둡니다. 이는 최상위 수준 풀이며, 이 풀에서 직접 VPC에 CIDR을 할당하지 않습니다. 대신 이 풀에서 생성하는 하위 풀에서 CIDR을 할당합니다.

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

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

Configure this pool's allocation rule settings

13. 풀 생성을 선택합니다. 풀이 생성되고 CIDR이 프로비저닝 보류 중 상태입니다.

Sent request to provision 10.0.0.0/16

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

Global pool (ipam-pool-06fb4cace4bc1e551)

Pool summary

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

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

CIDRs (1) Info

Deprovision CIDRs | Provision CIDR

Filter CIDRs

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

14. 다음 단계로 이동하기 전에 프로비저닝됨 상태가 될 때까지 기다립니다.

✓ Sent request to provision 10.0.0.0/16

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

Global pool (ipam-pool-06fb4cace4bc1e551)

Pool summary

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

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

CIDRs (1) Info

Deprovision CIDRs | Provision CIDR

Filter CIDRs

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

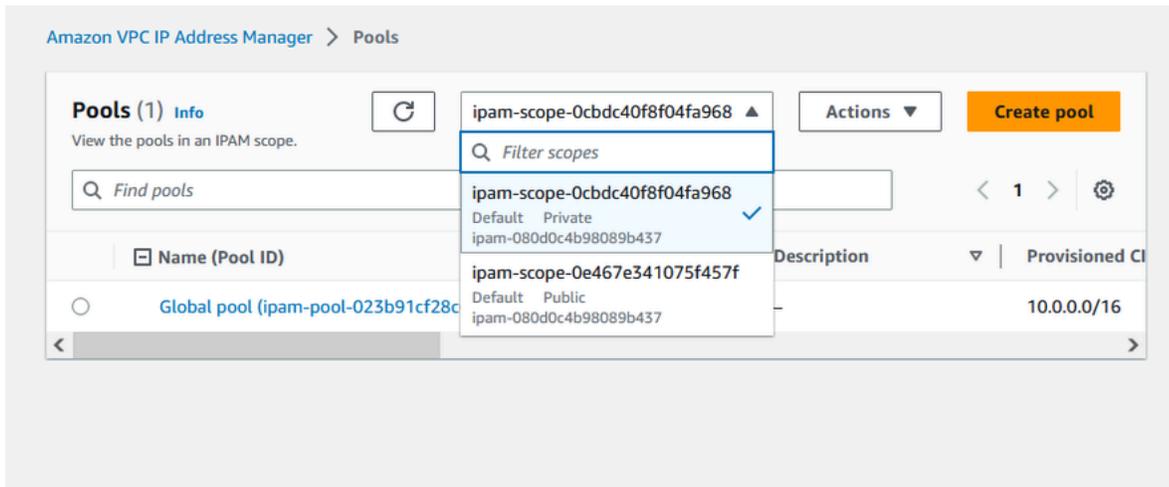
최상위 수준 풀을 생성했으므로 이제 us-west-1과 us-west-2에 리전 풀을 생성합니다.

4단계: 리전 IPAM 풀 생성

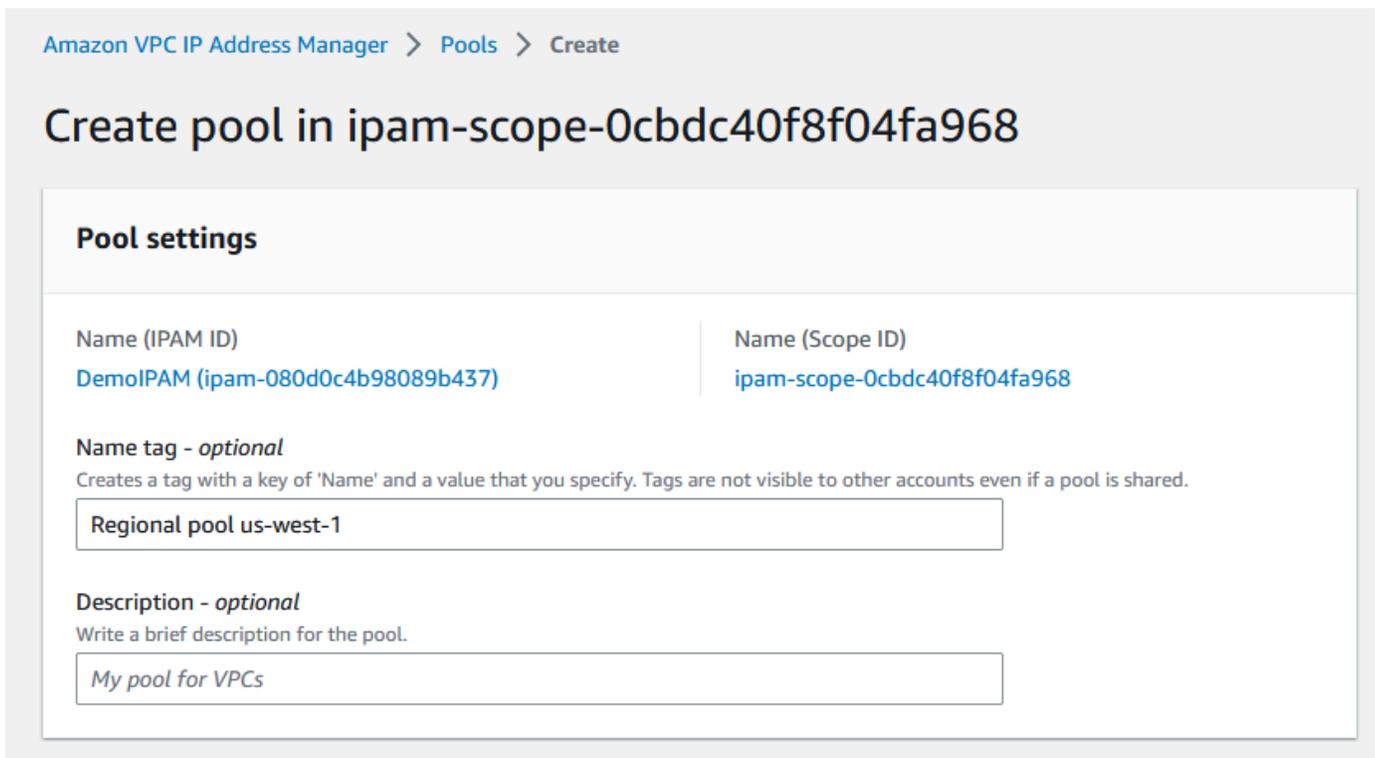
이 섹션에서는 2개의 리전 풀을 사용하여 IP 주소를 구성하는 방법을 설명합니다. 이 자습서에서는 [예제 IPAM 풀 플랜](#) 중 하나를 따르고 조직의 멤버 계정에서 VPC에 CIDR을 할당하는 데 사용할 수 있는 2개의 리전 풀을 생성합니다.

리전 풀 생성

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택합니다.



4. 풀 생성을 선택합니다.
5. IPAM 범위에서 프라이빗 범위를 선택한 상태로 둡니다.
6. (선택 사항) 풀에 대한 이름 태그와 설명(예: Regional pool us-west-1)을 추가합니다.



7. 소스에서 IPAM 풀을 선택하고 [3단계: 최상위 IPAM 풀 생성](#)에서 생성한 최상위 풀('Global pool')을 선택합니다. 그런 다음 로컬에서 us-west-1을 선택합니다.

Pool hierarchy [Info](#)

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

Global pool (ipam-pool-023b91cf28c61a0fb) ▼

▼ **Source pool summary**

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

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

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

US West (N. California) - us-west-1 ▼

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

8. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
9. 프로비저닝할 CIDR에서 10.0.0.0/18을 입력합니다. 그러면 이 풀에 약 16,000개의 사용 가능한 IP 주소가 제공됩니다.

CIDRs to provision [Info](#)

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

IP space visualization (source pool)

■ Zoom ■ Overlapping ■ New allocation ■ Allocated ■ Available

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

**CIDR**

Enter a CIDR to be provisioned.

10.0.0.0/18 16K IPs Remove

< > ^ v

Add specific CIDR

Add CIDR by size

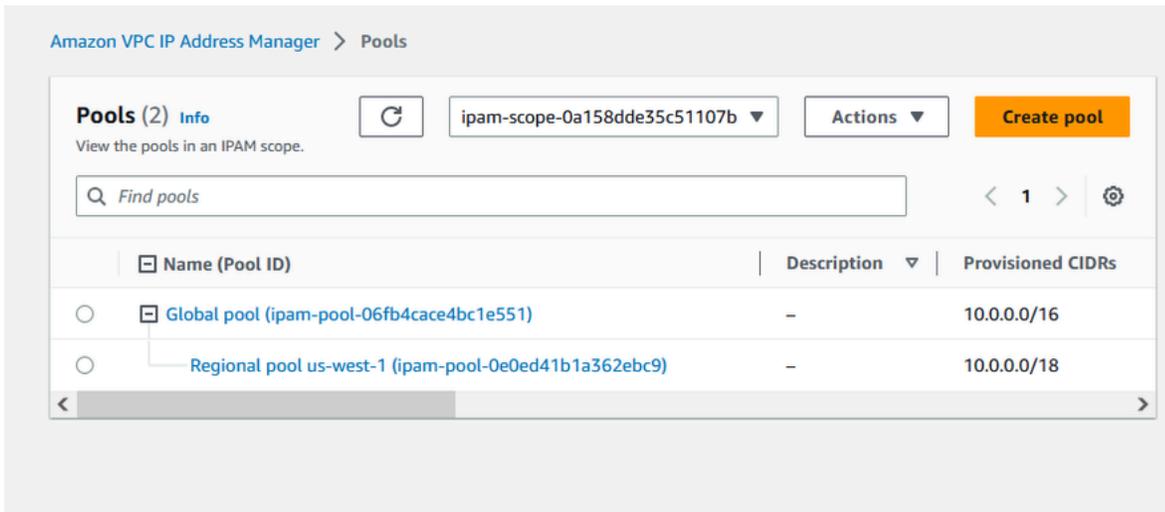
10. 이 풀의 할당 규칙 설정 구성을 비활성화된 상태로 둡니다. 이 풀에서 직접 VPC에 CIDR을 할당하지 않습니다. 대신 이 풀에서 생성하는 하위 풀에서 CIDR을 할당합니다.

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

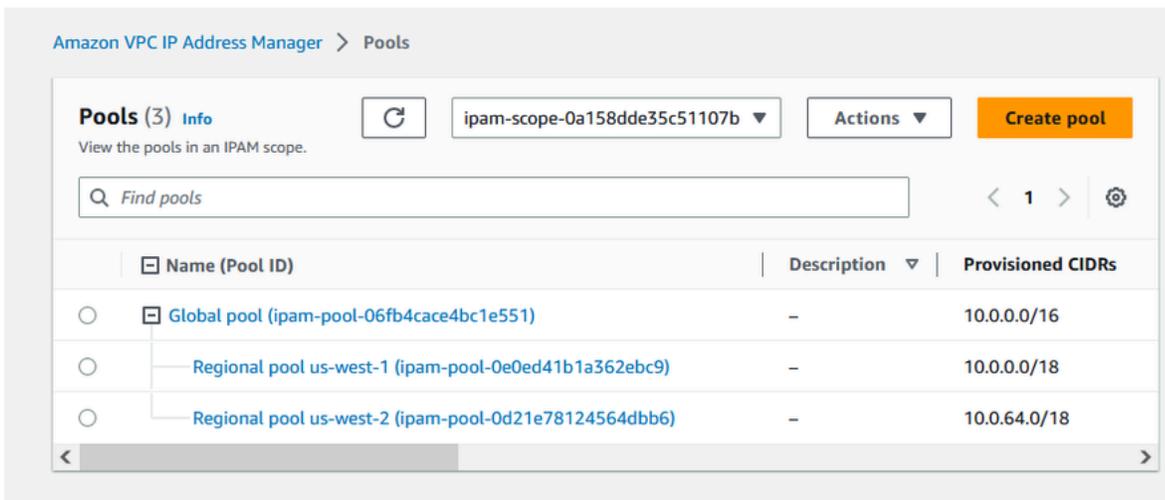
We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize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

Configure this pool's allocation rule settings

11. 풀 생성을 선택합니다.
12. 풀 뷰로 돌아가 생성한 IPAM 풀의 계층 구조를 봅니다.



13. 이 섹션의 단계를 반복하고 CIDR 10.0.64.0/18이 프로비저닝된 us-west-2 로컬에 두 번째 리전 풀을 생성합니다. 해당 프로세스를 완료하면 계층 구조에 다음과 비슷한 3개의 풀이 생깁니다.



5단계: 사전 프로덕션 개발 풀 생성

이 섹션의 단계에 따라 리전 풀 중 하나 내에 사전 프로덕션 리소스에 대한 개발 풀을 생성합니다.

사전 프로덕션 개발 풀 생성

- 이전 섹션에서와 동일한 방식으로 IPAM 관리자 계정을 사용하여 Pre-prod pool이라는 풀을 생성합니다. 단, 이번에는 Regional pool us-west-1을 소스 풀로 사용합니다.

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

Name (IPAM ID)

DemoIPAM (ipam-080d0c4b98089b437)

Name (Scope ID)

ipam-scope-0cbdc40f8f04fa968

Name tag - *optional*

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

Pre-prod pool

Description - *optional*

Write a brief description for the pool.

My pool for VPCs

Pool hierarchy [Info](#)

Source pool

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

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

▼ Source pool summary

Name (Pool ID)

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

Provisioned CIDRs

10.0.0.0/18

Description

-

Locale

us-west-1

2. 프로비저닝할 CIDR을 10.0.0.0/20으로 지정합니다. 그러면 이 풀에 약 4,000개의 IP 주소가 제공됩니다.

CIDRs to provision [Info](#)

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

IP space visualization (source pool)

■ Zoom
 ■ Overlapping
 ■ New allocation
 ■ Allocated
 ■ Available

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

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/20 4K IPs Remove

< > ^ v

Add specific CIDR
Add CIDR by size

3. 이 풀의 할당 규칙 설정 구성 옵션을 전환합니다. 다음을 따릅니다.

1. CIDR 관리 아래의 검색된 리소스 자동 가져오기에서 기본값인 허용 안 함 옵션을 선택된 상태로 둡니다. 이 옵션을 사용하면 IPAM이 풀의 로컬에서 검색한 리소스 CIDR을 자동으로 가져올 수 있습니다. 이 옵션에 대한 자세한 설명은 이 자습서의 범위를 벗어나지만 [최상위 IPv4 풀 생성](#)에서 옵션에 대한 자세한 내용을 읽을 수 있습니다.
2. 넷마스크 규정 준수 아래에서 최소, 기본 및 최대 넷마스크 길이로 /24를 선택합니다. 이 옵션에 대한 자세한 설명은 이 자습서의 범위를 벗어나지만 [최상위 IPv4 풀 생성](#)에서 옵션에 대한 자세한 내용을 읽을 수 있습니다. 중요한 점은 나중에 이 풀의 CIDR을 사용하여 생성하는 VPC가 여기에서 설정한 내용에 따라 /24로 제한된다는 것입니다.
3. 태그 규정 준수 아래에서 environment/pre-prod를 입력합니다. 이 태그는 VPC가 풀에서 스페이스를 할당하는 데 필요합니다. 이것이 어떻게 작동하는지 나중에 보여드리겠습니다.

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



AWS best practice

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

Configure this pool's allocation rule settings

CIDR management

Automatically import discovered resources

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

- Allow automatic import
- Don't allow

Netmask compliancy

Minimum netmask length

The minimum netmask length for allocating resources within the pool.

/24 (256 IPs)

Default netmask length

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

/24 (256 IPs)

Maximum netmask length

The maximum netmask length for allocating resources within the pool.

/24 (256 IPs)

Tag compliancy

Tagging requirements

Add tagging requirements for resources in this pool.

Key

environment



Value - *optional*

pre-prod



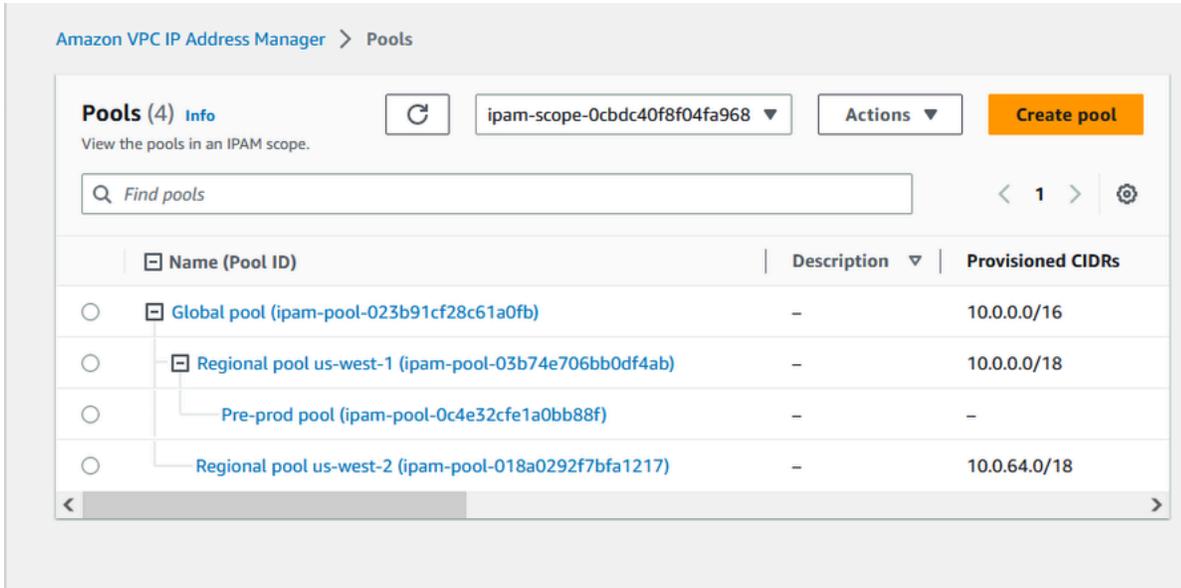
Remove

Add new required tag

You can add up to 49 more tags.

4. 풀 생성을 선택합니다.

5. 이제 풀 계층 구조에는 Regional pool us-west-1 아래에 추가 하위 풀이 포함됩니다.



이제 IPAM 풀을 조직의 다른 멤버 계정과 공유하고 해당 계정이 풀에서 CIDR을 할당하도록 설정하여 VPC를 생성할 준비가 되었습니다.

6단계: IPAM 풀 공유

이 섹션의 단계에 따라 AWS Resource Access Manager(RAM)를 사용하여 사전 프로덕션 IPAM 풀을 공유합니다.

이 섹션은 2개의 하위 섹션으로 구성되어 있습니다.

- [6.1단계. AWS RAM에서 리소스 공유 활성화](#): 이 단계는 AWS Organizations 관리 계정으로 수행해야 합니다.
- [6.2단계. AWS RAM을 사용하여 IPAM 풀 공유](#): 이 단계는 IPAM 관리자로 수행해야 합니다.

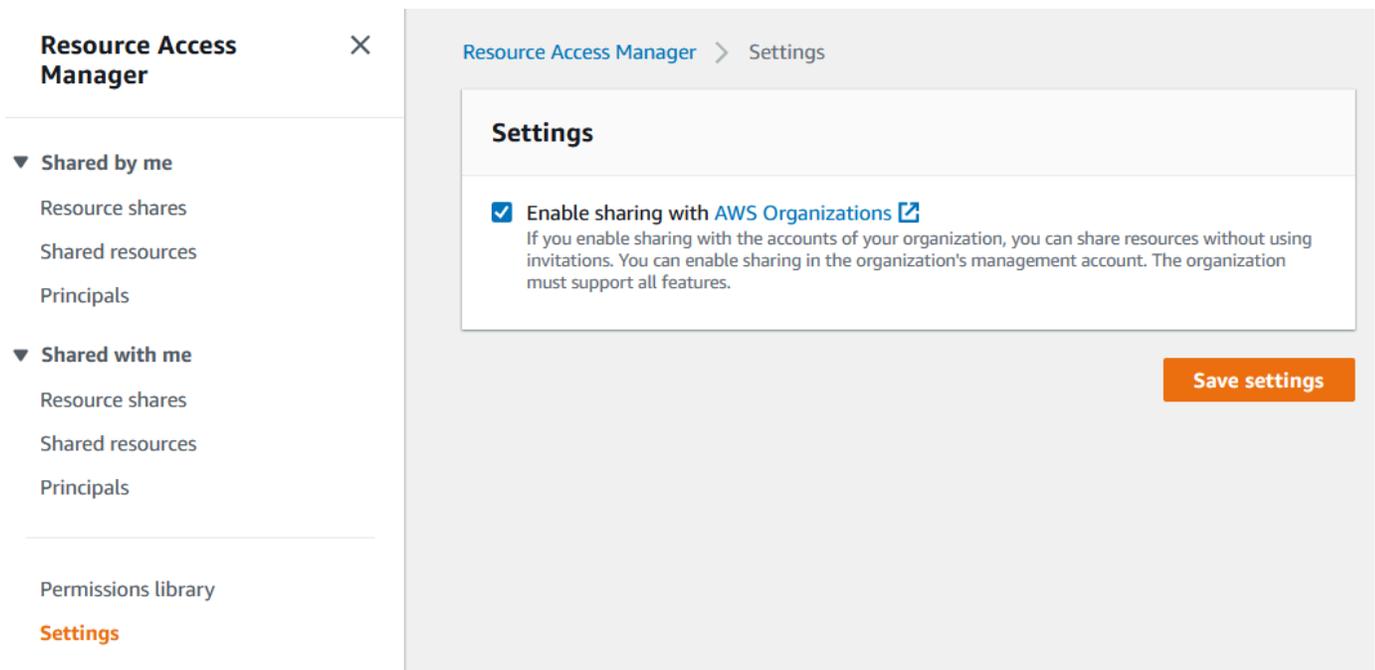
6.1단계. AWS RAM에서 리소스 공유 활성화

IPAM을 생성한 후에는 IP 주소 풀을 조직의 다른 계정과 공유할 수 있습니다. IPAM 풀을 공유하기 전에 이 단원의 단계를 완료하여 AWS RAM과 리소스 공유를 활성화합니다.

리소스 공유 활성화

1. AWS Organizations 관리 계정을 사용하여 <https://console.aws.amazon.com/ram/>에서 AWS RAM 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 설정을 선택하고 공유 활성화 범위 - AWS Organizations를 선택한 다음 설정 저장 장을 선택합니다.



이제 IPAM 풀을 조직의 다른 멤버와 공유할 수 있습니다.

6.2단계. AWS RAM을 사용하여 IPAM 풀 공유

이 섹션에서는 사전 프로덕션 개발 풀을 다른 AWS Organizations 멤버 계정과 공유합니다. 필수 IAM 권한에 대한 정보를 포함하여 IPAM 풀 공유에 대한 전체 지침은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요.

AWS RAM을 사용하여 IPAM 풀 공유

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택하고 사전 프로덕션 IPAM 풀을 선택한 다음 작업 > 세부 정보 보기를 선택합니다.
4. 리소스 공유(Resource sharing)에서 리소스 공유 생성(Create resource share)을 선택합니다. AWS RAM 콘솔이 열립니다. AWS RAM을 사용하여 풀을 공유합니다.
5. 리소스 공유 생성(Create a resource share)을 선택합니다.

Sent request to provision 10.0.0.0/20

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

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

Pool summary

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

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

Resource sharing Info

Filter resource shares

Resource share ARN | Status | Created at

No shares
This resource is not part of any resource share.

Create resource share

AWS RAM 콘솔이 열립니다.

6. AWS RAM 콘솔에서 리소스 공유 생성을 다시 선택합니다.
7. 공유 풀에 대한 이름을 추가합니다.
8. 리소스 유형 선택에서 IPAM 풀을 선택한 다음 사전 프로덕션 개발 풀의 ARN을 선택합니다.

Specify resource share details

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

Resource share name

Name

Provide a descriptive name for the resource share.

Pre-prod dev pool

Resources - optional

Choose the resources to add to the resource share.

Select resource type

IPAM Pools

Filter by attributes or search by keyword

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

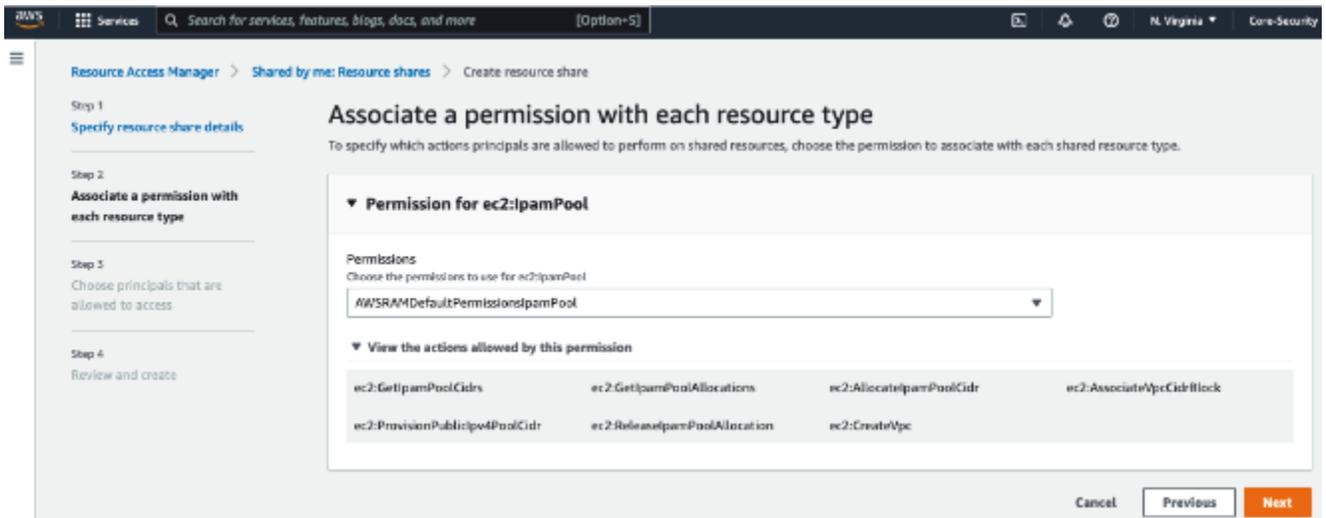
Selected resources (1)

Deselect

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

9. 다음을 선택합니다.

10. 기본값인 `AWSRAMDefaultPermissionsIpamPool` 권한을 선택된 상태로 둡니다. 권한 옵션에 대한 세부 정보는 이 자습서의 범위를 벗어나지만 [AWS RAM을 사용하여 IPAM 풀 공유](#)에서 이러한 옵션에 대해 자세히 알아볼 수 있습니다.



11. 다음을 선택합니다.

12. 보안 주체 아래에서 조직 내에서만 공유 허용을 선택합니다. [AWS Organizations가 IPAM과 통합되는 방식](#)에 설명된 대로 AWS Organizations 조직 단위 ID를 입력한 다음 추가를 선택합니다.

Grant access to principals

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

Principals - *optional*

Allow sharing with anyone

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

Allow sharing only within your organization

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

Principals

You can add multiple principals of different types.

Organizational unit (OU) ▼

ou-fssg-q5brfv9c

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

Add

▼ Selected principals (0)

Deselect

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

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

No selected principals.

Cancel

Previous

Next

13. 다음을 선택합니다.

14. 리소스 공유 옵션 및 공유할 보안 주체를 검토하고 생성을 선택합니다.

이제 폴이 공유되었으므로 다음 단계로 이동하여 IPAM 폴에서 할당된 CIDR을 사용하여 VPC를 생성합니다.

7단계: IPAM 폴에서 할당된 CIDR을 사용하여 VPC 생성

이 섹션의 단계에 따라 사전 프로덕션 폴에서 할당된 CIDR을 사용하여 VPC를 생성합니다. 이 단계는 이전 섹션에서 IPAM 폴을 공유한 OU의 멤버 계정으로 완료해야 합니다([AWS Organizations가 IPAM](#)

[과 통합되는 방식](#)에서는 example-member-account-2). VPC를 생성하는 데 필요한 IAM 권한에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [Amazon VPC 정책 예](#)를 참조하세요.

IPAM 풀에서 할당된 CIDR을 사용하여 VPC 생성

1. 멤버 계정을 사용하여 개발자 계정으로 사용할 멤버 계정으로 <https://console.aws.amazon.com/vpc/>에서 VPC 콘솔을 엽니다.
2. VPC 생성을 선택합니다.
3. 다음을 따릅니다.
 1. 이름(예: Example VPC)을 입력합니다.
 2. IPAM 할당 IPv4 CIDR 블록을 선택합니다.
 3. IPv4 IPAM 풀 아래에서 사전 프로덕션 풀의 ID를 선택합니다.
 4. 넷마스크 길이를 선택합니다. 넷마스크 길이를 선택합니다. 이 풀에 사용 가능한 넷마스크 길이를 /24로 제한했기 때문에([5단계: 사전 프로덕션 개발 풀 생성](#)) 사용할 수 있는 넷마스크 옵션은 /24뿐입니다.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

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

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

 VPC only

 VPC and more

Name tag - optional

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

IPv4 CIDR block [Info](#)

 IPv4 CIDR manual input

 IPAM-allocated IPv4 CIDR block

IPv4 IPAM pool

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

Netmask

4. 시연을 위해 지금은 태그 아래에서 태그를 더 추가하지 마세요. 사전 프로덕션 풀을 생성할 때(5. [사전 프로덕션 개발 풀 생성](#)) 이 풀의 CIDR로 생성된 모든 VPC에 환경/사전 프로덕션 태그가 있어야 한다는 할당 규칙을 추가했습니다. 필수 태그가 추가되지 않았다는 오류가 표시되는 것을 볼 수 있게 environment/pre-prod 태그를 꺼둡니다.
5. VPC 생성을 선택합니다.
6. 필수 태그가 추가되지 않았다는 오류 메시지가 나타납니다. 사전 프로덕션 풀을 생성할 때(5단계: [사전 프로덕션 개발 풀 생성](#)) 할당 규칙을 설정했기 때문에 이 오류가 나타납니다. 할당 규칙에 따라 이 풀의 CIDR로 생성된 모든 VPC에는 environment/pre-prod 태그가 있어야 합니다.

⊗ **There was an error creating your VPC**
The resource is missing one or more of the resource tags required by the IPAM pool.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

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

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

VPC only

VPC and more

Name tag - *optional*

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

Example VPC

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input

IPAM-allocated IPv4 CIDR block

7. 이제 태그 아래에서 environment/pre-prod 태그를 추가하고 VPC 생성을 다시 선택합니다.

Tags

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

Key

Q Name X

Q environment X

Add new tag

You can add 48 more tags.

Value - *optional*

Q Example VPC X

Q pre-prod X

Remove

Remove

8. VPC가 성공적으로 생성되고 VPC가 사전 프로덕션 풀의 태그 규칙을 준수합니다.

☑ You successfully created vpc-07701f4fcc6549b8d / Example VPC

VPC > Your VPCs > vpc-07701f4fcc6549b8d

vpc-07701f4fcc6549b8d / Example VPC

Actions ▼

Details [Info](#)

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

IPAM 콘솔의 리소스 창에서 IPAM 관리자는 VPC와 할당된 CIDR을 보고 관리할 수 있습니다. VPC가 리소스 창에 표시되는 데 시간이 좀 걸립니다.

8단계: 정리

이 자습서에서는 위임된 관리자로 IPAM을 생성하고, 여러 풀을 생성하고, 조직의 멤버 계정이 풀에서 VPC CIDR을 할당하도록 설정했습니다.

이번 섹션의 단계에 따라 이 자습서에서 생성한 리소스를 정리합니다.

이 자습서에서 생성한 리소스 정리

1. 예제 VPC를 생성한 멤버 계정을 사용하여 VPC를 삭제합니다. 자세한 지침은 Amazon Virtual Private Cloud 사용 설명서의 [VPC 삭제](#)를 참조하세요.
2. IPAM 관리자 계정을 사용하여 AWS RAM 콘솔에서 예제 리소스 공유를 삭제합니다. 자세한 지침은 AWS Resource Access Manager 사용 설명서의 [AWS RAM에서 리소스 공유 삭제](#)를 참조하세요.

3. IPAM 관리자 계정을 사용하여 RAM 콘솔에 로그인하고 [6.1단계. AWS RAM에서 리소스 공유 활성화](#)에서 활성화하는 AWS Organizations와의 공유를 비활성화합니다.
4. IPAM 관리자 계정을 사용하여 IPAM 콘솔에서 IPAM을 선택한 다음 작업 > 삭제를 선택하여 예제 IPAM을 삭제합니다. 자세한 지침은 [IPAM 삭제](#) 섹션을 참조하십시오.
5. IPAM을 삭제하라는 메시지가 나타나면 하위 항목 삭제를 선택합니다. 그러면 IPAM을 삭제하기 전에 IPAM 내의 모든 범위와 풀이 삭제됩니다.

Delete IPAM DemoIPAM (ipam-080d0c4b98089b437) ✕

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

Cascade delete

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

delete

Cancel

Delete

6. delete를 입력하고 삭제를 선택합니다.
7. AWS Organizations 관리 계정을 사용하여 IPAM 콘솔에 로그인하고 설정을 선택한 다음 위임된 관리자 계정을 제거합니다.
8. (선택 사항) IPAM을 AWS Organizations와 통합하면 [IPAM은 각 멤버 계정에 서비스 연결 역할을 자동으로 생성합니다](#). 각 AWS Organizations 멤버 계정을 사용하여 IAM에 로그인하고 각 멤버 계정에서 AWSServiceRoleForIPAM 서비스 연결 역할을 삭제합니다.
9. 정리가 완료되었습니다.

자습서: AWS CLI를 사용하여 IPAM 및 풀 생성

이 자습서의 단계를 따라 AWS CLI를 사용하여 IPAM을 생성하고, IP 주소 풀을 생성하고, IPAM 풀에서 CIDR을 사용하여 VPC를 할당합니다.

다음은 이 섹션의 단계를 따르면 생성할 수 있는 풀 구조의 계층에 대한 예입니다.

- AWS 리전 1 및 AWS 리전 2에서 작동하는 IPAM

- 프라이빗 범위
 - 최상위 풀
 - AWS 리전 2의 리전 풀
 - 개발 풀
 - VPC 대한 할당

Note

이 섹션에서는 IPAM을 생성합니다. 기본적으로 IPAM 하나만 생성할 수 있습니다. 자세한 내용은 [IPAM의 할당량](#) 섹션을 참조하세요. IPAM 계정을 이미 위임하고 IPAM을 생성한 경우 1단계와 2단계를 건너뛸 수 있습니다.

내용

- [1단계: 조직에서 IPAM 사용 설정](#)
- [2단계: IPAM 생성](#)
- [3단계: IPv4 주소 풀 생성](#)
- [4단계: 최상위 풀에 CIDR 프로비저닝](#)
- [5단계. 최상위 풀에서 소싱된 CIDR을 사용하여 리전 풀 생성](#)
- [6단계: 리전 풀에 CIDR 프로비저닝](#)
- [7단계. 계정 간 IP 할당을 사용 설정하기 위한 RAM 공유 생성](#)
- [8단계. VPC 생성](#)
- [9단계. 정리](#)

1단계: 조직에서 IPAM 사용 설정

이 단계는 선택 사항입니다. 조직에서 IPAM을 사용 설정하고 AWS CLI를 사용하여 위임된 IPAM을 구성하려면 이 단계를 완료하세요. IPAM 계정의 역할에 대한 자세한 내용은 [AWS Organization에서 계정과 IPAM 통합](#) 섹션을 참조하세요.

이 요청은 AWS Organizations 관리 계정에서 이루어져야 합니다. 다음 명령을 실행하는 경우 다음 작업을 허용하는 IAM 정책을 통해 역할을 사용하고 있는지 확인합니다.

- `ec2:EnableIpamOrganizationAdminAccount`

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

```
aws ec2 enable-ipam-organization-admin-account --region us-east-1 --delegated-admin-account-id 111111111111
```

사용 설정이 성공했음을 나타내는 다음과 같은 출력이 표시되어야 합니다.

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

2단계: IPAM 생성

이 섹션의 단계에 따라 IPAM을 생성하고 생성된 범위에 대한 추가 정보를 확인합니다. 이후 단계에서 풀을 생성하고 해당 풀에 대한 IP 주소 범위를 프로비저닝할 때 이 IPAM을 사용합니다.

Note

운영 리전 옵션에 따라 IPAM 풀을 사용할 수 있는 AWS 리전을 확인합니다. 운영 리전에 대한 자세한 내용은 [IPAM 생성](#) 섹션을 참조하세요.

AWS CLI를 사용하여 IPAM 생성

1. 다음 명령을 실행하여 IPAM 인스턴스를 생성합니다.

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

IPAM을 생성할 때 AWS는 자동으로 다음 작업을 수행합니다.

- IPAM의 전역 고유 리소스 ID(IpamId)를 반환합니다.
- 기본 퍼블릭 범위(PublicDefaultScopeId) 및 기본 프라이빗 범위(PrivateDefaultScopeId)를 만듭니다.

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

- 다음 명령을 실행하여 범위 관련 추가 정보를 확인합니다. 퍼블릭 범위는 공용 인터넷을 통해 액세스할 IP 주소를 위한 것입니다. 프라이빗 범위는 공용 인터넷을 통해 액세스하지 않을 IP 주소를 위한 것입니다.

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

출력에 사용 가능한 범위가 표시됩니다. 다음 단계에서 프라이빗 범위 ID를 사용합니다.

```
{
  "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
  }
]
}

```

3단계: IPv4 주소 풀 생성

이 섹션의 단계를 따르면 IPv4 주소 풀을 생성할 수 있습니다.

Important

최상위 풀의 `--locale` 옵션을 사용하지 않습니다. 리전 풀에서 나중에 로캘 옵션을 설정합니다. 로캘은 풀을 CIDR 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 최상위 풀에서 로캘을 설정하지 않은 경우 로캘의 기본값은 None입니다. 풀에 None의 로캘이 있는 경우 모든 AWS 리전의 VPC 리소스에서는 풀을 사용할 수 없습니다. 공간을 예약하기 위해서는 풀에서 IP 주소 공간을 수동으로 할당할 수 있습니다.

AWS CLI를 사용하여 모든 AWS 리소스에 대해 IPv4 주소 풀을 생성하려면

1. 다음 명령을 실행하여 IPv4 주소 풀을 생성합니다. 이전 단계에서 생성한 IPAM의 프라이빗 범위 ID를 사용합니다.

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

출력에 풀의 `create-in-progress` 상태가 표시됩니다.

```
{
  "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. 출력에 create-complete의 상태가 표시될 때까지 다음 명령을 실행합니다.

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

다음 예 출력에서는 현재 상태를 보여줍니다.

```

{
  "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"
    }
  ]
}

```

```
}

```

4단계: 최상위 풀에 CIDR 프로비저닝

이 섹션의 단계에 따라 CIDR을 최상위 풀에 프로비저닝한 다음, CIDR이 프로비저닝되었는지 확인합니다. 자세한 내용은 [풀에 CIDR 프로비저닝](#) 단원을 참조하십시오.

AWS CLI를 사용하여 CIDR 블록을 풀에 프로비저닝하려면

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

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

출력에서 프로비저닝 상태를 확인할 수 있습니다.

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

2. 출력에 provisioned의 상태가 표시될 때까지 다음 명령을 실행합니다.

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

다음 예 출력에서는 현재 상태를 보여줍니다.

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

5단계. 최상위 풀에서 소싱된 CIDR을 사용하여 리전 풀 생성

IPAM 풀을 생성하는 경우 풀은 기본적으로 IPAM의 AWS 리전에 속합니다. VPC를 생성하는 경우 VPC가 생성되는 풀은 VPC와 동일한 리전에 있어야 합니다. IPAM 리전 이외의 리전의 서비스에서 풀을 사용할 수 있도록 해당 풀을 생성하는 경우 `--locale` 옵션을 선택할 수 있습니다. 이 섹션의 단계를 따르면 다른 로컬에서 리전 풀을 생성할 수 있습니다.

AWS CLI를 사용하여 이전 풀에서 소싱된 CIDR으로 풀 생성

1. 다음 명령을 실행하여 풀을 만들고 이전 풀에서 알려진 사용 가능한 CIDR을 사용하여 공간을 삽입합니다.

```
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
```

출력에 생성한 풀의 ID가 표시됩니다. 다음 단계에서 이 ID를 사용합니다.

```
{
  "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. 출력에 `create-complete`의 상태가 표시될 때까지 다음 명령을 실행합니다.

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

출력에는 IPAM에 있는 풀이 표시됩니다. 이 자습서에서 최상위 수준 풀 및 리전 풀을 만들었으므로 두 풀이 모두 표시됩니다.

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

```
}

```

6단계: 리전 풀에 CIDR 프로비저닝

이 섹션의 단계에 따라 CIDR 블록을 풀에 할당하고 해당 블록이 성공적으로 프로비저닝되었는지 확인합니다.

AWS CLI를 사용하여 리전 풀에 CIDR 블록을 할당하려면

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

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

출력에 풀의 상태가 표시됩니다.

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

2. 출력에 provisioned의 상태가 표시될 때까지 다음 명령을 실행합니다.

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

다음 예 출력에서는 현재 상태를 보여줍니다.

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

3. 최상위 풀을 쿼리하여 할당을 확인하려면 다음 명령을 실행합니다. 리전 풀은 최상위 풀 내의 할당으로 간주됩니다.

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

출력에 최상위 풀의 할당으로 리전 풀이 표시됩니다.

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

7단계. 계정 간 IP 할당을 사용 설정하기 위한 RAM 공유 생성

이 단계는 선택 사항입니다. [AWS Organization에서 계정과 IPAM 통합](#)을 완료한 경우에만 이 단계를 완료할 수 있습니다.

IPAM 풀 AWS RAM 공유를 생성하는 경우 계정 간 IP 할당을 사용 설정합니다. RAM 공유는 홈 AWS 리전에서만 사용할 수 있습니다. 이 공유는 풀의 로컬 리전이 아닌 IPAM과 동일한 리전에서 생성한다는 점에 유의하세요. IPAM 리소스에 대한 모든 관리 작업은 IPAM의 홈 리전을 통해 이루어집니다. 이 자습서의 예에서는 단일 풀에 대해 단일 공유를 만들지만 단일 공유에 여러 풀을 추가할 수도 있습니다. 입력해야 하는 옵션에 대한 설명을 포함하여 자세한 내용은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요.

다음 명령을 실행하여 리소스 공유를 생성합니다.

```
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
```

출력에 풀이 생성되었다고 표시됩니다.

```
{
  "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
  }
}
```

8단계. VPC 생성

다음 명령을 실행하여 VPC 생성하고 새로 생성된 IPAM의 풀에서 VPC로 CIDR 블록을 할당합니다.

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

출력에 VPC가 생성되었다고 표시됩니다.

```
{
  "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
  }
}
```

```
}
```

9단계. 정리

이번 섹션의 단계를 따르면 이 자습서에서 생성한 IPAM 리소스를 삭제할 수 있습니다.

1. VPC를 삭제합니다.

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

2. IPAM 풀 RAM 공유를 삭제합니다.

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

3. 리전 풀의 풀 CIDR을 프로비저닝 해제합니다.

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

4. 최상위 풀의 풀 CIDR을 프로비저닝 해제합니다.

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

5. IPAM 삭제

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

자습서: AWS CLI를 사용하여 IP 주소 기록 보기

이 섹션의 시나리오에서는 AWS CLI를 사용하여 IP 주소 사용을 분석하고 감사하는 방법을 보여줍니다. AWS CLI 사용에 대한 일반적인 내용은 AWS Command Line Interface 사용 설명서의 [AWS CLI 사용](#)을 참조하세요.

내용

- [개요](#)
- [시나리오](#)

개요

IPAM은 IP 주소 모니터링 데이터를 최대 3년 동안 자동으로 유지합니다. 기록 데이터를 사용하여 네트워크 보안 및 라우팅 정책을 분석하고 감사할 수 있습니다. 다음 리소스 유형에 대한 기록 정보를 검색할 수 있습니다.

- VPC
- VPC 서브넷
- 탄력적 IP 주소
- 실행 중인 EC2 인스턴스
- 인스턴스에 연결된 EC2 네트워크 인터페이스

Important

IPAM은 Amazon EC2 인스턴스 또는 인스턴스에 연결된 EC2 네트워크 인터페이스를 모니터링하지 않지만 IP 기록 검색 기능을 사용하여 EC2 인스턴스 및 네트워크 인터페이스 CIDR에서 기록 데이터를 검색할 수 있습니다.

Note

- 이 자습서의 명령은 IPAM을 소유하는 계정과 IPAM을 호스팅하는 AWS 리전을 사용하여 실행해야 합니다.
- CIDR에 대한 변경 사항 레코드는 주기적 스냅샷에서 선택됩니다. 즉, 레코드가 나타나거나 업데이트되는 데 어느 정도 시간이 걸릴 수 있으며 SampledStartTime 및 SampledEndTime 값은 실제 발생 시간과 다를 수 있습니다.

시나리오

이 섹션의 시나리오에서는 AWS CLI를 사용하여 IP 주소 사용을 분석하고 감사하는 방법을 보여줍니다. 샘플링된 종료 시간 및 시작 시간과 같이 이 자습서에서 언급한 값에 대한 자세한 내용은 [IP 주소 기록 보기](#) 섹션을 참조하세요.

시나리오 1: 2021년 12월 27일(UTC) 오전 1시에서 오후 9시 사이에 어느 리소스가 **10.2.1.155/32**와 연결되었나요?

1. 다음 명령을 실행합니다:

```
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. 분석 결과를 봅니다. 아래 예에서 CIDR은 일정 기간 동안 네트워크 인터페이스와 EC2 인스턴스에 할당되었습니다. 참고: SampledEndTime 값이 없으면 레코드가 여전히 활성 상태인 것입니다. 다음 출력에 표시된 값에 대한 자세한 내용은 [IP 주소 기록 보기](#) 섹션을 참조하세요.

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

네트워크 인터페이스가 연결된 인스턴스의 소유자 ID가 네트워크 인터페이스의 소유자 ID와 다른 경우(NAT 게이트웨이, VPC의 Lambda 네트워크 인터페이스 및 기타 AWS 서비스의 경우) ResourceOwnerId는 네트워크 인터페이스 소유자의 계정 ID가 아니라 amazon-aws입니다. 다음 예에서는 NAT 게이트웨이와 연결된 CIDR에 대한 레코드를 보여줍니다.

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

시나리오 2: 2021년 12월 1일부터 2021년 12월 27일(UTC)까지 어느 리소스가 **10.2.1.0/24**과 연결되었나요?

1. 다음 명령을 실행합니다:

```
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. 분석 결과를 봅니다. 아래 예에서 CIDR은 일정 기간 동안 서브넷과 VPC에 할당되었습니다. 참고: SampledEndTime 값이 없으면 레코드가 여전히 활성 상태인 것입니다. 다음 출력에 표시된 값에 대한 자세한 내용은 [IP 주소 기록 보기](#) 섹션을 참조하세요.

```
{
  "HistoryRecords": [
    {
      "ResourceOwnerId": "123456789012",
      "ResourceRegion": "us-east-1",
```

```

    "ResourceType": "subnet",
    "ResourceId": "subnet-0864c82a42f5bffd",
    "ResourceCidr": "10.2.1.0/24",
    "VpcId": "vpc-0f5ee7e1ba908a378",
    "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
  },
  {
    "ResourceOwnerId": "123456789012",
    "ResourceRegion": "us-east-1",
    "ResourceType": "vpc",
    "ResourceId": "vpc-0f5ee7e1ba908a378",
    "ResourceCidr": "10.2.1.0/24",
    "ResourceComplianceStatus": "compliant",
    "ResourceOverlapStatus": "nonoverlapping",
    "VpcId": "vpc-0f5ee7e1ba908a378",
    "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
  }
]
}

```

시나리오 3: 2021년 12월 1일부터 2021년 12월 27일(UTC)까지 어느 리소스가 **2605:9cc0:409::/56**과 연결되었나요?

1. 다음 명령을 실행합니다. 여기서 --region은 IPAM 홈 리전입니다.

```

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. 분석 결과를 봅니다. 아래 예에서 CIDR은 IPAM 홈 리전 외부의 리전에서 일정 기간 동안 2개의 서로 다른 VPC에 할당되었습니다. 참고: SampledEndTime 값이 없으면 레코드가 여전히 활성 상태인 것입니다. 다음 출력에 표시된 값에 대한 자세한 내용은 [IP 주소 기록 보기](#) 섹션을 참조하세요.

```

{
  "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"
  }
]
}

```

시나리오 4: 지난 24시간 동안 어느 리소스가 **10.0.0.0/24**와 연결되었나요(현재 시간이 2021년 12월 27일 자정(UTC)이라고 가정)?

1. 다음 명령을 실행합니다:

```
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. 분석 결과를 봅니다. 아래 예에서 CIDR은 일정 기간 동안 수많은 서브넷과 VPC에 할당되었습니다. 참고: SampledEndTime 값이 없으면 레코드가 여전히 활성 상태인 것입니다. 다음 출력에 표시된 값에 대한 자세한 내용은 [IP 주소 기록 보기](#) 섹션을 참조하세요.

```

{
  "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"
  }
]
}

```

시나리오 5: 현재 어느 리소스가 **10.2.1.155/32**와 연결되었나요?

1. 다음 명령을 실행합니다:

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

2. 분석 결과를 봅니다. 아래 예에서 CIDR은 일정 기간 동안 네트워크 인터페이스와 EC2 인스턴스에 할당되었습니다. 참고: SampledEndTime 값이 없으면 레코드가 여전히 활성 상태인 것입니다. 다음 출력에 표시된 값에 대한 자세한 내용은 [IP 주소 기록 보기](#) 섹션을 참조하세요.

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

시나리오 6: 현재 어느 리소스가 **10.2.1.0/24**와 연결되었나요?

1. 다음 명령을 실행합니다:

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

2. 분석 결과를 봅니다. 아래 예에서 CIDR은 일정 기간 동안 VPC와 서브넷에 할당되었습니다. /24 CIDR 내의 모든 /32 가 아니라 이 정확한 /24 CIDR과 일치하는 결과만 반환됩니다. 참고: `SampledEndTime` 값이 없으면 레코드가 여전히 활성 상태인 것입니다. 다음 출력에 표시된 값에 대한 자세한 내용은 [IP 주소 기록 보기](#) 섹션을 참조하세요.

```
{
  "HistoryRecords": [
    {
      "ResourceOwnerId": "123456789012",
      "ResourceRegion": "us-east-1",
      "ResourceType": "subnet",
      "ResourceId": "subnet-0864c82a42f5bffd",
      "ResourceCidr": "10.2.1.0/24",
      "VpcId": "vpc-0f5ee7e1ba908a378",
      "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
    },
    {
      "ResourceOwnerId": "123456789012",
      "ResourceRegion": "us-east-1",
      "ResourceType": "vpc",
      "ResourceId": "vpc-0f5ee7e1ba908a378",
      "ResourceCidr": "10.2.1.0/24",
      "ResourceComplianceStatus": "compliant",
      "ResourceOverlapStatus": "nonoverlapping",
      "VpcId": "vpc-0f5ee7e1ba908a378",
      "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
    }
  ]
}
```

시나리오 7: 현재 어느 리소스가 **54.0.0.9/32**와 연결되었나요?

이 예에서 54.0.0.9/32는 IPAM과 통합된 AWS Organization의 일부가 아닌 탄력적 IP 주소에 할당됩니다.

1. 다음 명령을 실행합니다:

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

2. 이 예에서 54.0.0.9/32는 IPAM과 통합된 AWS Organization의 일부가 아닌 탄력적 IP 주소에 할당되므로 레코드가 반환되지 않습니다.

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

자습서: IPAM으로 ASN 가져오기

애플리케이션에서 파트너 또는 고객이 네트워크에 허용한 신뢰할 수 있는 IP 주소 및 Autonomous System Number(ASN)를 사용하는 경우 파트너나 고객이 허용 목록을 변경하지 않고도 AWS에서 이러한 애플리케이션을 실행할 수 있습니다.

Autonomous System Number(ASN)는 인터넷을 통해 네트워크 그룹을 식별하고 [Border Gateway Protocol](#)을 사용하여 동적으로 다른 네트워크와 라우팅 데이터를 교환할 수 있도록 하는 글로벌 고유 번호입니다. 예를 들어 인터넷 서비스 제공업체(ISP)는 ASN을 사용하여 네트워크 트래픽 소스를 식별합니다. 모든 조직이 자체 ASN을 구매하는 것은 아니지만, 구매하는 조직의 경우 ASN을 AWS로 가져올 수 있습니다.

기존 보유 자율 시스템 번호 가져오기(BYOASN)를 사용하면 AWS ASN 대신 자체 퍼블릭 ASN을 사용하여 AWS로 가져오는 IP 주소를 알릴 수 있습니다. BYOASN을 사용하면 IP 주소에서 발생하는 트래픽이 ASN 대신 ASN을 전달하므로 IP 주소 및 AWS ASN을 기반으로 나열된 트래픽을 허용하는 고객이나 파트너가 워크로드에 연결할 수 있습니다.

Important

- IPAM 홈 리전의 IPAM 관리자 계정을 사용하여 이 자습서를 완료하세요.
- 이 자습서에서는 IPAM으로 가져오려는 퍼블릭 ASN을 소유하고 있으며 이미 BYOIP CIDR을 AWS로 가져와 퍼블릭 범위의 풀에 프로비저닝했다고 가정합니다. 언제든지 IPAM에 ASN을 가져올 수 있지만, 이를 사용하려면 AWS 계정에 가져온 CIDR과 연결해야 합니다. 이 자습서에서는 그것을 이미 완료했다고 가정합니다. 자세한 내용은 [자습서: IPAM으로 IP 주소 가져오기](#) 단원을 참조하십시오.
- 지체 없이 자체 ASN 또는 AWS ASN을 알리도록 변경할 수 있지만 한 시간에 한 번만 AWS ASN에서 자체 ASN으로 변경할 수 있습니다.
- BYOIP CIDR이 현재 알려지고 있는 경우 ASN과 연계하기 위해 광고에서 BYOIP CIDR을 철회할 필요가 없습니다.

ASN에 대한 온보딩 사전 조건

이 자습서를 완료하려면 다음이 필요합니다.

- 퍼블릭 2바이트 또는 4바이트 ASN.
- 이미 [자습서: IPAM으로 IP 주소 가져오기](#)를 통해 AWS로 IP 주소 범위를 가져왔다면 IP 주소 CIDR 범위가 필요합니다. 프라이빗 키도 필요합니다. AWS로 IP 주소 CIDR 범위를 가져올 때 생성한 프라이빗 키를 사용하거나 EC2 사용 설명서의 [프라이빗 키 생성 및 X.509 인증서 생성](#)에 설명된 대로 새 프라이빗 키를 생성할 수 있습니다.
- AWS에 [자습서: IPAM으로 IP 주소 가져오기](#)(으)로 IP 주소 범위를 가져오는 경우 [X.509 인증서를 생성](#)하고 [X.509 인증서를 RIR의 RDAP 레코드에 업로드](#)합니다. 생성한 동일한 인증서를 ASN용 RIR에 있는 RDAP 레코드에 업로드 해야 합니다. 인코딩된 부분 앞과 뒤에 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 문자열을 포함해야 합니다. 이 모든 내용은 하나의 긴 줄에 있어야 합니다. RDAP를 업데이트하는 절차는 RIR에 따라 다릅니다.
 - ARIN의 경우 [계정 관리자 포털](#)을 통해 “공개 주식” 섹션에 인증서를 추가하세요. 인증서는 “Network Information” 개체를 위해 쓰이며 “Modify ASN” 옵션을 사용하여 ASN을 표시합니다. 조직의 주식 섹션에 추가하지 마세요.
 - RIPE의 경우 ASN을 나타내는 “aut-num” 개체에 새 “descr” 필드로 인증서를 추가합니다. 인증서는 “내 리소스” 섹션에서 찾을 수 있습니다.

[RIPE 데이터베이스 포털](#) 참조. 조직의 주식 섹션이나 “aut-num” 개체의 “비고” 필드에 추가하지 마세요.

- APNIC의 경우 이메일을 통해 인증서를 helpdesk@apnic.net로 전송하여 ASN의 “설명” 필드에 수동으로 추가합니다. ASN의 APNIC 공인 연락처를 사용하여 이메일을 전송합니다.

자습서 단계

AWS 콘솔 또는 AWS CLI를 사용하여 아래 단계를 완료하세요.

AWS Management Console

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 IPAM을 선택합니다.
3. IPAM을 선택합니다.
4. BYOASN 탭을 선택하고 BYOASN 프로비저닝을 선택합니다.

5. ASN을 입력합니다. 결과적으로 메시지 필드는 다음 단계에서 서명해야 할 메시지로 자동으로 채워집니다.
 - 메시지 형식은 다음과 같습니다. 여기서 ACCOUNT는 AWS 계정 번호이고, ASN은 IPAM으로 가져오는 ASN이며, YYYYMMDD는 메시지 만료 날짜(기본값은 다음 달 말일)입니다. 예제

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

6. 원하는 경우 메시지를 복사하고 만료 날짜를 원하는 값으로 바꾸세요.
7. 프라이빗 키를 사용하여 메시지에 서명합니다. 예제

```
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. 서명에 서명을 입력합니다.
9. (선택 사항) 다른 ASN을 프로비저닝하려면 다른 ASN 프로비저닝을 선택합니다. 최대 5개의 ASN을 프로비저닝할 수 있습니다. 이 할당량을 늘리려면 [IPAM의 할당량](#)을 참조하세요.
10. 프로비저닝을 선택합니다.
11. BYOASN 탭에서 프로비저닝 프로세스를 확인합니다. 상태가 프로비저닝 보류 중에서 프로비저닝됨으로 변경될 때까지 기다리세요. 프로비저닝 실패 상태의 BYOASN은 7일 후에 자동으로 제거됩니다. ASN이 성공적으로 프로비저닝되면 이를 BYOIP CIDR에 연결할 수 있습니다.
12. 왼쪽 탐색 창에서 풀을 선택합니다.
13. 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
14. BYOIP CIDR이 프로비저닝된 리전 풀을 선택합니다. 풀에는 서비스가 EC2로 설정되어 있어야 하며 로케일이 선택되어 있어야 합니다.
15. CIDR 탭을 선택하고 BYOIP CIDR을 선택합니다.
16. 작업 > BYOASN 연결 관리를 선택합니다.
17. 연결된 BYOASN에서 AWS로 가져온 ASN을 선택합니다. ASN이 여러 개 있는 경우 여러 ASN을 BYOIP CIDR에 연결할 수 있습니다. IPAM에 가져올 수 있는 만큼 많은 ASN을 연결할 수 있습니다. 참고로 기본적으로 최대 5개의 ASN을 IPAM으로 가져올 수 있습니다. 자세한 내용은 [IPAM의 할당량](#) 단원을 참조하십시오.
18. Associate(연결)를 선택합니다.
19. ASN 연결이 완료될 때까지 기다립니다. ASN이 BYOIP CIDR에 성공적으로 연결되면 BYOIP CIDR을 다시 알릴 수 있습니다.

20. 풀 CIDR 탭을 선택합니다.
21. BYOIP CIDR을 선택하고 작업(Actions) > 알리기(Advertise)를 선택합니다. 결과적으로 Amazon ASN 및 IPAM으로 가져온 모든 ASN 등 ASN 옵션이 표시됩니다.
22. IPAM으로 가져온 ASN을 선택하고 CIDR 알리기를 선택합니다. 결과적으로 BYOIP CIDR이 알려지고 알림 열의 값이 철회됨에서 알려짐으로 변경됩니다. 자율 시스템 번호 열에는 CIDR과 연결된 ASN이 표시됩니다.
23. (선택 사항) ASN 연결을 Amazon ASN으로 다시 변경하려면 BYOIP CIDR을 선택하고 작업 > 알리기를 다시 선택합니다. 이번에는 Amazon ASN을 선택합니다. 언제든지 Amazon ASN으로 다시 스왑할 수 있지만 사용자 지정 ASN으로 1시간에 한 번만 변경할 수 있습니다.

튜토리얼이 완료되었습니다.

정리

1. BYOIP CIDR에서 AS를 분리
 - 알림에서 BYOIP CIDR을 철회하려면 퍼블릭 범위 풀에서 BYOIP CIDR을 선택하고 작업 > 알림 철회를 선택합니다.
 - CIDR에서 ASN을 분리하려면 작업 > BYOASN 연결 관리를 선택합니다.
2. ASN 프로비저닝 해제
 - ASN을 프로비저닝 해제하려면 BYOASN 탭에서 ASN을 선택하고 ASN 프로비저닝 해제를 선택합니다. 결과적으로 ASN이 프로비저닝 해제됩니다. 프로비저닝 해제 상태의 BYOASN은 7일 후에 자동으로 제거됩니다.

정리가 완료되었습니다.

Command line

1. ASN과 권한 부여 메시지를 포함하여 ASN을 프로비저닝합니다. 서명은 프라이빗 키로 서명된 메시지입니다.

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

2. 프로비저닝 프로세스를 추적할 수 있도록 ASN을 설명하세요. 요청이 성공하면 몇 분 후에 ProvisionStatus가 프로비저닝됨으로 설정된 것을 확인할 수 있습니다.

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

- ASN을 BYOIP CIDR과 연결합니다. 알리려는 모든 사용자 지정 ASN은 먼저 CIDR에 연결되어야 합니다.

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

- 연결 프로세스를 추적하려면 CIDR을 설명하세요.

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

- ASN을 통해 CIDR을 알립니다. CIDR이 이미 알려진 경우, 원본 ASN이 Amazon의 ASN에서 사용자의 ASN으로 교체됩니다.

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

- ASN 상태가 연결됨에서 알려짐으로 변경되는지 확인하려면 CIDR을 설명하세요.

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

튜토리얼이 완료되었습니다.

정리

- 다음 중 하나를 수행하십시오.

- ASN 알림만 철회하고 다시 CIDR 알림을 유지하면서 Amazon ASN을 다시 사용하려면 `asn` 파라미터에 대한 특수 AWS 값을 사용하여 `advertise-byoip-cidr`를 호출해야 합니다. 언제든지 Amazon ASN으로 다시 스왑할 수 있지만 사용자 지정 ASN으로 1시간에 한 번만 변경할 수 있습니다.

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

- CIDR과 ASN 알림을 동시에 철회하려면 `withdraw-byoip-cidr`를 호출할 수 있습니다.

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

- ASN을 정리하려면 먼저 BYOIP CIDR에서 ASN을 분리해야 합니다.

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

- ASN이 연결된 모든 BYOIP CIDR에서 ASN의 연결이 해제되면 해당 ASN을 프로비저닝 해제할 수 있습니다.

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

- 또한 모든 ASN 연결이 제거되면 BYOIP CIDR을 프로비저닝 해제할 수 있습니다.

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

- 프로비저닝 해제를 확인합니다.

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

정리가 완료되었습니다.

자습서: IPAM으로 IP 주소 가져오기

이 섹션의 자습서에서는 퍼블릭 IP 주소 공간을 AWS로 가져오고 IPAM을 사용하여 공간을 관리하는 프로세스를 안내합니다.

IPAM을 사용하여 퍼블릭 IP 주소 공간을 관리하면 다음과 같은 이점이 있습니다.

- 조직 전체에 걸쳐 퍼블릭 IP 주소 활용도 향상(Improves public IP addresses utilization across your organization): IPAM을 사용하여 AWS 계정 전체에 걸쳐 IP 주소 공간을 공유할 수 있습니다. IPAM을 사용하지 않으면 AWS Organizations 계정 전체에 걸쳐 퍼블릭 IP 공간을 공유할 수 없습니다.
- 퍼블릭 IP 공간을 AWS로 가져오는 프로세스 단순화: IPAM을 사용하여 퍼블릭 IP 주소 공간을 한 번 온보딩한 다음, IPAM을 사용하여 리전 전체에 걸쳐 퍼블릭 IP를 배포할 수 있습니다. IPAM이 없으면 각 AWS 리전의 퍼블릭 IP를 온보딩해야 합니다.

Important

- 이 자습서를 시작하기 전에 Amazon EC2 사용 설명서의 [BYOIP 주소 범위에 대한 온보딩 사전 조건](#)의 단계를 완료하세요.

ROA를 생성할 때 IPv4 CIDR의 경우 IP 주소 접두사의 최대 길이를 /24로 설정해야 합니다. IPv6 CIDR의 경우 알릴 수 있는 풀에 해당 CIDR을 추가하면 IP 주소 접두사의 최대 길이는 /48여야 합니다. 이렇게 하면 퍼블릭 IP 주소를 AWS 리전 전체에 걸쳐 충분히 유연하게 분할할 수 있습니다. IPAM은 사용자가 설정한 최대 길이를 적용합니다. 최대 길이는 이 라우팅에 허용되는 가장 작은 접두사 길이 알림입니다. 예를 들어 /20 CIDR 블록을 AWS로 가져오는 경우 최대 길이를 /24로 설정하여 원하는 대로 더 큰 블록(예: /21, /22 또는 /24)을 분할하고, 더 작은 CIDR 블록을 모든 리전에 배포할 수 있습니다. 최대 길이를 /23으로 설정하는 경우 더 큰 블록의 /24를 분할하여 알릴 수 없게 됩니다. 또한, /24는 가장 작은 IPv4 블록이며 /48은 리전에서 인터넷으로 알릴 수 있는 가장 작은 IPv6 블록입니다.

- 사용하여 AWS로 IPv4 주소 범위를 가져오면 첫 번째 주소(네트워크 주소)와 마지막 주소(브로드캐스트 주소)를 포함하여 범위 내의 IP 주소를 모두 사용할 수 있습니다.

내용

- [AWS 관리 콘솔과 AWS CLI를 모두 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#)
- [AWS CLI만 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#)

AWS 관리 콘솔과 AWS CLI를 모두 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기

다음 단계에 따라 AWS 관리 콘솔과 AWS CLI를 모두 사용하여 IPv4 또는 IPv6 CIDR을 IPAM으로 가져오세요.

Important

- 이 자습서를 시작하기 전에 Amazon EC2 사용 설명서의 [BYOIP 주소 범위에 대한 온보딩 사전 조건](#)의 단계를 완료하세요.

ROA를 생성할 때 IPv4 CIDR의 경우 IP 주소 접두사의 최대 길이를 /24로 설정해야 합니다. IPv6 CIDR의 경우 알릴 수 있는 풀에 해당 CIDR을 추가하면 IP 주소 접두사의 최대 길이는 /48여야 합니다. 이렇게 하면 퍼블릭 IP 주소를 AWS 리전 전체에 걸쳐 충분히 유연하게 분할할 수 있습니다. IPAM은 사용자가 설정한 최대 길이를 적용합니다. 최대 길이는 이 라우팅에 허용되는 가장 작은 접두사 길이 알림입니다. 예를 들어 /20 CIDR 블록을 AWS로 가져오는 경우 최대 길이를 /24로 설정하여 원하는 대로 더 큰 블록(예: /21, /22 또는 /24)을 분할하고, 더 작은 CIDR 블록을 모든 리전에 배포할 수 있습니다. 최대 길이를 /23으로 설정하

는 경우 더 큰 블록의 /24를 분할하여 알릴 수 없게 됩니다. 또한, /24는 가장 작은 IPv4 블록이며 /48은 리전에서 인터넷으로 알릴 수 있는 가장 작은 IPv6 블록입니다.

- 사용하여 AWS로 IPv4 주소 범위를 가져오면 첫 번째 주소(네트워크 주소)와 마지막 주소(브로드캐스트 주소)를 포함하여 범위 내의 IP 주소를 모두 사용할 수 있습니다.

내용

- [AWS 관리 콘솔과 AWS CLI를 모두 사용하여 IPAM으로 고유 IPv4 CIDR 가져오기](#)
- [AWS 관리 콘솔을 모두 사용하여 IPAM으로 고유 IPv6 CIDR 가져오기](#)

AWS 관리 콘솔과 AWS CLI를 모두 사용하여 IPAM으로 고유 IPv4 CIDR 가져오기

다음 단계에 따라 IPv4 CIDR을 IPAM으로 가져오고 AWS 관리 콘솔과 AWS CLI를 모두 사용하여 탄력적 IP 주소(EIP)를 할당합니다.

Important

- 지금은 Local Zones에서 BYOIP 주소 범위를 프로비저닝하거나 홍보할 수 없습니다.
- 이 자습서에서는 다음 섹션의 단계를 이미 수행한 것으로 가정합니다.
 - [AWS Organization에서 계정과 IPAM 통합](#).
 - [IPAM 생성](#).
- 이 자습서의 각 단계는 다음 3개의 AWS Organizations 계정 중 하나로 수행해야 합니다.
 - 관리 계정.
 - [AWS Organization에서 계정과 IPAM 통합](#)에서 IPAM 관리자로 구성된 멤버 계정. 이 자습서에서는 이 계정을 IPAM 계정이라고 합니다.
 - IPAM 풀에서 CIDR을 할당할 조직의 멤버 계정입니다. 이 자습서에서는 이 계정을 멤버 계정이라고 합니다.

내용

- [1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성](#)
- [2단계: 최상위 IPAM 풀 생성](#)
- [단계 3. 최상위 풀 내에 리전 풀 생성](#)

- [4단계: 리전 풀 공유](#)
- [5단계: 퍼블릭 IPv4 풀 생성](#)
- [6단계: 퍼블릭 IPv4 CIDR을 퍼블릭 IPv4 풀에 프로비저닝](#)
- [7단계: 퍼블릭 IPv4 풀에서 탄력적 IP 주소 생성](#)
- [8단계: EC2 인스턴스와 탄력적 IP 주소 연결](#)
- [9단계: CIDR 알리기](#)
- [10단계: 정리](#)

1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성

단일 AWS 사용자로 이 자습서를 완료하려면 AWS CLI 명령 프로파일을 사용하여 IAM 역할 간에 전환할 수 있습니다. [명명 프로파일](#)은 AWS CLI와(과) 함께 `--profile` 옵션을 사용할 때 참조하는 설정 및 보안 인증 정보의 모음입니다. AWS 계정에 대한 IAM 역할 및 명명 프로파일 생성 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [AWS CLI에서 IAM 역할 사용](#)을 참조하세요.

이 자습서에서 사용할 세 AWS 계정 각각에 대해 역할 하나와 명명 프로파일 하나를 만듭니다:

- AWS Organizations 관리 계정에 대한 `management-account`라는 프로파일
- IPAM 관리자로 구성된 AWS Organizations 멤버 계정의 `ipam-account`라는 프로파일
- IPAM 풀에서 CIDR을 할당할 조직의 AWS Organizations 멤버 계정에 대한 `member-account`라는 프로파일

IAM 역할 및 명명 프로파일을 생성한 후 이 페이지로 돌아와서 다음 단계로 이동합니다. 이 자습서의 나머지 부분에서 샘플 AWS CLI 명령이 명명된 프로파일 중 하나와 함께 `--profile` 옵션을 사용하여 명령을 실행해야 하는 계정을 나타냅니다.

2단계: 최상위 IPAM 풀 생성

이 섹션의 단계에 따라 최상위 IPAM 풀을 생성하세요.

이 단계는 IPAM 계정으로 수행해야 합니다.

풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.

2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 풀 생성(Create pool)을 선택합니다.
5. (선택 사항) 풀에 대한 이름 태그(Name tag)와 설명(Description)을 추가합니다.
6. 소스에서 IPAM 범위를 선택합니다.
7. 주소 패밀리(Address family)에서 IPv4를 선택합니다.
8. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
9. 로캘(Locale)에서 없음(None)을 선택합니다.

로캘은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를 들어 VPC의 리전과 로캘을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로캘을 선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로캘이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다.

BYOIP와 IPAM을 통합하려면 BYOIP CIDR에 사용할 모든 풀에 로캘이 설정되어야 합니다. 최상위 IPAM 풀 내의 리전 풀을 통해 최상위 IPAM 풀을 생성하고 리전 풀의 탄력적 IP 주소에 공간을 할당하기 때문에 최상위 풀이 아닌 리전 풀에 로캘을 설정합니다. 이후 단계에서 리전 풀을 생성하는 경우 리전 풀에 로캘을 추가합니다.

Note

단일 풀만 생성하고 해당 풀 내에 리전 풀이 있는 최상위 풀을 생성하지 않는 경우 풀을 할당에 사용할 수 있도록 이 풀에 대한 로캘을 선택할 수 있습니다.

10. 퍼블릭 IP 소스에서 다음 옵션 중 하나를 선택합니다.
 - BYOIP: 기존 보유 IPv4 또는 IPv6 주소 범위(BYOIP)를 이 풀로 가져옵니다.
 - Amazon 소유: Amazon이 이 풀에 IPv6 주소 범위를 프로비저닝하기를 원합니다.
11. 다음 중 하나를 수행하십시오.
 - 이전 단계에서 BYOIP를 선택했다면 프로비저닝할 CIDR에서 풀에 프로비저닝할 CIDR을 선택합니다. 최상위 풀 내의 풀에 IPv4 CIDR을 프로비저닝하는 경우 프로비저닝할 수 있는 최소 IPv4 CIDR은 /24이며, 더 구체적인 CIDR(예: /25)은 허용되지 않습니다. CIDR, BYOIP 메시지

및 인증서 서명을 요청에 포함해야 사용자가 퍼블릭 공간을 소유하고 있는지 확인할 수 있습니다. 이 BYOIP 메시지 및 인증서 서명을 가져오는 방법을 포함한 BYOIP 사전 조건 목록은 [AWS 관리 콘솔과 AWS CLI를 모두 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#) 섹션을 참조하세요.

Important

대부분의 프로비저닝은 2시간 내에 완료되지만 공개적으로 알려진 범위에 대한 프로비저닝 프로세스를 완료하려면 최대 1주가 걸릴 수 있습니다.

- Amazon 소유를 선택했다면 넷마스크 길이에서 /40~/52 사이의 넷마스크 길이를 선택합니다. 기본값은 /52입니다.

12. 이 풀의 할당 규칙 설정 구성을 선택 취소된 상태로 둡니다.

13. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.

14. 풀 생성을 선택합니다.

계속하기 전에 이 CIDR이 프로비저닝되었는지 확인합니다. 풀 세부 정보 페이지의 CIDR(CIDRs) 탭에서 프로비저닝 상태를 볼 수 있습니다.

단계 3. 최상위 풀 내에 리전 풀 생성

최상위 풀 내에 리전 풀을 생성합니다. BYOIP와 IPAM을 통합하려면 BYOIP CIDR에 사용할 모든 풀에 로컬이 설정되어야 합니다. 이 단계에서 리전 풀을 생성하는 경우 리전 풀에 로컬을 추가합니다. Locale은 IPAM을 생성할 때 구성한 운영 리전 중 하나여야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

최상위 풀 내에 리전 풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 기본 개인 범위를 사용하지 않으려는 경우 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 풀 생성(Create pool)을 선택합니다.
5. (선택 사항) 풀에 대한 이름 태그(Name tag)와 설명(Description)을 추가합니다.
6. 소스에서 이전 섹션에서 생성한 최상위 풀을 선택합니다.

7. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
8. 로캘(Locale)에서 풀에 대한 로캘을 선택합니다. 이 자습서에서는 us-east-2를 리전 풀의 로캘로 사용합니다. 사용할 수 있는 옵션은 IPAM을 생성할 때 선택한 운영 리전에서 비롯된 것입니다.

로캘은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를 들어 VPC의 리전과 로캘을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로캘을 선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로캘이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다. 로캘을 선택하면 풀 및 풀에서 할당되는 리소스 간에 교차 리전 종속성이 없어집니다.
9. 서비스(Service)에서 EC2(EIP/VPC)를 선택합니다. 선택한 서비스에 따라 CIDR이 알릴 AWS 서비스가 결정됩니다. 현재, 유일한 옵션은 EC2(EIP/VPC)입니다. 즉, 이 풀에서 할당된 CIDR은 Amazon EC2 서비스(탄력적 IP 주소용) 및 Amazon VPC 서비스(VPC에 연결된 CIDR용)에 대해 알릴 수 있음을 의미합니다.
10. 프로비저닝할 CIDR(CIDRs to provision)에서 풀에 프로비저닝할 CIDR을 선택합니다. 최상위 풀 내의 풀에 CIDR을 프로비저닝하는 경우 프로비저닝할 수 있는 최소 IPv4 CIDR은 /24이며, 더 구체적인 CIDR(예: /25)은 허용되지 않습니다. 첫 번째 지역 풀을 만든 후 지역 풀 내에 더 작은 풀(예:/25)을 만들 수 있습니다.
11. 이 풀의 할당 규칙 설정 구성을 활성화합니다. 최상위 풀을 생성할 때와 동일한 할당 규칙 옵션이 여기에 적용됩니다. 풀을 생성할 때 사용할 수 있는 옵션에 대한 설명은 [최상위 IPv4 풀 생성](#) 섹션을 참조하세요. 리전 풀에 대한 할당 규칙은 최상위 풀에서 상속되지 않습니다. 여기에 규칙을 적용하지 않으면 풀에 대한 설정된 할당 규칙이 없어집니다.
12. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.
13. 풀 구성을 마쳤으면 풀 생성(Create pool)을 선택합니다.

계속하기 전에 이 CIDR이 프로비저닝되었는지 확인합니다. 풀 세부 정보 페이지의 CIDR(CIDRs) 탭에서 프로비저닝 상태를 볼 수 있습니다.

4단계. 리전 풀 공유

이 섹션의 단계에 따라 AWS Resource Access Manager(RAM)를 사용하여 IPAM 풀을 공유합니다.

AWS RAM에서 리소스 공유 활성화

IPAM을 생성한 후에는 리전 풀을 조직의 다른 계정과 공유할 수 있습니다. IPAM 풀을 공유하기 전에 이 단원의 단계를 완료하여 AWS RAM과 리소스 공유를 활성화합니다. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile management-account` 옵션을 사용합니다.

리소스 공유 활성화

1. AWS Organizations 관리 계정을 사용하여 <https://console.aws.amazon.com/ram/>에서 AWS RAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택하고 공유 활성화 범위 - AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

이제 IPAM 풀을 조직의 다른 멤버와 공유할 수 있습니다.

AWS RAM을 사용하여 IPAM 풀 공유

이 섹션에서는 리전 풀을 다른 AWS Organizations 멤버 계정과 공유합니다. 필수 IAM 권한에 대한 정보를 포함하여 IPAM 풀 공유에 대한 전체 지침은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile ipam-account` 옵션을 사용합니다.

AWS RAM을 사용하여 IPAM 풀 공유

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택하고, IPAM 풀을 선택하고, 작업 > 세부 정보 보기를 선택합니다.
4. 리소스 공유(Resource sharing)에서 리소스 공유 생성(Create resource share)을 선택합니다. AWS RAM 콘솔이 열립니다. AWS RAM을 사용하여 풀을 공유합니다.
5. 리소스 공유 생성(Create a resource share)을 선택합니다.
6. AWS RAM 콘솔에서 리소스 공유 생성을 다시 선택합니다.
7. 공유 풀에 대한 이름을 추가합니다.
8. 리소스 유형 선택에서 IPAM 풀을 선택한 다음에 공유하려는 풀의 ARN을 선택합니다.
9. Next(다음)를 선택합니다.
10. `AWSRAMPermissionIpamPoolByoipCidrImport` 권한을 선택합니다. 권한 옵션에 대한 세부 정보는 이 자습서의 범위를 벗어나지만 [AWS RAM을 사용하여 IPAM 풀 공유](#)에서 이러한 옵션에 대해 자세히 알아볼 수 있습니다.

11. Next(다음)를 선택합니다.
12. 보안 주체 > 보안 주체 유형 선택에서 AWS 계정을 선택하고 IP 주소 범위를 IPAM으로 가져올 계정의 계정 ID를 입력한 다음 추가를 선택합니다.
13. Next(다음)를 선택합니다.
14. 리소스 공유 옵션 및 공유할 보안 주체를 검토하고 생성을 선택합니다.
15. **member-account** 계정이 IPAM 풀에서 IP 주소 CIDRS를 할당할 수 있도록 하려면 `AWSRAMDefaultPermissionsIpamPool`으로 두 번째 리소스 공유를 생성하고 두 번째 리소스 공유를 생성합니다. `--resource-arns`의 값은 이전 섹션에서 생성한 IPAM 풀의 ARN입니다. `--principals` 값은 **member-account**의 계정 ID입니다. `--permission-arns`의 값은 `AWSRAMDefaultPermissionsIpamPool` 권한의 ARN입니다.

5단계: 퍼블릭 IPv4 풀 생성

퍼블릭 IPv4 풀 생성은 퍼블릭 IPv4 주소를 AWS로 가져와 IPAM을 사용하여 관리하는 필수 단계입니다. 이 단계는 탄력적 IP 주소를 프로비저닝할 멤버 계정으로 수행해야 합니다.

Important

- 이 단계는 AWS CLI를 사용하여 멤버 계정으로 수행해야 합니다.
- 퍼블릭 IPv4 풀 및 IPAM 풀은 AWS의 고유한 리소스에 의해 관리됩니다. 퍼블릭 IPv4 풀은 공개 소유의 CIDR을 탄력적 IP 주소로 변환할 수 있는 단일 계정 리소스입니다. IPAM 풀을 사용하여 퍼블릭 공간을 퍼블릭 IPv4 풀에 할당할 수 있습니다.

AWS CLI를 사용하여 퍼블릭 IPv4 풀 생성

- 다음 명령을 실행하여 CIDR을 프로비저닝합니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 `Locale` 옵션과 일치해야 합니다.

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

출력에 퍼블릭 IPv4 풀 ID가 표시됩니다. 다음 단계에서 이 ID를 사용합니다.

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

6단계: 퍼블릭 IPv4 CIDR을 퍼블릭 IPv4 풀에 프로비저닝

퍼블릭 IPv4 CIDR을 퍼블릭 IPv4 풀에 프로비저닝합니다. `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 `Locale` 값과 일치해야 합니다. `--netmask-length`는 퍼블릭 풀로 가져오려는 IPAM 풀의 공간 크기입니다. 이 값은 IPAM 풀의 넷마스크 길이보다 크기 않아야 합니다. 가져올 수 있는 가장 덜 구체적인 IPv4 접두사는 `/24`입니다.

Note

AWS Organization 전체에서 공유하기 위해 IPAM에 `/24` CIDR 범위를 가져오는 경우 이 자습서에 표시된 것처럼 전체 `/24` CIDR을 프로비저닝(`-- netmask-length 24` 사용)하는 대신 여러 IPAM 풀에 `/27`과 같은 더 작은 접두사를 프로비저닝(`-- netmask-length 27` 사용)할 수 있습니다.

Important

이 단계는 AWS CLI를 사용하여 멤버 계정으로 수행해야 합니다.

AWS CLI를 사용하여 퍼블릭 IPv4 풀 생성

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

```
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
```

출력에 프로비저닝된 CIDR이 표시됩니다.

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

2. 다음 명령을 실행하여 퍼블릭 IPv4 풀에 프로비저닝된 CIDR을 확인합니다.

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

출력에 프로비저닝된 CIDR이 표시됩니다. 기본적으로 CIDR은 알리지 않으므로 인터넷을 통해 공개적으로 액세스할 수 없습니다. 이 자습서의 마지막 단계에서 이 CIDR을 알리도록 설정할 수 있습니다.

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

퍼블릭 IPv4 풀을 생성한 후 IPAM 리전 풀에 할당된 퍼블릭 IPv4 풀을 보려면 IPAM 콘솔을 열고 할당 (Allocations) 또는 리소스(Resources) 아래의 리전 풀에서 할당을 확인합니다.

7단계: 퍼블릭 IPv4 풀에서 탄력적 IP 주소 생성

Amazon EC2 사용 설명서의 [탄력적 IP 주소 할당](#) 단계에 따라 퍼블릭 IPv4 풀에서 탄력적 IP 주소(EIP)를 생성하세요. AWS 관리 콘솔에서 EC2를 열 때 EIP를 할당하는 AWS 리전은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 Locale 옵션과 일치해야 합니다.

이 단계는 멤버 계정으로 수행해야 합니다. AWS CLI를 사용하는 경우 `--profile member-account` 옵션을 사용합니다.

8단계: EC2 인스턴스와 탄력적 IP 주소 연결

Amazon EC2 사용 설명서의 [인스턴스 또는 네트워크 인터페이스에 탄력적 IP 주소 연결](#) 단계에 따라 EIP를 EC2 인스턴스와 연결하세요. AWS 관리 콘솔에서 EC2를 열 때 EIP를 연결하는 AWS 리전은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 Locale 옵션과 일치해야 합니다. 이 자습서에서는 해당 풀이 리전 풀입니다.

이 단계는 멤버 계정으로 수행해야 합니다. AWS CLI를 사용하는 경우 `--profile member-account` 옵션을 사용합니다.

9단계: CIDR 알리기

이 섹션의 단계는 IPAM 계정에서 수행해야 합니다. 탄력적 IP 주소(EIP)를 인스턴스 또는 Elastic Load Balancer와 연결하면 서비스 EC2(EIP/VPC)가 구성된 풀에 있는 AWS로 가져온 CIDR 알림을 시작할 수 있습니다. 이 자습서에서는 리전 풀이 해당됩니다. 기본적으로 CIDR은 알리지 않으므로 인터넷을 통해 공개적으로 액세스할 수 없습니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

CIDR 알리기

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 이 자습서에서 생성한 리전 풀을 선택합니다.
5. CIDR 탭을 선택합니다.
6. BYOIP CIDR을 선택하고 작업(Actions) > 알리기(Advertise)를 선택합니다.
7. CIDR 알리기(Advertise CIDR)를 선택합니다.

결과적으로 BYOIP CIDR이 알려지고 알림(Advertising) 열의 값이 철회됨(Withdrawn)에서 알려짐(Advertised)으로 변경됩니다.

10단계: 정리

이번 섹션의 단계를 따르면 이 자습서에서 프로비저닝하고 생성한 리소스를 정리할 수 있습니다.

1단계: 알림에서 CIDR 철회

이 단계는 IPAM 계정으로 수행해야 합니다.

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 퍼블릭 범위를 선택합니다.
4. 이 자습서에서 생성한 리전 풀을 선택합니다.
5. CIDR 탭을 선택합니다.
6. BYOIP CIDR을 선택하고 작업(Actions) > 알림에서 철회(Withdraw from advertising)를 선택합니다.
7. CIDR 철회(Withdraw CIDR)를 선택합니다.

결과적으로 BYOIP CIDR이 더 이상 알려지지 않고 알림(Advertising) 열의 값이 알려짐(Advertised)에서 철회됨(Withdrawn)으로 변경됩니다.

2단계: 탄력적 IP 주소 연결 해제

이 단계는 멤버 계정으로 수행해야 합니다. AWS CLI를 사용하는 경우 `--profile member-account` 옵션을 사용합니다.

- Amazon EC2 사용 설명서의 [탄력적 IP 주소 연결 해제](#) 단계에 따라 EIP를 연결 해제하세요. AWS 관리 콘솔에서 EC2를 열 때 EIP를 연결 해제하는 AWS 리전은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 Local 옵션과 일치해야 합니다. 이 자습서에서는 해당 풀이 리전 풀입니다.

3단계: 탄력적 IP 주소 해제

이 단계는 멤버 계정으로 수행해야 합니다. AWS CLI를 사용하는 경우 `--profile member-account` 옵션을 사용합니다.

- Amazon EC2 사용 설명서의 [탄력적 IP 주소 릴리스](#) 단계에 따라 퍼블릭 IPv4 풀에서 탄력적 IP 주소(EIP)를 릴리스하세요. AWS 관리 콘솔에서 EC2를 열 때 EIP를 할당하는 AWS 리전은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 Local 옵션과 일치해야 합니다.

4단계: 퍼블릭 IPv4 풀에서 퍼블릭 IPv4 CIDR 프로비저닝 해제

Important

이 단계는 AWS CLI를 사용하여 멤버 계정으로 수행해야 합니다.

1. BYOIP CIDR을 확인합니다.

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

출력에 BYOIP CIDR의 IP 주소가 표시됩니다.

```
{
  "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. 다음 명령을 실행하여 퍼블릭 IPv4 풀에서 CIDR의 마지막 IP 주소를 해제합니다. 넷마스크가 /32인 IP 주소를 입력합니다.

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

출력에 프로비저닝 해제된 CIDR이 표시됩니다.

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

```

    "130.137.245.255"
  ]
}

```

Important

CIDR 범위의 각 IP 주소에 대해 이 명령을 다시 실행해야 합니다. CIDR이 /24인 경우 이 명령을 실행하여 /24 CIDR의 256개 IP 주소 각각을 프로비저닝 해제해야 합니다.

3. BYOIP CIDR을 다시 확인하고 프로비저닝된 주소가 더 이상 없는지 확인합니다. 이 섹션의 명령을 실행하는 경우 --region의 값은 IPAM 리전과 일치해야 합니다.

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

출력에 퍼블릭 IPv4 풀의 IP 주소 수가 표시됩니다.

```

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

```

Note

IPAM이 퍼블릭 IPv4 풀 할당이 제거되었음을 발견하는 데 어느 정도 시간이 걸릴 수 있습니다. IPAM에서 할당이 제거됐는지 확인할 때까지 IPAM 풀 CIDR을 정리하고 프로비저닝 해제할 수 없습니다.

5단계: 퍼블릭 IPv4 풀 삭제

이 단계는 멤버 계정으로 수행해야 합니다.

- 다음 명령을 실행하여 CIDR의 퍼블릭 IPv4 풀을 삭제합니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 Locale 옵션과 일치해야 합니다. 이 자습서에서는 해당 풀이 리전 풀입니다. 이 단계는 AWS CLI를 사용하여 수행해야 합니다.

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

출력에서 반환 값이 true임을 확인할 수 있습니다.

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

풀을 삭제한 후 IPAM에서 관리하지 않는 할당을 보려면 IPAM 콘솔을 열고 할당(Allocations)에서 리전 풀의 세부 정보를 확인합니다.

6단계: RAM 공유 삭제 및 AWS Organizations와의 RAM 통합 사용 중지

이 단계는 각각 IPAM 계정과 관리 계정으로 수행해야 합니다. AWS CLI를 사용하여 RAM 공유를 삭제하고 RAM 통합을 사용 중지하는 경우 `--profile ipam-account` 및 `--profile management-account` 옵션을 사용합니다.

- AWS RAM 사용 설명서의 [AWS RAM의 리소스 공유 삭제](#) 및 [AWS Organizations와의 리소스 공유 비활성화](#)의 단계를 순서대로 완료하여 RAM 공유를 삭제하고 AWS Organizations와의 RAM 통합을 사용 중지합니다.

7단계: 리전 풀 및 최상위 풀에서 CIDR 프로비저닝 해제

이 단계는 IPAM 계정으로 수행해야 합니다. AWS CLI를 사용하여 풀을 공유하는 경우 `--profile ipam-account` 옵션을 사용합니다.

- [풀에서 CIDR 프로비저닝 해제](#)의 단계에 따라 리전 풀과 최상위 풀에서 순서대로 CIDR을 프로비저닝 해제하세요.

8단계: 리전 풀 및 최상위 풀 삭제

이 단계는 IPAM 계정으로 수행해야 합니다. AWS CLI를 사용하여 풀을 공유하는 경우 `--profile ipam-account` 옵션을 사용합니다.

- [풀 삭제](#)의 단계에 따라 리전 풀과 최상위 풀을 순서대로 삭제하세요.

AWS 관리 콘솔을 모두 사용하여 IPAM으로 고유 IPv6 CIDR 가져오기

이 자습서의 단계에 따라 IPv6 CIDR을 IPAM으로 가져오고 AWS Management 콘솔 및 AWS CLI를 사용하여 CIDR과 함께 VPC를 할당하세요.

Important

- 지금은 Local Zones에서 BYOIP 주소 범위를 프로비저닝하거나 홍보할 수 없습니다.
- 이 자습서에서는 다음 섹션의 단계를 이미 수행한 것으로 가정합니다.
 - [AWS Organization에서 계정과 IPAM 통합](#).
 - [IPAM 생성](#).
- 이 자습서의 각 단계는 다음 3개의 AWS Organizations 계정 중 하나로 수행해야 합니다.
 - 관리 계정.
 - [AWS Organization에서 계정과 IPAM 통합](#)에서 IPAM 관리자로 구성된 멤버 계정. 이 자습서에서는 이 계정을 IPAM 계정이라고 합니다.
 - IPAM 풀에서 CIDR을 할당할 조직의 멤버 계정입니다. 이 자습서에서는 이 계정을 멤버 계정이라고 합니다.

내용

- [1단계: 최상위 IPAM 풀 생성](#)
- [단계 2. 최상위 풀 내에 리전 풀 생성](#)
- [단계 3. 리전 풀 공유](#)
- [4단계: VPC 생성](#)
- [5단계: CIDR 알리기](#)
- [6단계: 정리](#)

1단계: 최상위 IPAM 풀 생성

최상위 IPAM 풀 내의 리전 풀을 통해 최상위 IPAM 풀을 생성하고 리전 풀의 리소스에 공간을 할당하기 때문에 최상위 풀이 아닌 리전 풀에 로컬을 설정합니다. 이후 단계에서 리전 풀을 생성하는 경우 리전 풀에 로컬을 추가합니다. BYOIP와 IPAM을 통합하려면 BYOIP CIDR에 사용할 모든 풀에 로컬이 설정되어야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 풀 생성(Create pool)을 선택합니다.
5. (선택 사항) 풀에 대한 이름 태그(Name tag)와 설명(Description)을 추가합니다.
6. 소스에서 IPAM 범위를 선택합니다.
7. 주소 패밀리(Address family)에서 IPv6를 선택합니다.

IPv6을 선택하면 AWS가 이 풀에서 CIDR을 공개적으로 광고할 수 있는지 여부를 제어할 수 있는 전환 옵션이 나타납니다. 이 옵션을 활성화된 상태로 둡니다.

8. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
9. 이 풀의 CIDR을 공개적으로 알릴 수 있도록 허용이 선택되어 있는지 확인합니다.
10. 로컬(Locale)에서 없음(None)을 선택합니다. 리전 풀에서 로컬을 설정합니다.

로컬은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를 들어 VPC의 리전과 로컬을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로컬을 선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로컬이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다.

Note

단일 풀만 생성하고 해당 풀 내에 리전 풀이 있는 최상위 풀을 생성하지 않는 경우 풀을 할당에 사용할 수 있도록 이 풀에 대한 로컬을 선택할 수 있습니다.

11. 퍼블릭 IP 소스에는 기본적으로 BYOIP가 선택되어 있습니다.
12. 프로비저닝할 CIDR(CIDRs to provision)에서 풀에 프로비저닝할 CIDR을 선택합니다. 최상위 풀 내의 풀에 IPv6 CIDR를 프로비저닝할 때 가져올 수 있는 가장 구체적인 IPv6 주소 범위는 공개적으로 알려진 CIDR의 경우 /48이고 공개적으로 알려지지 않은 CIDR의 경우 /60입니다. CIDR, BYOIP 메시지 및 인증서 서명을 요청에 포함해야 사용자가 퍼블릭 공간을 소유하고 있는지 확인할 수 있습니다. 이 BYOIP 메시지 및 인증서 서명을 가져오는 방법을 포함한 BYOIP 사전 조건 목록은 [AWS 관리 콘솔과 AWS CLI를 모두 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#) 섹션을 참조하세요.

Important

대부분의 프로비저닝은 2시간 내에 완료되지만 공개적으로 알려진 범위에 대한 프로비저닝 프로세스를 완료하려면 최대 1주가 걸릴 수 있습니다.

13. 이 풀의 할당 규칙 설정 구성을 선택 취소된 상태로 둡니다.
14. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.
15. 풀 생성을 선택합니다.

계속하기 전에 이 CIDR이 프로비저닝되었는지 확인합니다. 풀 세부 정보 페이지의 CIDR(CIDRs) 탭에서 프로비저닝 상태를 볼 수 있습니다.

단계 2. 최상위 풀 내에 리전 풀 생성

최상위 풀 내에 리전 풀을 생성합니다. 로컬은 풀에 필요하며 IPAM을 생성할 때 구성된 운영 리전 중 하나여야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

최상위 풀 내에 리전 풀을 생성하려면

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 기본 개인 범위를 사용하지 않으려는 경우 콘텐츠 창 상단의 드롭다운 메뉴에서 사용할 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 풀 생성(Create pool)을 선택합니다.
5. (선택 사항) 풀에 대해 이름 태그(Name tag) 및 풀에 대한 자세한 내용을 추가합니다.

6. 소스에서 이전 섹션에서 생성한 최상위 풀을 선택합니다.
7. 리소스 계획에서 범위 내에서 IP 공간 계획을 선택한 상태로 둡니다. 이 옵션을 사용하여 VPC 내 서브넷 IP 공간을 계획하는 방법에 대한 자세한 내용은 [자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획](#)를 참조하세요.
8. 풀의 로컬을 선택합니다. 로컬을 선택하면 풀 및 풀에서 할당되는 리소스 간에 교차 리전 종속성이 없어집니다. 사용할 수 있는 옵션은 IPAM을 생성할 때 선택한 운영 리전에서 비롯된 것입니다. 이 자습서에서는 us-east-2를 리전 풀의 로컬로 사용합니다.

로컬은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를 들어 VPC의 리전과 로컬을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로컬을 선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로컬이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다.

9. 서비스(Service)에서 EC2(EIP/VPC)를 선택합니다. 선택한 서비스에 따라 CIDR이 알릴 AWS 서비스가 결정됩니다. 현재, 유일한 옵션은 EC2 (EIP/VPC)입니다. 즉, 이 풀에서 할당된 CIDR은 Amazon EC2 서비스 및 Amazon VPC 서비스(VPC에 연결된 CIDR용)에 대해 알릴 수 있음을 의미합니다.
10. 프로비저닝할 CIDR(CIDRs to provision)에서 풀에 프로비저닝할 CIDR을 선택합니다. 최상위 풀 내의 풀에 IPv6 CIDR를 프로비저닝할 때 가져올 수 있는 가장 구체적인 IPv6 주소 범위는 공개적으로 알려진 CIDR의 경우 /48이고 공개적으로 알려지지 않은 CIDR의 경우 /60입니다.
11. 이 풀의 할당 규칙 설정 구성을 활성화하고 풀에 대한 선택적 할당 규칙을 선택합니다.
 - 검색된 리소스 자동으로 가져오기(Automatically import discovered resources): 이 옵션은 로컬(Locale)이 없음(None)으로 설정된 경우 사용할 수 없습니다. 이 옵션을 선택하면 IPAM은 이 풀의 CIDR 범위 내에 있는 리소스를 지속적으로 찾아서 자동으로 IPAM에 할당으로 가져옵니다. 유의할 사항:
 - 가져오기가 성공하려면 이러한 리소스에 할당될 CIDR이 아직 다른 리소스에 할당되지 않아야 합니다.
 - IPAM은 풀의 할당 규칙 관련 규정 준수 여부에 관계없이 CIDR을 가져오므로 리소스를 가져온 다음 비준수로 표시될 수 있습니다.
 - IPAM이 겹치는 여러 CIDR을 검색하는 경우 IPAM은 가장 큰 CIDR만 가져옵니다.
 - IPAM이 일치하는 CIDR이 있는 여러 개의 CIDR을 검색하는 경우 IPAM은 그중 하나만 임의로 가져옵니다.
 - 최소 넷마스크 길이(Minimum netmask length): 준수할 이 IPAM 풀의 CIDR 할당에 필요한 최소 넷마스크 길이 및 풀에서 할당할 수 있는 최대 크기의 CIDR 블록입니다. 최소 넷마스크 길이는

최대 넷마스크 길이보다 작아야 합니다. IPv4 주소에 사용할 수 있는 넷마스크 길이는 0~32입니다. IPv6 주소에 사용할 수 있는 넷마스크 길이는 0~128입니다.

- 기본 넷마스크 길이(Default netmask length): 이 풀에 추가된 할당의 기본 넷마스크 길이입니다.
- 최대 넷마스크 길이(Maximum netmask length): 이 풀의 CIDR 할당에 필요한 최대 넷마스크 길이입니다. 이 값은 풀에서 할당할 수 있는 가장 작은 크기의 CIDR 블록을 지정합니다. 이 값이 최소 /48인지 확인합니다.
- 태그 지정 요구 사항(Tagging requirements): 리소스가 풀에서 공간을 할당하는 데 필요한 태그입니다. 리소스가 공간을 할당한 후 태그를 변경하거나 할당 태그 지정 규칙이 풀에서 변경된 경우 리소스를 비준수로 표시할 수 있습니다.
- 로캘(Locale): 이 풀의 CIDR을 사용하는 리소스에 필요한 로캘입니다. 자동으로 가져온 리소스에 이 로캘이 없는 경우 비준수로 표시됩니다. 풀로 자동으로 가져오지 않은 리소스는 이 로캘에 있지 않으면 풀에서 공간을 할당할 수 없습니다.

12. (선택 사항) 풀에 대한 태그(Tags)를 선택합니다.

13. 풀 구성을 마쳤으면 풀 생성(Create pool)을 선택합니다.

계속하기 전에 이 CIDR이 프로비저닝되었는지 확인합니다. 풀 세부 정보 페이지의 CIDR(CIDRs) 탭에서 프로비저닝 상태를 볼 수 있습니다.

단계 3. 리전 풀 공유

이 섹션의 단계에 따라 AWS Resource Access Manager(RAM)를 사용하여 IPAM 풀을 공유합니다.

AWS RAM에서 리소스 공유 활성화

IPAM을 생성한 후에는 리전 풀을 조직의 다른 계정과 공유할 수 있습니다. IPAM 풀을 공유하기 전에 이 단원의 단계를 완료하여 AWS RAM과 리소스 공유를 활성화합니다. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile management-account` 옵션을 사용합니다.

리소스 공유 활성화

1. AWS Organizations 관리 계정을 사용하여 <https://console.aws.amazon.com/ram/>에서 AWS RAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택하고 공유 활성화 범위 - AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

이제 IPAM 풀을 조직의 다른 멤버와 공유할 수 있습니다.

AWS RAM을 사용하여 IPAM 풀 공유

이 섹션에서는 리전 풀을 다른 AWS Organizations 멤버 계정과 공유합니다. 필수 IAM 권한에 대한 정보를 포함하여 IPAM 풀 공유에 대한 전체 지침은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile ipam-account` 옵션을 사용합니다.

AWS RAM을 사용하여 IPAM 풀 공유

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택하고, IPAM 풀을 선택하고, 작업 > 세부 정보 보기를 선택합니다.
4. 리소스 공유(Resource sharing)에서 리소스 공유 생성(Create resource share)을 선택합니다. AWS RAM 콘솔이 열립니다. AWS RAM을 사용하여 풀을 공유합니다.
5. 리소스 공유 생성(Create a resource share)을 선택합니다.
6. AWS RAM 콘솔에서 리소스 공유 생성을 다시 선택합니다.
7. 공유 풀에 대한 이름을 추가합니다.
8. 리소스 유형 선택에서 IPAM 풀을 선택한 다음에 공유하려는 풀의 ARN을 선택합니다.
9. Next(다음)를 선택합니다.
10. AWSRAMPermissionIpamPoolByoipCidrImport 권한을 선택합니다. 권한 옵션에 대한 세부 정보는 이 자습서의 범위를 벗어나지만 [AWS RAM을 사용하여 IPAM 풀 공유](#)에서 이러한 옵션에 대해 자세히 알아볼 수 있습니다.
11. Next(다음)를 선택합니다.
12. 보안 주체 > 보안 주체 유형 선택에서 AWS 계정을 선택하고 IP 주소 범위를 IPAM으로 가져올 계정의 계정 ID를 입력한 다음 추가를 선택합니다.
13. Next(다음)를 선택합니다.
14. 리소스 공유 옵션 및 공유할 보안 주체를 검토하고 생성을 선택합니다.
15. **member-account** 계정이 IPAM 풀에서 IP 주소 CIDRS를 할당할 수 있도록 하려면 `AWSRAMDefaultPermissionsIpamPool`으로 두 번째 리소스 공유를 생성하고 두 번째 리소스 공유를 생성합니다. `--resource-arns`의 값은 이전 섹션에서 생성한 IPAM 풀의 ARN입니다. `--principals` 값은 **member-account**의 계정 ID입니다. `--permission-arns`의 값은 `AWSRAMDefaultPermissionsIpamPool` 권한의 ARN입니다.

4단계: VPC 생성

Amazon VPC 사용 설명서의 [VPC 생성](#) 단계를 수행하세요.

이 단계는 멤버 계정으로 수행해야 합니다.

Note

- AWS 관리 콘솔에서 VPC를 열 때 VPC를 생성하는 AWS 리전은 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 Locale 옵션과 일치해야 합니다.
- VPC 대한 CIDR을 선택하는 단계를 완료하면 IPAM 풀의 CIDR을 사용할 수 있는 옵션이 제공됩니다. 이 자습서에서 생성한 리전 풀을 선택합니다.

VPC를 생성할 때 AWS는 IPAM 풀의 CIDR을 VPC에 할당합니다. IPAM 콘솔의 콘텐츠 창에서 풀을 선택하고 풀의 할당(Allocations) 탭을 보면 IPAM에서 할당을 확인할 수 있습니다.

5단계: CIDR 알리기

이 섹션의 단계는 IPAM 계정에서 수행해야 합니다. VPC를 생성하면 서비스 EC2(EIP/VPC)(Service EC2 (EIP/VPC))가 구성된 풀에 있는 AWS로 가져온 CIDR 알림을 시작할 수 있습니다. 이 자습서에서는 리전 풀이 해당됩니다. 기본적으로 CIDR은 알리지 않으므로 인터넷을 통해 공개적으로 액세스할 수 없습니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

CIDR 알리기

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 퍼블릭 범위를 선택합니다. 범위에 대한 자세한 내용은 [IPAM 작동 방식](#) 섹션을 참조하세요.
4. 이 자습서에서 생성한 리전 풀을 선택합니다.
5. CIDR 탭을 선택합니다.
6. BYOIP CIDR을 선택하고 작업(Actions) > 알리기(Advertise)를 선택합니다.
7. CIDR 알리기(Advertise CIDR)를 선택합니다.

결과적으로 BYOIP CIDR이 알려지고 알림(Advertising) 열의 값이 철회됨(Withdrawn)에서 알려짐(Advertised)으로 변경됩니다.

6단계: 정리

이번 섹션의 단계를 따르면 이 자습서에서 프로비저닝하고 생성한 리소스를 정리할 수 있습니다.

1단계: 알림에서 CIDR 철회

이 단계는 IPAM 계정으로 수행해야 합니다.

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 기본적으로 풀을 생성하는 경우 기본 프라이빗 범위가 선택됩니다. 퍼블릭 범위를 선택합니다.
4. 이 자습서에서 생성한 리전 풀을 선택합니다.
5. CIDR 탭을 선택합니다.
6. BYOIP CIDR을 선택하고 작업(Actions) > 알림에서 철회(Withdraw from advertising)를 선택합니다.
7. CIDR 철회(Withdraw CIDR)를 선택합니다.

결과적으로 BYOIP CIDR이 더 이상 알려지지 않고 알림(Advertising) 열의 값이 알려짐(Advertised)에서 철회됨(Withdrawn)으로 변경됩니다.

2단계: VPC 삭제

이 단계는 멤버 계정으로 수행해야 합니다.

- Amazon VPC 사용 설명서의 [Deleting a VPC\(VPC 삭제\)](#) 단계에 따라 VPC를 삭제하세요. AWS 관리 콘솔에서 VPC를 열 때 AWS 리전의 VPC 삭제 위치는 BYOIP CIDR에 사용할 풀을 생성할 때 선택한 Local 옵션과 일치해야 합니다. 이 자습서에서는 해당 풀이 리전 풀입니다.

VPC를 삭제하면 IPAM이 리소스가 삭제되었음을 발견하고 VPC에 할당된 CIDR을 할당 해제하는데 시간이 걸립니다. 풀 세부 정보 할당(Allocations) 탭에서 IPAM이 풀에서 할당을 제거했음을 확인할 때까지 정리의 다음 단계를 계속할 수 없습니다.

3단계: RAM 공유 삭제 및 AWS Organizations와의 RAM 통합 사용 중지

이 단계는 각각 IPAM 계정과 관리 계정으로 수행해야 합니다.

- AWS RAM 사용 설명서의 [AWS RAM의 리소스 공유 삭제](#) 및 [AWS Organizations와의 리소스 공유 비활성화](#)의 단계를 순서대로 완료하여 RAM 공유를 삭제하고 AWS Organizations와의 RAM 통합을 사용 중지합니다.

4단계: 리전 풀 및 최상위 풀에서 CIDR 프로비저닝 해제

이 단계는 IPAM 계정으로 수행해야 합니다.

- [풀에서 CIDR 프로비저닝 해제](#)의 단계에 따라 리전 풀과 최상위 풀에서 순서대로 CIDR을 프로비저닝 해제하세요.

5단계: 리전 풀 및 최상위 풀 삭제

이 단계는 IPAM 계정으로 수행해야 합니다.

- [풀 삭제](#)의 단계에 따라 리전 풀과 최상위 풀을 순서대로 삭제하세요.

AWS CLI만 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기

다음 단계에 따라 AWS CLI만 사용하여 IPv4 또는 IPv6 CIDR을 IPAM으로 가져옵니다.

Important

- 이 자습서를 시작하기 전에 Amazon EC2 사용 설명서의 [BYOIP 주소 범위에 대한 온보딩 사전 조건](#)의 단계를 완료하세요.

ROA를 생성할 때 IPv4 CIDR의 경우 IP 주소 접두사의 최대 길이를 /24로 설정해야 합니다. IPv6 CIDR의 경우 알릴 수 있는 풀에 해당 CIDR을 추가하면 IP 주소 접두사의 최대 길이는 /48여야 합니다. 이렇게 하면 퍼블릭 IP 주소를 AWS 리전 전체에 걸쳐 충분히 유연하게 분할할 수 있습니다. IPAM은 사용자가 설정한 최대 길이를 적용합니다. 최대 길이는 이 라우팅에 허용되는 가장 작은 접두사 길이 알림입니다. 예를 들어 /20 CIDR 블록을 AWS로 가져오는 경우 최대 길이를 /24로 설정하여 원하는 대로 더 큰 블록(예: /21, /22 또는 /24)을 분할하고, 더 작은 CIDR 블록을 모든 리전에 배포할 수 있습니다. 최대 길이를 /23으로 설정하는 경우 더 큰 블록의 /24를 분할하여 알릴 수 없게 됩니다. 또한, /24는 가장 작은 IPv4 블록이며 /48은 리전에서 인터넷으로 알릴 수 있는 가장 작은 IPv6 블록입니다.

- 사용하여 AWS로 IPv4 주소 범위를 가져오면 첫 번째 주소(네트워크 주소)와 마지막 주소(브로드캐스트 주소)를 포함하여 범위 내의 IP 주소를 모두 사용할 수 있습니다.

내용

- [AWS CLI만 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#)
- [AWS CLI만 사용하여 IPAM으로 고유 IPv6 CIDR 가져오기](#)

AWS CLI만 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기

다음 단계에 따라 IPv4 CIDR을 IPAM으로 가져오고 AWS CLI만 사용하여 CIDR과 함께 탄력적 IP 주소 (EIP)를 할당하세요.

Important

- 지금은 Local Zones에서 BYOIP 주소 범위를 프로비저닝하거나 홍보할 수 없습니다.
- 이 자습서에서는 다음 섹션의 단계를 이미 수행한 것으로 가정합니다.
 - [AWS Organization에서 계정과 IPAM 통합](#).
 - [IPAM 생성](#).
- 이 자습서의 각 단계는 다음 3개의 AWS Organizations 계정 중 하나로 수행해야 합니다.
 - 관리 계정.
 - [AWS Organization에서 계정과 IPAM 통합](#)에서 IPAM 관리자로 구성된 멤버 계정. 이 자습서에서는 이 계정을 IPAM 계정이라고 합니다.
 - IPAM 풀에서 CIDR을 할당할 조직의 멤버 계정입니다. 이 자습서에서는 이 계정을 멤버 계정이라고 합니다.

내용

- [1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성](#)
- [2단계: IPAM 생성](#)
- [3단계: 최상위 IPAM 풀 생성](#)
- [4단계: 최상위 풀에 CIDR 프로비저닝](#)
- [5단계: 최상위 풀 내에 리전 풀 생성](#)
- [6단계: 리전 풀에 CIDR 프로비저닝](#)
- [7단계. 리전 풀 공유](#)
- [8단계: 퍼블릭 IPv4 풀 생성](#)

- [9단계: 퍼블릭 IPv4 CIDR을 퍼블릭 IPv4 풀에 프로비저닝](#)
- [10단계: 퍼블릭 IPv4 풀에서 탄력적 IP 주소 생성](#)
- [11단계: CIDR 알리기](#)
- [12단계: 정리](#)

1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성

단일 AWS 사용자로 이 자습서를 완료하려면 AWS CLI 명령 프로파일을 사용하여 IAM 역할 간에 전환할 수 있습니다. [명명 프로파일](#)은 AWS CLI와(과) 함께 `--profile` 옵션을 사용할 때 참조하는 설정 및 보안 인증 정보의 모음입니다. AWS 계정에 대한 IAM 역할 및 명명 프로파일 생성 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [AWS CLI에서 IAM 역할 사용](#)을 참조하세요.

이 자습서에서 사용할 세 AWS 계정 각각에 대해 역할 하나와 명명 프로필 하나를 만듭니다:

- AWS Organizations 관리 계정에 대한 `management-account`라는 프로파일
- IPAM 관리자로 구성된 AWS Organizations 멤버 계정의 `ipam-account`라는 프로파일
- IPAM 풀에서 CIDR을 할당할 조직의 AWS Organizations 멤버 계정에 대한 `member-account`라는 프로파일

IAM 역할 및 명명 프로파일을 생성한 후 이 페이지로 돌아와서 다음 단계로 이동합니다. 이 자습서의 나머지 부분에서 샘플 AWS CLI 명령이 명명된 프로파일 중 하나와 함께 `--profile` 옵션을 사용하여 명령을 실행해야 하는 계정을 나타냅니다.

2단계: IPAM 생성

이 단계는 선택 사항입니다. `us-east-1`과 `us-west-2`의 운영 리전에서 생성된 IPAM이 이미 있는 경우 이 단계를 건너뛸 수 있습니다. IPAM을 생성하고 `us-east-1`과 `us-west-2`의 운영 리전을 지정합니다. IPAM 풀을 생성하는 경우 로컬 옵션을 사용할 수 있도록 운영 리전을 선택해야 합니다. BYOIP와 IPAM을 통합하려면 BYOIP CIDR에 사용할 모든 풀에 로컬이 설정되어야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

다음 명령을 실행합니다:

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

출력에 생성한 IPAM이 표시됩니다. `PublicDefaultScopeId`의 값을 기록해 둡니다. 다음 단계에서 퍼블릭 범위 ID가 필요합니다. BYOIP CIDR은 퍼블릭 범위가 의미하는 것인 퍼블릭 IP 주소이기 때문에 퍼블릭 범위를 사용하고 있습니다.

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

3단계: 최상위 IPAM 풀 생성

이 섹션의 단계에 따라 최상위 IPAM 풀을 생성하세요.

이 단계는 IPAM 계정으로 수행해야 합니다.

AWS CLI를 사용하여 모든 AWS 리소스에 대한 IPv4 주소 풀 생성

1. 다음 명령을 실행하여 IPAM 풀을 생성합니다. 이전 단계에서 생성한 IPAM의 퍼블릭 범위 ID를 사용합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
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
```

출력에 풀 생성이 진행 중임을 나타내는 `create-in-progress`가 표시됩니다.

```
{
  "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. 출력에 `create-complete`의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

다음 예 출력에서는 풀의 상태를 보여줍니다.

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

```

4단계: 최상위 풀에 CIDR 프로비저닝

최상위 풀에 CIDR을 프로비저닝합니다. 최상위 풀 내의 풀에 IPv4 CIDR을 프로비저닝하는 경우 프로비저닝할 수 있는 최소 IPv4 CIDR은 /24이며, 더 구체적인 CIDR(예: /25)은 허용되지 않습니다. CIDR, BYOIP 메시지 및 인증서 서명을 요청에 포함해야 사용자가 퍼블릭 공간을 소유하고 있는지 확인할 수 있습니다. 이 BYOIP 메시지 및 인증서 서명을 가져오는 방법을 포함한 BYOIP 사전 조건 목록은 [AWS CLI만 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#) 섹션을 참조하세요.

이 단계는 IPAM 계정으로 수행해야 합니다.

Important

BYOIP CIDR을 최상위 풀에 프로비저닝하는 경우 `--cidr-authorization-context`를 추가하기만 하면 됩니다. 최상위 풀 내에 있는 지역 풀의 경우 `--cidr-authorization-context` 옵션을 생략할 수 있습니다. 일단 BYOIP를 IPAM에 온보드하면 리전 및 계정에서 BYOIP를 나눌 때 소유권 확인을 수행할 필요가 없습니다.

AWS CLI를 사용하여 CIDR 블록을 풀에 프로비저닝하기

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

```

aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --cidr-authorization-
context Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrnGM~cvGx~KCIsmAU0P7EN07VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRY0dRaNx8yt-uoZWzxc2yIhWngy-
du9pnEHB0X6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXE1T5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZ1afBbrFxrjFWRCTJhc7Cg3ASbR0-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account

```

출력에 프로비저닝이 보류 중인 CIDR이 표시됩니다.

```
{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "pending-provision"
  }
}
```

2. 계속하기 전에 이 CIDR이 프로비저닝되었는지 확인합니다.

⚠ Important

대부분의 프로비저닝은 2시간 내에 완료되지만 공개적으로 알려진 범위에 대한 프로비저닝 프로세스를 완료하려면 최대 1주가 걸릴 수 있습니다.

출력에 provisioned의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

다음 예 출력에서는 상태를 보여줍니다.

```
{
  "IpamPoolCidrs": [
    {
      "Cidr": "130.137.245.0/24",
      "State": "provisioned"
    }
  ]
}
```

5단계: 최상위 풀 내에 리전 풀 생성

최상위 풀 내에 리전 풀을 생성합니다. --locale은 풀에 필요하며 IPAM을 생성할 때 구성된 운영 리전 중 하나여야 합니다. 로캘은 이 IPAM 풀을 할당에 사용할 수 있도록 하려는 AWS 리전입니다. 예를

들어 VPC의 리전과 로컬을 공유하는 IPAM 풀의 VPC에 대한 CIDR만 할당할 수 있습니다. 풀에 대한 로컬을 선택한 경우에는 수정할 수 없습니다. 중단으로 인해 IPAM의 홈 리전을 사용할 수 없고 풀의 로컬이 IPAM의 홈 리전과 다른 경우에도 여전히 풀을 사용하여 IP 주소를 할당할 수 있습니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

로컬을 선택하면 풀 및 풀에서 할당되는 리소스 간에 교차 리전 종속성이 없어집니다. 사용할 수 있는 옵션은 IPAM을 생성할 때 선택한 운영 리전에서 비롯된 것입니다. 이 자습서에서는 us-west-2를 리전 풀의 로컬로 사용합니다.

Important

풀을 생성하는 경우 `--aws-service ec2`(를) 포함해야 합니다. 선택한 서비스에 따라 CIDR이 알릴 AWS 서비스가 결정됩니다. 현재, 유일한 옵션은 ec2입니다. 즉, 이 풀에서 할당된 CIDR은 Amazon EC2 서비스(탄력적 IP 주소용) 및 Amazon VPC 서비스(VPC에 연결된 CIDR용)에 대해 알릴 수 있음을 의미합니다.

AWS CLI를 사용하여 리전 풀을 생성하려면

1. 다음 명령을 실행하여 풀을 생성합니다.

```
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
```

출력에 풀을 생성하는 IPAM이 표시됩니다.

```
{
  "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. 출력에 `create-complete`의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

출력에는 IPAM에 있는 풀이 표시됩니다. 이 자습서에서 최상위 수준 풀 및 리전 풀을 만들었으므로 두 풀이 모두 표시됩니다.

6단계: 리전 풀에 CIDR 프로비저닝

리전 풀에 CIDR 블록을 프로비저닝합니다. 최상위 풀 내의 풀에 CIDR을 프로비저닝하는 경우 프로비저닝할 수 있는 최소 IPv4 CIDR은 /24이며, 더 구체적인 CIDR(예: /25)은 허용되지 않습니다. 첫 번째 지역 풀을 만든 후 지역 풀 내에 더 작은 풀(예: /25)을 만들 수 있습니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

AWS CLI를 사용하여 리전 풀에 CIDR 블록 할당

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

```
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
```

출력에 프로비저닝이 보류 중인 CIDR이 표시됩니다.

```

{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "pending-provision"
  }
}

```

```
    }
  }
}
```

- 출력에 `provisioned`의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

다음 예 출력에서는 현재 상태를 보여줍니다.

```
{
  "IpamPoolCidrs": [
    {
      "Cidr": "130.137.245.0/24",
      "State": "provisioned"
    }
  ]
}
```

7단계. 리전 풀 공유

이 섹션의 단계에 따라 AWS Resource Access Manager(RAM)를 사용하여 IPAM 풀을 공유합니다.

AWS RAM에서 리소스 공유 활성화

IPAM을 생성한 후에는 리전 풀을 조직의 다른 계정과 공유할 수 있습니다. IPAM 풀을 공유하기 전에 이 단원의 단계를 완료하여 AWS RAM과 리소스 공유를 활성화합니다. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile management-account` 옵션을 사용합니다.

리소스 공유 활성화

- AWS Organizations 관리 계정을 사용하여 <https://console.aws.amazon.com/ram/>에서 AWS RAM 콘솔을 엽니다.
- 왼쪽 탐색 창에서 설정을 선택하고 공유 활성화 범위 - AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

이제 IPAM 풀을 조직의 다른 멤버와 공유할 수 있습니다.

AWS RAM을 사용하여 IPAM 풀 공유

이 섹션에서는 리전 풀을 다른 AWS Organizations 멤버 계정과 공유합니다. 필수 IAM 권한에 대한 정보를 포함하여 IPAM 풀 공유에 대한 전체 지침은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile ipam-account` 옵션을 사용합니다.

AWS RAM을 사용하여 IPAM 풀 공유

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택하고, IPAM 풀을 선택하고, 작업 > 세부 정보 보기를 선택합니다.
4. 리소스 공유(Resource sharing)에서 리소스 공유 생성(Create resource share)을 선택합니다. AWS RAM 콘솔이 열립니다. AWS RAM을 사용하여 풀을 공유합니다.
5. 리소스 공유 생성(Create a resource share)을 선택합니다.
6. AWS RAM 콘솔에서 리소스 공유 생성을 다시 선택합니다.
7. 공유 풀에 대한 이름을 추가합니다.
8. 리소스 유형 선택에서 IPAM 풀을 선택한 다음에 공유하려는 풀의 ARN을 선택합니다.
9. Next(다음)를 선택합니다.
10. AWSRAMPermissionIpamPoolByoipCidrImport 권한을 선택합니다. 권한 옵션에 대한 세부 정보는 이 자습서의 범위를 벗어나지만 [AWS RAM을 사용하여 IPAM 풀 공유](#)에서 이러한 옵션에 대해 자세히 알아볼 수 있습니다.
11. Next(다음)를 선택합니다.
12. 보안 주체 > 보안 주체 유형 선택에서 AWS 계정을 선택하고 IP 주소 범위를 IPAM으로 가져올 계정의 계정 ID를 입력한 다음 추가를 선택합니다.
13. Next(다음)를 선택합니다.
14. 리소스 공유 옵션 및 공유할 보안 주체를 검토하고 생성을 선택합니다.
15. **member-account** 계정이 IPAM 풀에서 IP 주소 CIDRS를 할당할 수 있도록 하려면 `AWSRAMDefaultPermissionsIpamPool`으로 두 번째 리소스 공유를 생성하고 두 번째 리소스 공유를 생성합니다. `--resource-arns`의 값은 이전 섹션에서 생성한 IPAM 풀의 ARN입니다. `--principals` 값은 **member-account**의 계정 ID입니다. `--permission-arns`의 값은 `AWSRAMDefaultPermissionsIpamPool` 권한의 ARN입니다.

8단계: 퍼블릭 IPv4 풀 생성

퍼블릭 IPv4 풀 생성은 퍼블릭 IPv4 주소를 AWS로 가져와 IPAM을 사용하여 관리하는 필수 단계입니다. 이 단계는 일반적으로 탄력적 IP 주소를 프로비저닝하려는 다른 AWS 계정으로 수행합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

Important

퍼블릭 IPv4 풀 및 IPAM 풀은 AWS의 고유한 리소스에 의해 관리됩니다. 퍼블릭 IPv4 풀은 공개 소유의 CIDR을 탄력적 IP 주소로 변환할 수 있는 단일 계정 리소스입니다. IPAM 풀을 사용하여 퍼블릭 공간을 퍼블릭 IPv4 풀에 할당할 수 있습니다.

AWS CLI를 사용하여 퍼블릭 IPv4 풀 생성

- 다음 명령을 실행하여 CIDR을 프로비저닝합니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

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

출력에 퍼블릭 IPv4 풀 ID가 표시됩니다. 다음 단계에서 이 ID를 사용합니다.

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

9단계: 퍼블릭 IPv4 CIDR을 퍼블릭 IPv4 풀에 프로비저닝

퍼블릭 IPv4 CIDR을 퍼블릭 IPv4 풀에 프로비저닝합니다. `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 입력한 `--locale` 값과 일치해야 합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

AWS CLI를 사용하여 퍼블릭 IPv4 풀 생성

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

```
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
```

출력에 프로비저닝된 CIDR이 표시됩니다.

```
{
  "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
  "PoolAddressRange": {
    "FirstAddress": "130.137.245.0",
    "LastAddress": "130.137.245.255",
    "AddressCount": 256,
    "AvailableAddressCount": 256
  }
}
```

2. 다음 명령을 실행하여 퍼블릭 IPv4 풀에 프로비저닝된 CIDR을 확인합니다.

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-account
```

출력에 프로비저닝된 CIDR이 표시됩니다. 기본적으로 CIDR은 알리지 않으므로 인터넷을 통해 공개적으로 액세스할 수 없습니다. 이 자습서의 마지막 단계에서 이 CIDR을 알리도록 설정할 수 있습니다.

```
{
  "ByoipCidrs": [
    {
      "Cidr": "130.137.245.0/24",
      "StatusMessage": "Cidr successfully provisioned",
      "State": "provisioned"
    }
  ]
}
```

10단계: 퍼블릭 IPv4 풀에서 탄력적 IP 주소 생성

퍼블릭 IPv4 풀에서 탄력적 IP 주소를 생성합니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

AWS CLI를 사용하여 퍼블릭 IPv4 풀에서 EIP를 생성하려면

1. 다음 명령을 실행하여 EIP를 생성합니다.

```
aws ec2 allocate-address --region us-west-2 --public-ipv4-pool ipv4pool-ec2-0019eed22a684e0b2 --profile member-account
```

출력에 할당이 표시됩니다.

```
{
  "PublicIp": "130.137.245.100",
  "AllocationId": "eipalloc-0db3405026756dbf6",
  "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
  "NetworkBorderGroup": "us-east-1",
  "Domain": "vpc"
}
```

2. 다음 명령을 실행하여 IPAM에서 관리되는 EIP 할당을 확인할 수 있습니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

출력에 IPAM의 할당이 표시됩니다.

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "130.137.245.0/24",
      "IpamPoolAllocationId": "ipam-pool-alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
      "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
      "ResourceType": "ec2-public-ipv4-pool",
      "ResourceOwner": "123456789012"
    }
  ]
}
```

11단계: CIDR 알리기

이 섹션의 단계는 IPAM 계정에서 수행해야 합니다. 인스턴스 또는 Elastic Load Balancer와 탄력적 IP 주소(EIP)를 연결하면 `--aws-service ec2` 정의한 풀에 있는 AWS로 가져온 CIDR 알리를 시작할 수 있습니다. 이 자습서에서는 리전 풀이 해당됩니다. 기본적으로 CIDR은 알리지 않으므로 인터넷을 통해 공개적으로 액세스할 수 없습니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

AWS CLI를 사용하여 CIDR 알림 시작

- 다음 명령을 실행하여 CIDR을 알립니다.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
profile ipam-account
```

출력에 CIDR을 알리는 것이 표시됩니다.

```
{
  "ByoipCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "advertised"
  }
}
```

12단계: 정리

이번 섹션의 단계를 따르면 이 자습서에서 프로비저닝하고 생성한 리소스를 정리할 수 있습니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

AWS CLI를 사용하여 정리

1. IPAM에서 관리되는 EIP 할당을 봅니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

출력에 IPAM의 할당이 표시됩니다.

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "130.137.245.0/24",
      "IpamPoolAllocationId": "ipam-pool-alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
      "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
      "ResourceType": "ec2-public-ipv4-pool",
      "ResourceOwner": "123456789012"
    }
  ]
}
```

2. IPv4 CIDR 알림을 중지합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --profile ipam-account
```

출력에 CIDR 상태가 알림에서 프로비저닝으로 변경되었다고 표시됩니다.

```
{
  "ByoipCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "provisioned"
  }
}
```

3. 탄력적 IP 주소를 해제합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

```
aws ec2 release-address --region us-west-2 --allocation-id eipalloc-0db3405026756dbf6 --profile member-account
```

이 명령을 실행하면 어떤 출력도 표시되지 않습니다.

4. BYOIP CIDR을 확인합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

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

출력에 BYOIP CIDR의 IP 주소가 표시됩니다.

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

- 퍼블릭 IPv4 풀에서 CIDR의 마지막 IP 주소를 해제합니다. 넷마스크가 /32인 IP 주소를 입력합니다. CIDR 범위의 각 IP 주소에 대해 이 명령을 다시 실행해야 합니다. CIDR이 /24인 경우 이 명령을 실행하여 /24 CIDR의 256개 IP 주소 각각을 프로비저닝 해제해야 합니다. 이 섹션의 명령을 실행하는 경우 --region의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.255/32 --profile member-account
```

출력에 프로비저닝 해제된 CIDR이 표시됩니다.

```
{
```

```

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

    "DeprovisionedAddresses": [

        "130.137.245.255"

    ]

}

```

6. BYOIP CIDR을 다시 확인하고 프로비저닝된 주소가 더 이상 없는지 확인합니다. 이 섹션의 명령을 실행하는 경우 `--region`의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
```

출력에 퍼블릭 IPv4 풀의 IP 주소 수가 표시됩니다.

```

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

```

7. IPAM에서 더 이상 관리되지 않는 EIP 할당을 확인합니다. IPAM이 탄력적 IP 주소가 제거되었음을 확인하는 데 약간의 시간이 걸릴 수 있습니다. IPAM에서 할당이 제거됐는지 확인할 때까지 IPAM 풀 CIDR을 정리하고 프로비저닝 해제할 수 없습니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

출력에 IPAM의 할당이 표시됩니다.

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

- 리전 풀 CIDR을 프로비저닝 해제합니다. 이 단계의 명령을 실행하는 경우 `--region`의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
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
```

출력에 프로비저닝 해제가 보류 중인 CIDR이 표시됩니다.

```
{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "pending-deprovision"
  }
}
```

프로비저닝 해제를 완료하려면 시간이 걸립니다. 프로비저닝 해제 상태를 확인합니다.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account
```

프로비저닝 해제가 표시될 때까지 기다렸다가 다음 단계를 계속 진행합니다.

```
{
```

```

    "IpamPoolCidr": {
        "Cidr": "130.137.245.0/24",
        "State": "deprovisioned"
    }
}

```

9. RAM 공유를 삭제하고 AWS Organizations와의 RAM 통합을 사용 중지합니다. AWS RAM 사용 설명서의 [AWS RAM의 리소스 공유 삭제](#) 및 [AWS Organizations와의 리소스 공유 비활성화](#)의 단계를 순서대로 완료하여 RAM 공유를 삭제하고 AWS Organizations와의 RAM 통합을 사용 중지합니다.

이 단계는 각각 IPAM 계정과 관리 계정으로 수행해야 합니다. AWS CLI를 사용하여 RAM 공유를 삭제하고 RAM 통합을 사용 중지하는 경우 `--profile ipam-account` 및 `--profile management-account` 옵션을 사용합니다.

10. 리전 풀을 삭제합니다. 이 단계의 명령을 실행하는 경우 `--region`의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```

aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-pool-0d8f3646b61ca5987 --profile ipam-account

```

출력에서 삭제 상태를 확인할 수 있습니다.

```

{
  "IpamPool": {
    "OwnerId": "123456789012",
    "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
    "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
    "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-pool-0d8f3646b61ca5987",
    "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-scope-0087d83896280b594",
    "IpamScopeType": "public",
    "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
    "Locale": "us-east-1",
    "PoolDepth": 2,
  }
}

```

```

    "State": "delete-in-progress",
    "Description": "reg-ipv4-pool",
    "AutoImport": false,
    "Advertisable": true,
    "AddressFamily": "ipv4"
  }
}

```

11. 최상위 풀 CIDR을 프로비저닝 해제합니다. 이 단계의 명령을 실행하는 경우 `--region`의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```

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

```

출력에 프로비저닝 해제가 보류 중인 CIDR이 표시됩니다.

```

{
  "IpamPoolCidr": {
    "Cidr": "130.137.245.0/24",
    "State": "pending-deprovision"
  }
}

```

프로비저닝 해제를 완료하려면 시간이 걸립니다. 다음 명령을 실행하여 프로비저닝 해제 상태를 확인합니다.

```

aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --profile ipam-account

```

프로비저닝 해제가 표시될 때까지 기다렸다가 다음 단계를 계속 진행합니다.

```

{
  "IpamPoolCidr": {

```

```

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}

```

12. 최상위 풀을 삭제합니다. 이 단계의 명령을 실행하는 경우 `--region`의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```

aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --profile ipam-account

```

출력에서 삭제 상태를 확인할 수 있습니다.

```

{
  "IpamPool": {
    "OwnerId": "123456789012",
    "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
    "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-pool-0a03d430ca3f5c035",
    "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-scope-0087d83896280b594",
    "IpamScopeType": "public",
    "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
    "Locale": "us-east-1",
    "PoolDepth": 2,
    "State": "delete-in-progress",
    "Description": "top-level-pool",
    "AutoImport": false,
    "Advertisable": true,
    "AddressFamily": "ipv4"
  }
}

```

13. IPAM을 삭제합니다. 이 단계의 명령을 실행하는 경우 `--region`의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

출력에 IPAM 응답이 표시됩니다. 즉, IPAM이 삭제되었습니다.

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

AWS CLI만 사용하여 IPAM으로 고유 IPv6 CIDR 가져오기

다음 단계에 따라 IPv6 CIDR을 IPAM으로 가져오고 AWS CLI만 사용하여 VPC를 할당하세요.

Important

- 지금은 Local Zones에서 BYOIP 주소 범위를 프로비저닝하거나 홍보할 수 없습니다.
- 이 자습서에서는 다음 섹션의 단계를 이미 수행한 것으로 가정합니다.

- [AWS Organization에서 계정과 IPAM 통합](#).
- [IPAM 생성](#).
- 이 자습서의 각 단계는 다음 3개의 AWS Organizations 계정 중 하나로 수행해야 합니다.
 - 관리 계정.
 - [AWS Organization에서 계정과 IPAM 통합](#)에서 IPAM 관리자로 구성된 멤버 계정. 이 자습서에서는 이 계정을 IPAM 계정이라고 합니다.
 - IPAM 풀에서 CIDR을 할당할 조직의 멤버 계정입니다. 이 자습서에서는 이 계정을 멤버 계정이라고 합니다.

내용

- [1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성](#)
- [2단계: IPAM 생성](#)
- [3단계: IPAM 풀 생성](#)
- [4단계: 최상위 풀에 CIDR 프로비저닝](#)
- [5단계: 최상위 풀 내에 리전 풀 생성](#)
- [6단계: 리전 풀에 CIDR 프로비저닝](#)
- [7단계. 리전 풀 공유](#)
- [8단계: IPv6 CIDR을 사용하여 VPC 생성](#)
- [9단계: CIDR 알리기](#)
- [10단계: 정리](#)

1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성

단일 AWS 사용자로 이 자습서를 완료하려면 AWS CLI 명령 프로파일을 사용하여 IAM 역할 간에 전환할 수 있습니다. [명명 프로파일](#)은 AWS CLI와(과) 함께 `--profile` 옵션을 사용할 때 참조하는 설정 및 보안 인증 정보의 모음입니다. AWS 계정에 대한 IAM 역할 및 명명 프로파일 생성 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [AWS CLI에서 IAM 역할 사용](#)을 참조하세요.

이 자습서에서 사용할 세 AWS 계정 각각에 대해 역할 하나와 명명 프로필 하나를 만듭니다:

- AWS Organizations 관리 계정에 대한 `management-account`라는 프로파일

- IPAM 관리자로 구성된 AWS Organizations 멤버 계정의 ipam-account라는 프로파일
- IPAM 풀에서 CIDR을 할당할 조직의 AWS Organizations 멤버 계정에 대한 member-account라는 프로파일

IAM 역할 및 명명 프로파일을 생성한 후 이 페이지로 돌아와서 다음 단계로 이동합니다. 이 자습서의 나머지 부분에서 샘플 AWS CLI CLI 명령이 명명된 프로파일 중 하나와 함께 `--profile` 옵션을 사용하여 명령을 실행해야 하는 계정을 나타냅니다.

2단계: IPAM 생성

이 단계는 선택 사항입니다. us-east-1과 us-west-2의 운영 리전에서 생성된 IPAM이 이미 있는 경우 이 단계를 건너뛸 수 있습니다. IPAM을 생성하고 us-east-1과 us-west-2의 운영 리전을 지정합니다. IPAM 풀을 생성하는 경우 로컬 옵션을 사용할 수 있도록 운영 리전을 선택해야 합니다. BYOIP와 IPAM을 통합하려면 BYOIP CIDR에 사용할 모든 풀에 로컬이 설정되어야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

다음 명령을 실행합니다:

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

출력에 생성한 IPAM이 표시됩니다. PublicDefaultScopeId의 값을 기록해 둡니다. 다음 단계에서 퍼블릭 범위 ID가 필요합니다.

```
{
  "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": []
  }
}

```

3단계: IPAM 풀 생성

최상위 IPAM 풀 내의 리전 풀을 통해 최상위 IPAM 풀을 생성하고 리전 풀의 리소스(VPC)에 공간을 할당하기 때문에 최상위 풀이 아닌 리전 풀에 로컬을 설정합니다. 이후 단계에서 리전 풀을 생성하는 경우 리전 풀에 로컬을 추가합니다. BYOIP와 IPAM을 통합하려면 BYOIP CIDR에 사용할 모든 풀에 로컬이 설정되어야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

이 IPAM 풀 CIDR을 퍼블릭 인터넷을 통해 AWS에서 알릴 수 있도록 하려면 `--publicly-advertisable` 또는 `--no-publicly-advertisable`을 선택합니다.

Note

범위 ID는 퍼블릭 범위의 ID여야 하고 주소 패밀리는 `ipv6`여야 합니다.

AWS CLI를 사용하여 모든 AWS 리소스에 대해 IPv6 주소 풀을 생성하려면

1. 다음 명령을 실행하여 IPAM 풀을 생성합니다. 이전 단계에서 생성한 IPAM의 퍼블릭 범위 ID를 사용합니다.

```

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

```

출력에 풀 생성이 진행 중임을 나타내는 `create-in-progress`가 표시됩니다.

```

{
  "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": []

  }
}

```

- 출력에 create-complete의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

다음 예 출력에서는 풀의 상태를 보여줍니다.

```

{
  "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": []

  }
}

```

4단계: 최상위 풀에 CIDR 프로비저닝

최상위 풀에 CIDR을 프로비저닝합니다. 최상위 풀 내의 풀에 IPv6 CIDR를 프로비저닝할 때 가져올 수 있는 가장 구체적인 IPv6 주소 범위는 공개적으로 알려진 CIDR의 경우 /48이고 공개적으로 알려지지 않은 CIDR의 경우 /60입니다. CIDR, BYOIP 메시지 및 인증서 서명을 요청에 포함해야 사용자가 퍼블릭 공간을 소유하고 있는지 확인할 수 있습니다. 이 BYOIP 메시지 및 인증서 서명을 가져오는 방법을 포함한 BYOIP 사전 조건 목록은 [AWS CLI만 사용하여 IPAM으로 고유 퍼블릭 IPv4 CIDR 가져오기](#) 섹션을 참조하세요.

BYOIP CIDR을 최상위 풀에 프로비저닝하는 경우 `--cidr-authorization-context`를 추가하기만 하면 됩니다. 최상위 풀 내에 있는 지역 풀의 경우 `--cidr-authorization-context` 옵션을 생략할 수 있습니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

AWS CLI를 사용하여 CIDR 블록을 풀에 프로비저닝하기

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --cidr-authorization-
context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|
SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9R1pBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxFnp7RAJDvF1mBwxmSgH~C
Vp6LON3y00Xmp4JENB9uM7sMlu6oeoutGyyhXFeYPz1GSRdcdfKNKaimvPCqVsxGN5AwSi1KQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

출력에 프로비저닝이 보류 중인 CIDR이 표시됩니다.

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "pending-provision"
  }
}
```

- 계속하기 전에 이 CIDR이 프로비저닝되었는지 확인합니다.

Important

대부분의 프로비저닝은 2시간 내에 완료되지만 공개적으로 알려진 범위에 대한 프로비저닝 프로세스를 완료하려면 최대 1주가 걸릴 수 있습니다.

출력에 provisioned의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

다음 예 출력에서는 상태를 보여줍니다.

```
{
  "IpamPoolCidrs": [
    {
      "Cidr": "2605:9cc0:409::/48",
```

```

        "State": "provisioned"
      }
    ]
  }

```

5단계: 최상위 풀 내에 리전 풀 생성

최상위 풀 내에 리전 풀을 생성합니다. `--locale`은 풀에 필요하며 IPAM을 생성할 때 구성된 운영 리전 중 하나여야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

Important

풀을 생성하는 경우 `--aws-service ec2`을(를) 포함해야 합니다. 선택한 서비스에 따라 CIDR이 알릴 AWS 서비스가 결정됩니다. 현재, 유일한 옵션은 `ec2`입니다. 즉, 이 풀에서 할당된 CIDR은 Amazon EC2 서비스 및 Amazon VPC 서비스(VPC에 연결된 CIDR용)에 대해 알릴 수 있음을 의미합니다.

AWS CLI를 사용하여 리전 풀을 생성하려면

1. 다음 명령을 실행하여 풀을 생성합니다.

```

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

```

출력에 풀을 생성하는 IPAM이 표시됩니다.

```

{
  "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. 출력에 `create-complete`의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

출력에는 IPAM에 있는 풀이 표시됩니다. 이 자습서에서 최상위 수준 풀 및 리전 풀을 만들었으므로 두 풀이 모두 표시됩니다.

6단계: 리전 풀에 CIDR 프로비저닝

리전 풀에 CIDR 블록을 프로비저닝합니다. 최상위 풀 내의 풀에 CIDR를 프로비저닝할 때 가져올 수 있는 가장 구체적인 IPv6 주소 범위는 공개적으로 알려진 CIDR의 경우 /48이고 공개적으로 알려지지 않은 CIDR의 경우 /60입니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

AWS CLI를 사용하여 리전 풀에 CIDR 블록 할당

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

출력에 프로비저닝이 보류 중인 CIDR이 표시됩니다.

```

{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",

```

```

    "State": "pending-provision"
  }
}

```

- 출력에 `provisioned`의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

다음 예 출력에서는 현재 상태를 보여줍니다.

```

{
  "IpamPoolCidrs": [
    {
      "Cidr": "2605:9cc0:409::/48",
      "State": "provisioned"
    }
  ]
}

```

7단계. 리전 풀 공유

이 섹션의 단계에 따라 AWS Resource Access Manager(RAM)를 사용하여 IPAM 풀을 공유합니다.

AWS RAM에서 리소스 공유 활성화

IPAM을 생성한 후에는 리전 풀을 조직의 다른 계정과 공유할 수 있습니다. IPAM 풀을 공유하기 전에 이 단원의 단계를 완료하여 AWS RAM과 리소스 공유를 활성화합니다. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile management-account` 옵션을 사용합니다.

리소스 공유 활성화

- AWS Organizations 관리 계정을 사용하여 <https://console.aws.amazon.com/ram/>에서 AWS RAM 콘솔을 엽니다.
- 왼쪽 탐색 창에서 설정을 선택하고 공유 활성화 범위 - AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

이제 IPAM 풀을 조직의 다른 멤버와 공유할 수 있습니다.

AWS RAM을 사용하여 IPAM 풀 공유

이 섹션에서는 리전 풀을 다른 AWS Organizations 멤버 계정과 공유합니다. 필수 IAM 권한에 대한 정보를 포함하여 IPAM 풀 공유에 대한 전체 지침은 [AWS RAM을 사용하여 IPAM 풀 공유](#) 섹션을 참조하세요. AWS CLI를 사용하여 리소스 공유를 사용 설정하는 경우 `--profile ipam-account` 옵션을 사용합니다.

AWS RAM을 사용하여 IPAM 풀 공유

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택하고, IPAM 풀을 선택하고, 작업 > 세부 정보 보기를 선택합니다.
4. 리소스 공유(Resource sharing)에서 리소스 공유 생성(Create resource share)을 선택합니다. AWS RAM 콘솔이 열립니다. AWS RAM을 사용하여 풀을 공유합니다.
5. 리소스 공유 생성(Create a resource share)을 선택합니다.
6. AWS RAM 콘솔에서 리소스 공유 생성을 다시 선택합니다.
7. 공유 풀에 대한 이름을 추가합니다.
8. 리소스 유형 선택에서 IPAM 풀을 선택한 다음에 공유하려는 풀의 ARN을 선택합니다.
9. Next(다음)를 선택합니다.
10. AWSRAMPermissionIpamPoolByoipCidrImport 권한을 선택합니다. 권한 옵션에 대한 세부 정보는 이 자습서의 범위를 벗어나지만 [AWS RAM을 사용하여 IPAM 풀 공유](#)에서 이러한 옵션에 대해 자세히 알아볼 수 있습니다.
11. Next(다음)를 선택합니다.
12. 보안 주체 > 보안 주체 유형 선택에서 AWS 계정을 선택하고 IP 주소 범위를 IPAM으로 가져올 계정의 계정 ID를 입력한 다음 추가를 선택합니다.
13. Next(다음)를 선택합니다.
14. 리소스 공유 옵션 및 공유할 보안 주체를 검토하고 생성을 선택합니다.
15. **member-account** 계정이 IPAM 풀에서 IP 주소 CIDRS를 할당할 수 있도록 하려면 `AWSRAMDefaultPermissionsIpamPool`으로 두 번째 리소스 공유를 생성하고 두 번째 리소스 공유를 생성합니다. `--resource-arns`의 값은 이전 섹션에서 생성한 IPAM 풀의 ARN입니다. `--principals` 값은 **member-account**의 계정 ID입니다. `--permission-arns`의 값은 `AWSRAMDefaultPermissionsIpamPool` 권한의 ARN입니다.

8단계: IPv6 CIDR을 사용하여 VPC 생성

IPAM 풀 ID를 사용하여 VPC 생성합니다. `--cidr-block` 옵션을 사용하여 VPC에 IPv4 CIDR 블록을 연결해야 합니다. 그렇지 않으면 요청이 실패합니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

AWS CLI를 사용하여 IPv6 CIDR로 VPC를 생성하려면

1. 다음 명령을 실행하여 CIDR을 프로비저닝합니다.

```
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
```

출력에 VPC가 생성되는 것이 표시됩니다.

```
{
  "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. IPAM에서 VPC 할당을 확인합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

출력에 IPAM의 할당이 표시됩니다.

```

{
  "IpamPoolAllocations": [
    {
      "Cidr": "2605:9cc0:409::/56",
      "IpamPoolAllocationId": "ipam-pool-alloc-5f8db726fb9e4ff0a33836e649283a52",
      "ResourceId": "vpc-00b5573ffc3b31a29",
      "ResourceType": "vpc",
      "ResourceOwner": "123456789012"
    }
  ]
}

```

9단계: CIDR 알리기

IPAM에 할당된 CIDR을 사용하여 VPC를 생성하면 --aws-service ec2 정의된 풀에 있는 AWS로 가져온 CIDR 알림을 시작할 수 있습니다. 이 자습서에서는 리전 풀이 해당됩니다. 기본적으로 CIDR은 알리지 않으므로 인터넷을 통해 공개적으로 액세스할 수 없습니다. 이 섹션에서 명령을 실행하는 경우 --region의 값은 BYOIP CIDR에 사용할 리전 풀을 생성할 때 입력한 --locale 옵션과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

AWS CLI를 사용하여 CIDR 알림 시작

- 다음 명령을 실행하여 CIDR을 알립니다.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

출력에 CIDR을 알리는 것이 표시됩니다.

```
{
  "ByoipCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "advertised"
  }
}
```

10단계: 정리

이번 섹션의 단계를 따르면 이 자습서에서 프로비저닝하고 생성한 리소스를 정리할 수 있습니다. 이 섹션에서 명령을 실행하는 경우 --region의 값은 BYOIP CIDR에 사용할 리전 풀을 생성할 때 입력한 --locale 옵션과 일치해야 합니다.

AWS CLI를 사용하여 정리

1. 다음 명령을 실행하여 IPAM에서 관리되는 VPC 할당을 봅니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

출력에 IPAM의 할당이 표시됩니다.

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "2605:9cc0:409::/56",
      "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
      "ResourceId": "vpc-00b5573ffc3b31a29",
      "ResourceType": "vpc",
      "ResourceOwner": "123456789012"
    }
  ]
}
```

```
]
}
```

2. 다음 명령을 실행하여 CIDR 알림을 중단합니다. 이 단계에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 리전 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

출력에 CIDR 상태가 알림에서 프로비저닝으로 변경되었다고 표시됩니다.

```
{
  "ByoipCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "provisioned"
  }
}
```

3. 다음 명령을 실행하여 VPC를 삭제합니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 리전 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

이 단계는 멤버 계정으로 수행해야 합니다.

```
aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
profile member-account
```

이 명령을 실행하면 어떤 출력도 표시되지 않습니다.

4. 다음 명령을 실행하여 IPAM에서 VPC 할당을 봅니다. IPAM이 VPC가 삭제되었는지 발견하고 이 할당을 제거하는 데 약간의 시간이 걸릴 수 있습니다. 이 섹션에서 명령을 실행하는 경우 `--region`의 값은 BYOIP CIDR에 사용할 리전 풀을 생성할 때 입력한 `--locale` 옵션과 일치해야 합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

출력에 IPAM의 할당이 표시됩니다.

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "2605:9cc0:409::/56",
      "IpamPoolAllocationId": "ipam-pool-alloc-5f8db726fb9e4ff0a33836e649283a52",
      "ResourceId": "vpc-00b5573ffc3b31a29",
      "ResourceType": "vpc",
      "ResourceOwner": "123456789012"
    }
  ]
}
```

명령을 다시 실행하고 제거할 할당을 찾습니다. IPAM에서 할당이 제거됐는지 확인할 때까지 IPAM 풀 CIDR을 정리하고 프로비저닝 해제할 수 없습니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

출력에 IPAM에서 제거된 할당이 표시됩니다.

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

5. RAM 공유를 삭제하고 AWS Organizations와의 RAM 통합을 사용 중지합니다. AWS RAM 사용 설명서의 [AWS RAM의 리소스 공유 삭제](#) 및 [AWS Organizations와의 리소스 공유 비활성화](#)의 단계를 순서대로 완료하여 RAM 공유를 삭제하고 AWS Organizations와의 RAM 통합을 사용 중지합니다.

이 단계는 각각 IPAM 계정과 관리 계정으로 수행해야 합니다. AWS CLI를 사용하여 RAM 공유를 삭제하고 RAM 통합을 사용 중지하는 경우 `--profile ipam-account` 및 `--profile management-account` 옵션을 사용합니다.

6. 다음 명령을 실행하여 리전 풀 CIDR을 프로비저닝 해제합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

출력에 프로비저닝 해제가 보류 중인 CIDR이 표시됩니다.

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "pending-deprovision"
  }
}
```

프로비저닝 해제를 완료하려면 시간이 걸립니다. CIDR 상태가 프로비저닝 해제로 표시될 때까지 명령을 계속 실행합니다.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

출력에 프로비저닝 해제가 보류 중인 CIDR이 표시됩니다.

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "deprovisioned"
  }
}
```

7. 다음 명령을 실행하여 리전 풀을 삭제합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-pool-0053b7d2b4fc3f730 --profile ipam-account
```

출력에서 삭제 상태를 확인할 수 있습니다.

```
{
  "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. 다음 명령을 실행하여 최상위 풀 CIDR을 프로비저닝 해제합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

출력에 프로비저닝 해제가 보류 중인 CIDR이 표시됩니다.

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "pending-deprovision"
  }
}
```

```
}

```

프로비저닝 해제를 완료하려면 시간이 걸립니다. 다음 명령을 실행하여 프로비저닝 해제 상태를 확인합니다.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --profile ipam-account
```

프로비저닝 해제가 표시될 때까지 기다렸다가 다음 단계를 계속 진행합니다.

```
{
  "IpamPoolCidr": {
    "Cidr": "2605:9cc0:409::/48",
    "State": "deprovisioned"
  }
}
```

9. 다음 명령을 실행하여 최상위 풀을 삭제합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-pool-07f2466c7158b50c4 --profile ipam-account
```

출력에서 삭제 상태를 확인할 수 있습니다.

```
{
  "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. 다음 명령을 실행하여 IPAM을 삭제합니다.

이 단계는 IPAM 계정으로 수행해야 합니다.

```

aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account

```

출력에 IPAM 응답이 표시됩니다. 즉, IPAM이 삭제되었습니다.

```

{
  "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"
      }
    ]
  }
}

```

자습서: IPAM으로 BYOIP IPv4 CIDR 전송

다음 단계에 따라 기존 IPv4 CIDR을 IPAM으로 전송합니다. AWS가 포함된 IPv4 BYOIP CIDR이 이미 있는 경우 CIDR을 퍼블릭 IPv4 풀에서 IPAM으로 이동할 수 있습니다. IPv6 CIDR을 IPAM으로 이동할 수 없습니다.

이 자습서에서는 [Bring your own IP addresses \(BYOIP\) in Amazon EC2](#)에 설명된 프로세스를 사용하여 IP 주소 범위를 AWS로 이미 성공적으로 가져왔고 이제 해당 IP 주소 범위를 IPAM으로 전송하려고 한다고 가정합니다. 새 IP 주소를 처음으로 AWS로 가져오고 있는 중인 경우 [자습서: IPAM으로 IP 주소 가져오기](#)의 단계를 완료하세요.

퍼블릭 IPv4 풀을 IPAM으로 전송하는 경우 기존 할당에는 영향을 미치지 않습니다. 퍼블릭 IPv4 풀을 IPAM으로 전송한 후에는 리소스 유형에 따라 기존 할당을 모니터링할 수 있습니다. 자세한 내용은 [리소스별 CIDR 사용량 모니터링](#) 단원을 참조하십시오.

Important

- 이 자습서에서는 [IPAM 생성](#)의 단계를 이미 수행한 것으로 가정합니다.
- 이 자습서의 각 단계는 다음 2개의 AWS 계정 중 하나로 수행해야 합니다.
 - IPAM 관리자의 계정입니다. 이 자습서에서는 이 계정을 IPAM 계정이라고 합니다.
 - BYOIP CIDR을 소유한 조직의 계정입니다. 이 자습서에서는 이 계정을 BYOIP CIDR 소유자 계정이라고 합니다.

내용

- [1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성](#)
- [2단계: IPAM의 퍼블릭 범위 ID 가져오기](#)
- [3단계: IPAM 풀 생성](#)
- [4단계: AWS RAM을 사용하여 IPAM 풀 공유](#)
- [5단계: IPAM으로 기존 BYOIP IPv4 CIDR 전송](#)
- [6단계: IPAM에서 CIDR 보기](#)
- [7단계: 정리](#)

1단계: AWS CLI 명령 프로파일 및 IAM 역할 생성

단일 AWS 사용자로 이 자습서를 완료하려면 AWS CLI 명령 프로파일을 사용하여 IAM 역할 간에 전환할 수 있습니다. [명명 프로파일](#)은 AWS CLI와(과) 함께 `--profile` 옵션을 사용할 때 참조하는 설정 및 보안 인증 정보의 모음입니다. AWS 계정에 대한 IAM 역할 및 명명 프로파일 생성 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [AWS CLI에서 IAM 역할 사용](#)을 참조하세요.

이 자습서에서 사용할 세 AWS 계정 각각에 대해 역할 하나와 명명 프로파일 하나를 만듭니다:

- IPAM 관리자인 AWS 계정에 대한 `ipam-account`라는 프로파일
- BYOIP CIDR을 소유하는 조직의 AWS 계정에 대한 `byoip-owner-account`라는 프로파일

IAM 역할 및 명명 프로파일을 생성한 후 이 페이지로 돌아와서 다음 단계로 이동합니다. 이 자습서의 나머지 부분에서 샘플 AWS CLI 명령이 명명된 프로파일 중 하나와 함께 `--profile` 옵션을 사용하여 명령을 실행해야 하는 계정을 나타냅니다.

2단계: IPAM의 퍼블릭 범위 ID 가져오기

이 섹션의 단계를 따르면 IPAM의 퍼블릭 범위 ID를 가져올 수 있습니다. 이 단계는 `ipam-account` 계정에서 수행해야 합니다.

다음 명령을 실행하여 퍼블릭 범위 ID를 가져옵니다.

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

출력에 퍼블릭 범위 ID가 표시됩니다. `PublicDefaultScopeId`의 값을 기록해 둡니다. 다음 단계에서 이 값을 사용할 것입니다.

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

```

3단계: IPAM 풀 생성

이 섹션의 단계를 따르면 IPAM 풀을 생성할 수 있습니다. 이 단계는 **ipam-account** 계정에서 수행해야 합니다. 생성하는 IPAM 풀은 BYOIP CIDR AWS 리전과 일치하는 `--locale` 옵션이 포함된 최상위 풀이어야 합니다. BYOIP는 최상위 IPAM 풀로만 전송할 수 있습니다.

Important

풀을 생성하는 경우 `--aws-service ec2`(를) 포함해야 합니다. 선택한 서비스에 따라 CIDR이 알릴 AWS 서비스가 결정됩니다. 현재, 유일한 옵션은 `ec2`입니다. 즉, 이 풀에서 할당된 CIDR은 Amazon EC2 서비스(탄력적 IP 주소용) 및 Amazon VPC 서비스(VPC에 연결된 CIDR용)에 대해 알릴 수 있음을 의미합니다.

AWS CLI를 사용하여 전송된 BYOIP CIDR에 대한 IPv4 주소 풀을 생성하려면

1. 다음 명령을 실행하여 IPAM 풀을 생성합니다. 이전 단계에서 검색한 IPAM의 퍼블릭 범위 ID를 사용합니다.

```

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

```

출력에 풀 생성이 진행 중임을 나타내는 `create-in-progress`가 표시됩니다.

```

{
  "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. 출력에 `create-complete`의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

다음 예 출력에서는 풀의 상태를 보여줍니다. 다음 단계에서 `OwnerId`가 필요합니다.

```

{
  "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"
    }
  ]
}

```

```

    }
  ]
}

```

4단계: AWS RAM을 사용하여 IPAM 풀 공유

이 섹션의 단계에 따라 다른 AWS 계정이 기존 BYOIP IPv4 CIDR을 IPAM 풀로 전송하고 IPAM 풀을 사용할 수 있도록 AWS RAM을 사용하여 IPAM 풀을 공유합니다. 이 단계는 **ipam-account** 계정에서 수행해야 합니다.

AWS CLI를 사용하여 IPv4 주소 풀 공유

1. IPAM 풀에 사용할 수 있는 AWS RAM 권한을 봅니다. 이 섹션의 단계를 완료하려면 두 ARN이 모두 필요합니다.

```
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. **byoip-owner-account** 계정이 BYOIP CIDR을 IPAM으로 가져올 수 있도록 리소스 공유를 생성합니다. `--resource-arns`의 값은 이전 섹션에서 생성한 IPAM 풀의 ARN입니다. `--principals`의 값은 BYOIP CIDR 소유자 계정의 계정 ID입니다. `--permission-arns`의 값은 `AWSRAMPermissionIpamPoolByoipCidrImport` 권한의 ARN입니다.

```

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. (선택 사항) 전송이 완료된 후 **byoip-owner-account** 계정이 IPAM 풀에서 퍼블릭 IPv4 풀로 IP 주소 CIDRS를 할당하도록 허용하려면 `AWSRAMDefaultPermissionsIpamPool`에 대한 ARN을 복사하고 두 번째 리소스 공유를 생성합니다. `--resource-arns`의 값은 이전 섹션에서 생성

한 IPAM 풀의 ARN입니다. `--principals`의 값은 BYOIP CIDR 소유자 계정의 계정 ID입니다. `--permission-arns`의 값은 `AWSRAMDefaultPermissionsIpamPool` 권한의 ARN입니다.

```
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"
  }
}
```

RAM에서 리소스 공유를 생성한 결과로 이제 `byoip-owner-account` 계정이 CIDR을 IPAM으로 이동할 수 있습니다.

5단계: IPAM으로 기존 BYOIP IPv4 CIDR 전송

이 섹션의 단계를 따르면 기존 IPv4 CIDR을 IPAM으로 전송할 수 있습니다. 이 단계는 `byoip-owner-account` 계정에서 수행해야 합니다.

⚠ Important

사용하여 AWS로 IPv4 주소 범위를 가져오면 첫 번째 주소(네트워크 주소)와 마지막 주소(브로드캐스트 주소)를 포함하여 범위 내의 IP 주소를 모두 사용할 수 있습니다.

BYOIP CIDR을 IPAM으로 전송하려면 BYOIP CIDR 소유자가 IAM 정책에서 다음 권한을 보유해야 합니다.

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

ℹ Note

이 단계에서 AWS Management Console 또는 AWS CLI를 사용할 수 있습니다.

AWS Management Console

BYOIP CIDR을 IPAM 풀로 전송하는 방법:

1. <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 **byoip-owner-account** 계정으로 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 이 자습서에서 생성 및 공유한 최상위 풀을 선택합니다.
4. 작업 > BYOIP CIDR 전송을 선택합니다.
5. BYOIP CID 전송을 선택합니다.
6. BYOIP CIDR을 선택합니다.
7. 프로비저닝을 선택합니다.

Command line

다음의 AWS CLI 명령을 사용하여 BYOIP CIDR을 AWS CLI을 사용하는 IPAM 풀로 전송하는 방법:

1. 다음 명령을 실행하여 CIDR을 전송합니다. `--region` 값이 BYOIP CIDR의 AWS 리전인지 확인합니다.

```
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
```

출력에 프로비저닝이 보류 중인 CIDR이 표시됩니다.

```
{
  "ByoipCidr": {
    "Cidr": "130.137.249.0/24",
    "State": "pending-transfer"
  }
}
```

2. CIDR이 전송되었는지 확인합니다. 출력에 `complete-transfer`의 상태가 표시될 때까지 다음 명령을 실행합니다.

```
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
```

다음 예 출력에서는 상태를 보여줍니다.

```
{
  "ByoipCidr": {
    "Cidr": "130.137.249.0/24",
    "State": "complete-transfer"
  }
}
```

6단계: IPAM에서 CIDR 보기

이 섹션의 단계를 따르면 IPAM에서 CIDR을 볼 수 있습니다. 이 단계는 **ipam-account** 계정에서 수행해야 합니다.

AWS CLI를 사용하여 IPAM 풀에서 전송된 BYOIP CIDR을 보려면

- 다음 명령을 실행하여 IPAM에서 관리되는 할당을 봅니다. `--region` 값이 BYOIP CIDR의 AWS 리전인지 확인합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

출력에 IPAM의 할당이 표시됩니다.

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "130.137.249.0/24",
      "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
      "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
      "ResourceType": "ec2-public-ipv4-pool",
      "ResourceOwner": "111122223333"
    }
  ]
}
```

7단계: 정리

이번 섹션의 단계를 따르면 이 자습서에서 생성한 리소스를 제거할 수 있습니다. 이 단계는 **ipam-account** 계정에서 수행해야 합니다.

AWS CLI를 사용하여 이 자습서에서 생성한 리소스를 정리하려면

1. IPAM 풀 공유 리소스를 삭제하려면 다음 명령을 실행하여 첫 번째 리소스 공유 ARN을 가져옵니다.

```
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. 리소스 공유 ARN을 복사하고 이를 사용하여 IPAM 풀 리소스 공유를 삭제합니다.

```
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. [4단계: AWS RAM을 사용하여 IPAM 풀 공유](#)에서 추가 리소스 공유를 생성한 경우 이전 두 단계를 반복하여 PoolShare2에 대한 두 번째 리소스 공유 ARN을 가져오고 두 번째 리소스 공유를 삭제합니다.
4. 다음 명령을 실행하여 BYOIP CIDR의 할당 ID를 가져옵니다. --region 값이 BYOIP CIDR의 AWS 리전과 일치하는지 확인합니다.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

출력에 IPAM의 할당이 표시됩니다.

```
{
  "IpamPoolAllocations": [
    {
      "Cidr": "130.137.249.0/24",
      "IpamPoolAllocationId": "ipam-pool-alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
      "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
      "ResourceType": "ec2-public-ipv4-pool",
      "ResourceOwner": "111122223333"
    }
  ]
}
```

- 퍼블릭 IPv4 풀에서 CIDR의 마지막 IP 주소를 해제합니다. 넷마스크가 /32인 IP 주소를 입력합니다. CIDR 범위의 각 IP 주소에 대해 이 명령을 다시 실행해야 합니다. CIDR이 /24인 경우 이 명령을 실행하여 /24 CIDR의 256개 IP 주소 각각을 프로비저닝 해제해야 합니다. 이 섹션의 명령을 실행하는 경우 --region의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 **byoip-owner-account** 계정으로 수행해야 합니다.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --profile byoip-owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.255/32
```

출력에 프로비저닝 해제된 CIDR이 표시됩니다.

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

- BYOIP CIDR을 다시 확인하고 프로비저닝된 주소가 더 이상 없는지 확인합니다. 이 섹션의 명령을 실행하는 경우 --region의 값은 IPAM 리전과 일치해야 합니다.

이 단계는 **byoip-owner-account** 계정으로 수행해야 합니다.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
```

출력에 퍼블릭 IPv4 풀의 IP 주소 수가 표시됩니다.

```
{
  "PublicIpv4Pools": [
    {
      "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
      "Description": "",
      "PoolAddressRanges": [],
      "TotalAddressCount": 0,
      "TotalAvailableAddressCount": 0,
      "NetworkBorderGroup": "us-east-1",
      "Tags": []
    }
  ]
}
```

7. 다음 명령을 실행하여 최상위 풀을 삭제합니다.

```
aws ec2 delete-ipam-pool --region us-east-1 --profile ipam-account --ipam-pool-id ipam-pool-0a03d430ca3f5c035
```

출력에서 삭제 상태를 확인할 수 있습니다.

```
{
  "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"
  }
}

```

자습서: 서브넷 IP 할당을 위한 VPC IP 주소 공간 계획

이 자습서를 완료하면 VPC 서브넷에 IP 주소를 할당하기 위한 VPC IP 주소 공간을 계획하고 서브넷 및 VPC 수준에서 IP 주소 관련 지표를 모니터링할 수 있습니다.

Note

이 자습서에서는 프라이빗 IPAM 범위의 프라이빗 IPv4 주소 공간을 VPC와 서브넷에 할당하는 방법을 다룹니다. 또한 VPC 콘솔에서 Amazon 제공 IPv6 CIDR 블록 옵션으로 VPC를 생성하여 공개 범위 및 IPv6 CIDR 범위를 사용하여 이 자습서를 완료할 수 있습니다.

서브넷에 대한 VPC IP 주소 공간을 계획하면 다음을 수행할 수 있습니다.

- 서브넷에 할당할 VPC의 IP 주소 계획 및 구성: VPC IP 주소 공간을 더 작은 CIDR 블록으로 나누고 개발 또는 프로덕션 서브넷에서 워크로드를 실행하는 경우와 같이 비즈니스 요구 사항이 다른 서브넷에 해당 CIDR 블록을 프로비저닝할 수 있습니다.
- VPC 서브넷의 IP 주소 할당 간소화: VPC의 주소 공간을 계획하고 구성한 후에는 CIDR을 수동으로 입력하는 대신 넷마스크 길이를 선택할 수 있습니다. 예를 들어 개발자가 개발 워크로드를 호스팅하기 위해 서브넷을 생성하는 경우 서브넷에 대한 풀과 넷마스크 길이를 선택해야 합니다. 그러면 IPAM이 자동으로 CIDR 블록을 서브넷에 할당합니다.

다음 예에서는 이 자습서를 통해 생성할 풀과 리소스 구조의 계층을 보여줍니다.

- 프라이빗 범위
 - 리소스 계획 풀(10.0.0.0/20)
 - Dev 서브넷 풀(10.0.0.0/24)
 - Dev 서브넷(10.0.0.0/28)
 - Prod 서브넷 풀(10.0.0.1/24)
 - Prod 서브넷(10.0.0.16/28)

⚠ Important

- 리소스 계획 풀은 CIDR을 서브넷에 할당하는 데 사용하거나 다른 풀을 생성할 수 있는 소스 풀로 사용할 수 있습니다. 이 자습서에서는 리소스 계획 풀을 서브넷 풀의 소스 풀로 사용합니다.
- VPC에 CIDR이 두 개 이상 프로비저닝되어 있는 경우 동일한 VPC를 사용하여 여러 리소스 계획 풀을 생성할 수 있습니다. 예를 들어 VPC에 두 개의 CIDR이 할당된 경우 각 CIDR에서 하나씩 두 개의 리소스 계획 풀을 생성할 수 있습니다. 각 CIDR은 한 번에 하나의 풀에 할당할 수 있습니다.

1단계: VPC 생성

서브넷 IP 주소 계획에 사용할 VPC를 생성하려면 이 섹션의 단계를 완료하세요. VPC를 생성하는 데 필요한 IAM 권한에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [Amazon VPC 정책 예](#)를 참조하세요.

i Note

새 VPC를 만드는 대신 기존 VPC를 사용할 수 있지만, 이 자습서에서는 IPAM 할당 자동 CIDR 블록이 아닌 수동으로 할당된 CIDR 블록으로 VPC가 구성되는 시나리오에 중점을 둡니다.

VPC를 생성하려면

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/vpc/>에서 VPC 콘솔을 엽니다.
2. VPC 생성을 선택합니다.
3. VPC의 이름을 입력합니다(예: tutorial-vpc).
4. IPv4 CIDR 수동 입력을 선택하고 IPv4 CIDR 블록을 입력합니다. 이 자습서에서는 10.0.0.0/20을 사용합니다.
5. IPv6 CIDR 블록을 추가하는 옵션은 건너뛴니다.
6. VPC 생성을 선택합니다.
7. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
8. 왼쪽 탐색 창에서 리소스를 선택합니다.

9. 생성한 VPC가 나타날 때까지 기다립니다. 이 작업이 수행되는 데는 시간이 걸리며 해당 창이 나타나도록 하려면 창을 새로 고쳐야 할 수도 있습니다. 다음 단계로 넘어가기 전에 IPAM에서 VPC를 검색해야 합니다.

2단계: 리소스 계획 풀 생성

리소스 계획 풀을 생성하려면 이 섹션의 단계를 완료하세요.

리소스 계획 풀을 생성하려면

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택합니다.
4. 풀 생성을 선택합니다.
5. IPAM 범위에서 프라이빗 범위를 선택한 상태로 둡니다.
6. (선택 사항) 풀에 대한 이름 태그 추가합니다(예: 'Resource-planning-pool').
7. 소스에서 IPAM 범위를 선택합니다.
8. 리소스 계획에서 VPC 내 IP 공간 계획을 선택하고 이전 단계에서 생성한 VPC를 선택합니다. VPC는 리소스 계획 풀에 CIDR을 프로비저닝하는 데 사용되는 리소스입니다.
9. 프로비저닝할 CIDR에서 리소스 풀에 프로비저닝할 VPC CIDR을 선택합니다. 리소스 계획 풀에 프로비저닝하는 CIDR은 VPC에 프로비저닝된 CIDR과 일치해야 합니다. 이 자습서에서는 10.0.0.0/20을 사용합니다.
10. 풀 생성을 선택합니다.
11. 풀이 생성되면 CIDR 탭을 선택하여 프로비저닝된 CIDR의 상태를 확인합니다. 페이지를 새로 고치고 CIDR 상태가 프로비저닝 보류 중 상태에서 프로비저닝됨으로 변경될 때까지 기다린 후 다음 단계로 넘어갑니다.

3단계: 서브넷 풀 생성

서브넷에 IP 공간을 할당하는 데 사용할 두 개의 서브넷 풀을 생성하려면 이 섹션의 단계를 완료하세요.

서브넷 풀을 생성하려면

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.

2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택합니다.
4. 풀 생성을 선택합니다.
5. IPAM 범위에서 프라이빗 범위를 선택한 상태로 돕니다.
6. (선택 사항) 풀에 대한 이름 태그 추가합니다(예: 'dev-subnet-pool').
7. 소스에서 IPAM 풀을 선택하고 3단계에서 생성한 리소스 계획 풀을 선택합니다. 주소 패밀리, 리소스 계획 구성 및 로케일은 소스 풀에서 자동으로 상속됩니다.
8. 프로비저닝할 CIDR에서 서브넷 풀에 프로비저닝할 CIDR을 선택합니다. 이 자습서에서는 10.0.0.0/24를 사용합니다.
9. 풀 생성을 선택합니다.
10. 풀이 생성되면 CIDR 탭을 선택하여 프로비저닝된 CIDR의 상태를 확인합니다. 페이지를 새로 고치고 CIDR 상태가 프로비저닝 보류 중 상태에서 프로비저닝됨으로 변경될 때까지 기다린 후 다음 단계로 넘어갑니다.
11. 이 프로세스를 반복하여 'prod-subnet-pool'이라는 또 다른 서브넷을 생성합니다.

이때 이 서브넷 풀을 다른 AWS 계정에서 사용할 수 있도록 하려면 서브넷 풀을 공유하면 됩니다. 이를 수행하는 방법에 대한 지침은 [AWS RAM을 사용하여 IPAM 풀 공유](#)를 참조하세요. 그런 다음 여기로 돌아와 튜토리얼을 완료합니다.

4단계: 서브넷 생성

두 개의 서브넷을 생성하려면 다음 두 단계를 완료하세요.

서브넷을 생성하려면

1. 적절한 계정을 사용하여 <https://console.aws.amazon.com/vpc/>에서 VPC 콘솔을 엽니다.
2. 서브넷 > 서브넷 생성을 선택합니다.
3. 이 자습서를 시작할 때 생성한 VPC를 선택합니다.
4. 서브넷에 대한 이름을 입력합니다(예: "tutorial-subnet").
5. (선택 사항) 가용 영역을 선택합니다.
6. IPv4 CIDR 블록에서 IPAM 할당 IPV4 CIDR 블록을 선택하고 dev 서브넷 풀과 /28 넷마스크를 선택합니다.
7. 서브넷 생성(Create subnet)을 선택합니다.

8. 이 프로세스를 반복하여 또 다른 서브넷을 생성합니다. 이번에는 prod 서브넷 풀과 /28 넷마스크를 선택합니다.
9. IPAM 콘솔로 돌아와 왼쪽 탐색 창에서 리소스를 선택합니다.
10. 생성한 서브넷 풀을 찾아 생성한 서브넷이 그 아래에 나타날 때까지 기다립니다. 이 작업이 수행되는 데는 시간이 걸리며 해당 창이 나타나도록 하려면 창을 새로 고쳐야 할 수도 있습니다.

튜토리얼이 완료되었습니다. 필요에 따라 추가 서브넷 풀을 생성하거나 EC2 인스턴스에서 서브넷 중 하나로 시작할 수 있습니다.

IPAM은 서브넷의 IP 주소 사용과 관련된 지표를 게시합니다. SubnetIPUsage 지표에 CloudWatch 경보를 설정하여 IP 사용률 임계값 위반 시 조치를 취할 수 있습니다. 예를 들어 서브넷에 /24 CIDR(256 IP 주소)이 할당되어 있고 IP의 80%가 사용되었을 때 알림을 받고자 하는 경우, 이 임계값에 도달하면 알림을 보내도록 CloudWatch 경보를 설정할 수 있습니다. 서브넷 IP 사용에 대한 경보를 생성하는 방법에 대한 자세한 내용은 [경보 생성을 위한 간편 도움말](#)를 참조하세요.

5단계: 정리

이 자습서에서 생성한 리소스를 삭제하려면 다음 단계를 완료하세요.

리소스 정리

1. IPAM 관리자 계정을 사용하여 <https://console.aws.amazon.com/ipam/>에서 IPAM 콘솔을 엽니다.
2. 탐색 창에서 풀(Pools)을 선택합니다.
3. 프라이빗 범위를 선택합니다.
4. 리소스 계획 풀을 선택하고 작업 > 삭제를 선택합니다.
5. 계단식 삭제를 선택합니다. 리소스 계획 풀과 서브넷 풀이 삭제됩니다. 이렇게 해도 서브넷 자체는 삭제되지 않습니다. CIDR은 더 이상 IPAM 풀에서 제공되지 않지만 프로비저닝된 CIDR은 그대로 유지됩니다.
6. 삭제를 선택합니다.
7. [서브넷을 삭제합니다.](#)
8. [VPC를 삭제합니다.](#)

정리가 완료되었습니다.

IPAM의 자격 증명 및 액세스 관리

AWS는 보안 보안 인증을 사용하여 사용자를 식별하고 AWS리소스에 대한 액세스 권한을 부여합니다. AWS Identity and Access Management(IAM)의 기능을 사용하면 보안 보안 인증을 공유하지 않고도 다른 사용자, 서비스 및 애플리케이션이 AWS리소스를 완전히 또는 제한된 방식으로 사용할 수 있습니다.

이 섹션에서는 IPAM을 위해 특별히 생성된 AWS 서비스 연결 역할 및 IPAM 서비스 연결 역할에 연결된 관리형 정책에 대해 설명합니다. AWS IAM 역할 및 정책에 대한 자세한 내용은 IAM 사용 설명서의 [역할 용어 및 개념](#)을 참조하세요.

VPC의 자격 증명 및 액세스 관리에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [Amazon VPC의 자격 증명 및 액세스 관리](#)를 참조하세요.

내용

- [IPAM의 서비스 연결 역할](#)
- [IPAM에 대한 AWS 관리형 정책](#)
- [예제 정책](#)

IPAM의 서비스 연결 역할

AWS Identity and Access Management(IAM)의 서비스 연결 역할을 사용하면 AWS 서비스가 대신 다른 AWS 서비스를 호출할 수 있습니다. 서비스 연결 역할에 대한 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하세요

현재 IPAM에는 다음 서비스 연결 역할 1개만 있습니다. AWSServiceRoleForIPAM.

서비스 연결 역할에 부여된 권한

IPAM은 AWSServiceRoleForIPAM 서비스 연결 역할을 사용하여 연결된 AWSIPAMServiceRolePolicy 관리형 정책에서 작업을 호출합니다. 해당 정책에서 허용된 작업에 대한 자세한 내용은 [IPAM에 대한 AWS 관리형 정책](#) 섹션을 참조하세요.

또한 서비스 연결 역할에는 ipam.amazonaws.com 서비스가 서비스 연결 역할을 맡도록 허용하는 [IAM 신뢰 정책](#)이 연결되어 있습니다.

서비스 연결 역할 생성

IPAM은 계정에서 서비스 연결 역할을 맡고, 리소스 및 해당 CIDR을 검색하고, 리소스를 IPAM과 통합하여 하나 이상의 계정의 IP 주소 사용량을 모니터링합니다.

서비스 연결 역할은 다음의 두 가지 방법 중 하나로 생성됩니다.

- AWS Organizations과 통합하는 경우

IPAM 콘솔 [AWS Organization에서 계정과 IPAM 통합](#) 또는 `enable-ipam-organization-admin-account` AWS CLI 명령을 사용하는 경우 `AWSServiceRoleForIPAM` 서비스 연결 역할이 각 AWS Organizations 멤버 계정에서 자동으로 생성됩니다. 따라서 모든 멤버 계정 내의 리소스는 IPAM에서 검색할 수 있습니다.

Important

IPAM이 사용자를 대신하여 서비스 연결 역할을 생성할 수 있도록 하려면 다음을 수행합니다.

- AWS Organizations과 IPAM 통합을 사용하는 AWS Organizations 관리 계정에는 다음 작업을 허용하는 IAM 정책이 연결되어 있어야 합니다.
 - `ec2:EnableIpamOrganizationAdminAccount`
 - `organizations:EnableAwsServiceAccess`
 - `organizations:RegisterDelegatedAdministrator`
 - `iam:CreateServiceLinkedRole`
- IPAM 계정에는 `iam:CreateServiceLinkedRole` 작업을 허용하는 IAM 정책이 연결되어 있어야 합니다.

- 단일 AWS 계정을 사용하여 IPAM을 생성하는 경우

[단일 계정을 통해 IPAM 사용](#)이면 해당 계정으로 IPAM을 생성할 때 `AWSServiceRoleForIPAM` 서비스 연결 역할이 자동으로 생성됩니다.

Important

단일 AWS 계정으로 IPAM을 사용하는 경우, IPAM을 생성하기 전에 사용 중인 AWS 계정에 `iam:CreateServiceLinkedRole` 작업을 허용하는 IAM 정책이 연결되어 있는지 확인해야 합니다. IPAM을 생성할 경우 `AWSServiceRoleForIPAM` 서비스 연결 역할이 자동으로 생

성됩니다. IAM 정책 관리에 대한 자세한 내용은 [IAM 사용 설명서](#)의 IAM 정책 편집을 참조하세요.

서비스 연결 역할 편집

AWSServiceRoleForIPAM 서비스 연결 역할은 편집할 수 없습니다.

서비스 연결 역할 삭제

IPAM을 더 이상 사용할 필요 없는 경우 AWSServiceRoleForIPAM 서비스 연결 역할을 삭제하는 것이 좋습니다.

Note

서비스 연결 역할은 AWS 계정에서 IPAM 리소스를 모두 삭제한 후에만 삭제할 수 있습니다. 이렇게 하면 IPAM의 모니터링 기능은 실수로 제거될 수 없습니다.

AWS CLI를 통해 서비스 연결 역할을 삭제하려면 다음 단계를 따릅니다.

1. [deprovision-ipam-pool-cidr](#) 및 [delete-ipam](#)을 사용하여 IPAM 리소스를 삭제합니다. 자세한 내용은 [풀에서 CIDR 프로비저닝 해제 및 IPAM 삭제](#) 섹션을 참조하세요.
2. [disable-ipam-organization-admin-account](#)를 사용하여 IPAM 계정을 사용 중지합니다.
3. `--service-principal ipam.amazonaws.com` 옵션을 사용하여 [disable-aws-service-access](#)로 IPAM 서비스를 사용 중지합니다.
4. 서비스 연결 역할 삭제: [delete-service-linked-role](#). 서비스 연결 역할을 삭제하면 IPAM 관리형 정책도 삭제됩니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 삭제](#)를 참조하십시오.

IPAM에 대한 AWS 관리형 정책

단일 AWS 계정을 사용하여 IPAM을 사용 중이고 IPAM을 생성하는 경우 AWSIPAMServiceRolePolicy 관리형 정책이 IAM 계정에 자동으로 생성되고 AWSServiceRoleForIPAM [서비스 연결 역할](#)에 연결됩니다.

AWS Organizations과의 IPAM 통합을 사용하면 AWSIPAMServiceRolePolicy 관리형 정책이 IAM 계정과 각 AWS Organizations 멤버 계정에 자동으로 생성되고 관리형 정책은 AWSServiceRoleForIPAM 서비스 연결 역할에 연결됩니다.

이 관리형 정책을 사용하면 IPAM이 다음을 수행할 수 있습니다.

- AWS Organizations의 모든 멤버에 걸쳐 네트워킹 리소스와 연결된 CIDR을 모니터링합니다.
- IPAM 풀에서 사용 가능한 IP 주소 공간 및 할당 규칙을 준수하는 리소스 CIDR 수 등 IPAM과 관련된 지표를 Amazon CloudWatch에 저장합니다.

다음은 생성된 관리형 정책의 세부 정보를 보여주는 예입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAMDiscoveryDescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchMetricsPublishActions",
      "Effect": "Allow",
      "Action": "cloudwatch:PutMetricData",
```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": "AWS/IPAM"
      }
    }
  }
]
}

```

위 예의 첫 번째 명령문을 사용하면 IPAM이 단일 AWS 계정 또는 AWS Organizations의 멤버를 사용해 CIDR을 모니터링할 수 있습니다.

위 예의 두 번째 명령문은 `cloudwatch:PutMetricData` 조건 키를 사용하여 IPAM이 IPAM 지표를 AWS/IPAM [Amazon CloudWatch 네임스페이스](#)에 저장하도록 허용합니다. 이러한 지표는 IPAM 풀 및 범위의 할당에 대한 데이터를 표시하는 AWS 관리 콘솔에서 사용합니다. 자세한 내용은 [IPAM 대시보드를 사용하여 CIDR 사용량 모니터링](#) 섹션을 참조하세요.

AWS 관리형 정책으로 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후부터 IPAM의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다.

변경 사항	설명	날짜
AWSIPAMServiceRolePolicy	리소스 검색 중에 IPAM이 퍼블릭 IP 주소를 가져올 수 있도록 AWSIPAMServiceRolePolicy 관리형 정책(<code>ec2:GetIpamDiscoveredPublicAddresses</code>)에 작업이 추가되었습니다.	2023년 11월 13일
AWSIPAMServiceRolePolicy	리소스 검색 중에 IPAM이 퍼블릭 IP 주소를 가져올 수 있도록 AWSIPAMServiceRolePolicy 관리형 정책(<code>ec2:DescribeAccountAttributes</code>),	2023년 11월 1일

변경 사항	설명	날짜
	ec2:DescribeNetworkInterfaces , ec2:DescribeSecurityGroups , ec2:DescribeSecurityGroupRules , ec2:DescribeVpnConnections , globalaccelerator:ListAccelerators , globalaccelerator:ListByoipCidrs)에 작업이 추가되었습니다.	
AWSIPAMServiceRolePolicy	IPAM이 리소스 검색 중에 모니터링되는 AWS 계정과 리소스 CIDR을 가져올 수 있도록 AWSIPAMServiceRolePolicy 관리형 정책에 두 가지 작업 (ec2:GetIpamDiscoveredAccounts 및 ec2:GetIpamDiscoveredResourceCidrs)이 추가되었습니다.	2023년 1월 25일
IPAM이 변경 사항 추적 시작	IPAM이 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2021년 12월 2일

예제 정책

이 섹션의 예제 정책에는 전체 IPAM 사용에 대한 모든 관련 AWS Identity and Access Management(IAM) 작업이 포함되어 있습니다. IPAM을 사용하는 방식에 따라 모든 IAM 작업을 포함하지 않아도 될 수 있습니다. IPAM 콘솔을 완벽하게 사용하려면 AWS Organizations, AWS Resource Access Manager(RAM), Amazon CloudWatch 같은 서비스에 대한 추가 IAM 작업을 포함해야 할 수 있습니다.

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

IPAM의 할당량

이 섹션에는 IPAM과 관련된 할당량이 나열되어 있습니다. Service Quotas 콘솔은 IPAM 할당량에 대한 정보를 제공합니다. Service Quotas 콘솔을 사용하면 기본 할당량을 확인하고 조정 가능한 할당량에 대한 [할당량 증가를 요청](#)할 수 있습니다. 자세한 내용은 Service Quotas 사용 설명서의 [할당량 증가 요청](#)을 참조하십시오.

명칭	기본값	조정 가능
Amazon 제공 IPv6 CIDR 블록 넷마스크 길이	/52	예. AWS 일반 참조의 AWS Service Quotas 에 설명된 대로 AWS Support Center에 문의하세요.
리전당 Amazon 제공 IPv6 CIDR 블록	1	예. AWS 일반 참조의 AWS Service Quotas 에 설명된 대로 AWS Support Center에 문의하세요.
IPAM으로 가져올 수 있는 Autonomous System Number(ASN)	5	예. AWS 일반 참조의 AWS Service Quotas 에 설명된 대로 AWS Support Center에 문의하세요.
폴당 CIDR	50	예
조직당 IPAM 관리자	1	아니요
리전당 IPAM	1	아니요
폴 깊이(폴 내의 폴 수)	10	예
범위당 폴	50	예
IPAM당 리소스 검색 연결	5	예

명칭	기본값	조정 가능
리전당 리소스 검색	1	아니요
리소스 사용률 지표	50	예. AWS 일반 참조의 AWS Service Quotas 에 설명된 대로 AWS Support Center에 문의하세요.
IPAM당 범위	5	예 . IPAM을 생성하면 프라이빗 및 퍼블릭 기본 범위가 하나씩 생성됩니다. 추가 범위를 생성하려는 경우 프라이빗 범위를 생성할 수 있습니다. 프라이빗 범위를 추가로 생성할 수 없습니다.

IPAM 가격

이 섹션에서는 소스 검색의 세부 정보를 보는 방법을 설명합니다.

요금 정보 보기

IPAM은 프리 티어와 고급 티어로 제공됩니다. 각 티어에서 사용할 수 있는 기능 및 티어 관련 비용에 대한 자세한 내용은 [Amazon VPC 요금 페이지](#)의 IPAM 탭을 참조하세요.

AWS Cost Explorer을(를) 사용하여 현재 비용 및 사용량 확인

IPAM 고급 티어를 사용하는 경우 IPAM에서 관리하는 활성 IP 주소당 시간당 요금을 지불합니다. IPAM 비용 및 사용량을 보고 분석하려면 AWS Cost Explorer을(를) 사용합니다.

1. <https://console.aws.amazon.com/cost-management/home>에서 AWS Cost Management 콘솔을 엽니다.
2. Cost Explorer를 시작합니다.
3. 사용 유형을 선택하고 **IPAddressManager**을(를) 입력하여 IPAM 사용량을 필터링합니다.
4. 하나 이상의 체크 박스를 선택합니다. 각각 다른 AWS 리전을 나타냅니다.
5. 적용을 클릭합니다.

예를 들어 USE1-IPAddressManager-IP-Hours(시간)를 선택했을 때 us-east-1이 IPAM 홈 리전이 되면 IPAM이 청구하는 활성 IP 시간과 비용이 표시됩니다. 만약 사용량 시간이 18시간인 경우 18시간 동안 활성 IP 주소 1개를 사용하거나 세 리전에서 세 IP 주소를 각각 6시간 동안 활성화하거나 그것을 조합하여 어떤 방법으로든 최대 18시간을 사용할 수 있습니다.

AWS Cost Explorer에 대한 자세한 내용은 AWS Cost Management 사용 설명서의 [AWS Cost Explorer를 사용한 비용 분석](#)을 참조하세요.

관련 정보

다음의 관련 리소스는 이 서비스를 이용할 때 도움이 될 수 있습니다.

- [Amazon VPC IP 주소 관리자 모범 사례](#): VPC IP 주소 관리자를 사용하여 확장 가능한 주소 체계를 계획하고 생성하는 모범 사례를 다룬 AWS 블로그입니다.
- [Amazon VPC IP 주소 관리자를 통한 대규모 네트워크 주소 관리 및 감사](#): Amazon VPC IP 주소 관리자를 소개하고 AWS 콘솔에서 서비스를 사용하는 방법을 보여주는 AWS 블로그입니다.
- [Configure fine-grained access to your resources shared using AWS Resource Access Manager](#): IPAM 풀을 AWS Organizations 조직 단위의 계정과 공유하는 방법을 설명하는 AWS 블로그입니다.

IPAM 관련 문서 기록

다음 표에서는 IPAM의 릴리스를 설명합니다.

기능	설명	릴리스 날짜
IPAM 프리 티어 및 고급 티어	이제 IPAM에 대해 프리 티어와 고급 티어 중에서 선택할 수 있습니다.	2023년 11월 17일
퍼블릭 IP 인사이트	이전에는 단일 리전에서만 퍼블릭 IP 인사이트를 볼 수 있었습니다. 이제 여러 리전에 걸쳐 퍼블릭 IP 인사이트를 볼 수 있습니다. 또한 이제 Amazon CloudWatch에서 Amazon CloudWatch 을 볼 수 있습니다.	2023년 11월 17일
서브넷 IP 할당을 위한 VPC IP 주소 공간 계획	이제 IPAM을 사용하여 VPC 내 서브넷 IP 공간을 계획하고 서브넷 및 VPC 수준에서 IP 주소 관련 지표를 모니터링할 수 있습니다.	2023년 11월 17일
기존 보유 ASN 가져오기(BYOASN)	이제 기존 보유 Autonomous System Number(ASN)을 AWS로 가져올 수 있습니다.	2023년 11월 17일
AWS 관리형 정책 업데이트 - 기존 정책에 대한 업데이트	기존 AWSIPAMServiceRolePolicy가 업데이트되었습니다.	2023년 11월 17일
AWS 관리형 정책 업데이트 - 기존 정책에 대한 업데이트	기존 AWSIPAMServiceRolePolicy가 업데이트되었습니다.	2023년 11월 1일
리소스 사용률 지표	IPAM은 이제 IPAM이 모니터링하는 리소스에 대한 IP 사용률 지표를 Amazon CloudWatch에 게시합니다.	2023년 8월 2일
퍼블릭 IP 인사이트	퍼블릭 IP 인사이트는 계정에서 이 리전의 서비스에서 사용하는 모든 퍼블릭 IPv4 주소를 보여 줍니다. 이러한 인사이트를 사용하여 퍼블릭	2023년 7월 28일

기능	설명	릴리스 날짜
	IPv4 주소 사용을 식별하고 사용하지 않는 탄력적 IP 주소를 해제하기 위한 권장 사항을 볼 수 있습니다.	
AWS 관리형 정책 업데이트 - 기존 정책에 대한 업데이트	기존 AWSIPAMServiceRolePolicy가 업데이트되었습니다.	2023년 1월 25일
IPAM을 조직 외부 계정과 통합	이제 단일 IPAM 계정에서 조직 외부의 IP 주소를 관리하고 IPAM 풀을 다른 AWS Organizations의 계정과 공유할 수 있습니다.	2023년 1월 25일
IPAM 풀에 대한 Amazon 제공 IPv6 연속 CIDR 블록	퍼블릭 범위에서 IPAM 풀을 생성하면 이제 Amazon 제공 IPv6 연속 CIDR 블록을 풀에 프로비저닝할 수 있습니다. 자세한 내용은 IPv6 풀 생성 단원을 참조하십시오.	2023년 1월 25일
최초 릴리스	이번 릴리스에서는 Amazon VPC IP 주소 관리자를 도입합니다.	2021년 12월 2일