IP Address Manager

Amazon Virtual Private Cloud

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud: IP Address Manager

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione ad alcun prodotto o servizio che non sia di Amazon, in alcun modo che possa causare confusione tra i clienti, né in alcun modo che possa denigrare o screditare Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è IPAM? ... 1
Funzionamento di IPAM ... 2
Nozioni di base su IPAM ... 4
Accedi a IPAM ... 4
Configura le opzioni di integrazione per IPAM ... 5
Integrare IPAM con gli account di un'organizzazione AWS ... 6
Come integrare IPAM con account esterni alla tua organizzazione ... 8
Utilizza IPAM con un singolo account ... 11
Crea un IPAM ... 12
Pianificare il provisioning degli indirizzi IP ... 14
Esempio di piani di pool IPAM ... 16
Crea IPv4 pool ... 18
Crea pool IPv6 ... 28
Allocare CIDRs ... 36
Creare un VPC che utilizza un CIDR del pool IPAM ... 37
Assegna manualmente un CIDR a un pool per riservare lo spazio degli indirizzi IP ... 38
Gestione dello spazio degli indirizzi IP in IPAM ... 40
Modifica lo stato di monitoraggio del VPC CIDRs ... 41
Crea ambiti aggiuntivi ... 42
Elimina un IPAM ... 43
Elimina un pool ... 45
Elimina un ambito ... 46
Deapprovvigionamento CIDRs da un pool ... 48
Modifica un pool IPAM ... 49
Abilita la distribuzione dei costi ... 50
Abilita il provisioning GUA privato IPv6 CIDRs ... 51
Implementa l'uso di IPAM per la creazione di VPC con SCPs ... 53
Applica l'IPAM durante la creazione VPCs ... 53
Applica un pool IPAM durante la creazione VPCs ... 54
Applica l'IPAM per tutti tranne un determinato elenco di OUs ... 55
Escludi unità organizzative da IPAM ... 56
Come funzionano le esclusioni delle unità organizzative ... 56
Aggiungi o rimuovi esclusioni di unità organizzative ... 58
Modifica un livello IPAM ... 64

Modifica le regioni operative IPAM 66
Fornitura CIDRs a un pool 67
Sposta il VPC CIDRs tra gli ambiti 69
Rilasciare un'assegnazione 70
Condivisione di un pool IPAM tramite AWS RAM 72
Lavora con il rilevamento delle risorse 74
Come creare un rilevamento delle risorse 75
Come visualizzare i dettagli del rilevamento delle risorse 77
Come condividere un rilevamento delle risorse 79
Come associare un rilevamento delle risorse a un IPAM 81
Come annullare l'associazione di un rilevamento delle risorse 83
Come eliminare un rilevamento delle risorse 84
Monitoraggio dell'utilizzo dell'indirizzo IP in IPAM 85
Monitora l'utilizzo del CIDR con il pannello di controllo IPAM 85
Monitoraggio dell'utilizzo del CIDR per risorsa 89
Monitora l'IPAM con Amazon CloudWatch 93
Pool e metriche dell'ambito 94
Parametri di utilizzo delle risorse 97
Visualizzazione della cronologia degli indirizzi IP 102
Visualizzazione di informazioni dettagliate relative agli indirizzi IP pubblici 106
Tutorial 111
Guida introduttiva a IPAM utilizzando la CLI AWS 111
Prerequisiti 111
Crea un IPAM 112
Ottieni l'ID dell'ambito IPAM 112
Crea un pool di primo livello IPv4 113
Crea un pool regionale IPv4 113
Crea un pool di sviluppo IPv4 114
Creare un VPC utilizzando un pool IPAM CIDR 115
Verifica l'allocazione del pool IPAM 116
Risoluzione dei problemi 116
Pulizia delle risorse 117
Passaggi successivi 118
Creazione di IPAM e pool utilizzando la console 119
Prerequisiti 111
Come si AWS Organizations integra con IPAM 120

Fase 1: delega di un amministratore IPAM 121
Passaggio 2: creazione di un IPAM 123
Passaggio 3: creazione di un pool IPAM di livello superiore 125
Fase 4: creazione di pool IPAM regionali 130
Fase 5: creazione di un pool di sviluppo di pre-produzione 134
Fase 6: condivisione del pool IPAM 138
Fase 7: creazione di un VPC con un CIDR assegnato da un pool IPAM 143
Fase 8: eliminazione 147
Crea un IPAM e dei pool utilizzando il AWS CLI 149
Passaggio 1: abilitare IPAM nella tua organizzazione 150
Passaggio 2: creare un IPAM 150
Fase 3: Creare un pool di IPv4 indirizzi 152
Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore 154
Fase 5. Crea un pool Regionale con CIDR proveniente dal pool di livello superiore 155
Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale 157
Fase 7. Creare una condivisione RAM per abilitare le assegnazioni IP tra gli account 159
Fase 8. Crea un VPC 160
Fase 9. Rimozione 160
Visualizza la cronologia degli indirizzi IP utilizzando il AWS CLI 161
Panoramica 162
Scenari 162
Porta il tuo ASN in IPAM 170
Prerequisiti di onboarding per l'ASN 171
Passaggi del tutorial 172
Trasferisci i tuoi indirizzi IP su IPAM 176
Verifica il controllo del dominio 176
BYOIP con AWS console e CLI 183
Solo BYOIP con CLI AWS 211
Trasferire un CIDR BYOIP a IPAM IPv4 258
Fase 1: Creare profili AWS CLI denominati e ruoli IAM 259
Passaggio 2: ottenimento dell'ID di ambito pubblico dell'IPAM 260
Passaggio 3: creazione di un pool IPAM 261
Passaggio 4: condividere il pool IPAM utilizzando AWS RAM 263
Passaggio 5: trasferimento di un CIDR BYOIP IPV4 esistente in IPAM 265
Passaggio 6: visualizzazione del CIDR in IPAM 268
Passaggio 7: pulizia 268

Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti 271
Fase 1. Creazione di un VPC 273
Passaggio 2: Creazione di un pool di pianificazione delle risorse 274
Passaggio 3: Creazione di pool di sottoreti 274
Passaggio 4: Creazione di sottoreti 275
Fase 5: eliminazione 276
Assegna indirizzi IP elastici sequenziali da un pool IPAM 277
Fase 1: creare un IPAM 278
Passaggio 2: creazione di un pool IPAM e provisioning di un CIDR 280
Passaggio 3: assegnazione di un indirizzo IP elastico dal pool 284
Fase 4: Associare l'indirizzo IP elastico a un'istanza EC2 286
Passaggio 5: tracciamento e monitoraggio dell'utilizzo del pool 286
Rimozione 288
Identity and Access Management in IPAM 290
Ruoli collegati al servizio per IPAM 290
Autorizzazioni del ruolo collegato ai servizi 290
Creazione del ruolo collegato ai servizi 291
Modifica del ruolo collegato ai servizi 292
Eliminazione del ruolo collegato ai servizi 292
Policy gestite per IPAM 293
Aggiornamenti alla politica gestita AWS 294
Policy di esempio 296
Quote 299
Prezzi 302
Visualizza informazioni sui prezzi 302
Visualizza i costi e l'utilizzo attuali utilizzando AWS Cost Explorer 302
Informazioni correlate 304
Cronologia dei documenti 305
..... cccviii

Che cos'è IPAM?

Amazon VPC IP Address Manager (IPAM) è una funzionalità VPC che semplifica la pianificazione, il monitoraggio e il monitoraggio degli indirizzi IP per i carichi di lavoro. AWS È possibile utilizzare i flussi di lavoro automatizzati di IPAM per gestire in modo più efficiente gli indirizzi IP.

È possibile usare IPAM per le seguenti operazioni:

- Organizzare lo spazio degli indirizzi IP in domini di routing e sicurezza
- Monitorare lo spazio degli indirizzi IP in uso e monitorare le risorse che utilizzano lo spazio rispetto alle regole aziendali
- Visualizzare la cronologia delle assegnazioni di indirizzi IP nell'organizzazione
- Assegna automaticamente all'utilizzo di regole aziendali specifiche CIDRs VPCs
- Risolvere i problemi di connettività
- Abilita la condivisione tra regioni e tra account degli indirizzi Porta il tuo indirizzo IP (BYOIP)
- Esegui il provisioning di blocchi IPv6 CIDR contigui forniti da Amazon ai pool per la creazione di VPC

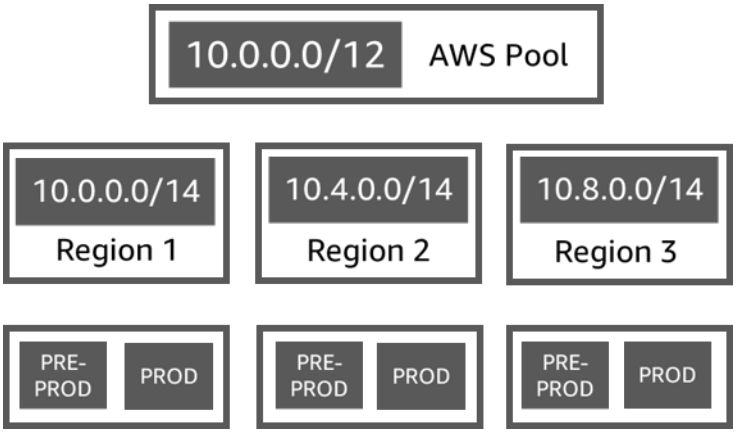
Questa guida contiene le sezioni seguenti:

- Funzionamento di IPAM: Concetti e terminologia IPAM.
- Nozioni di base su IPAM: passaggi per abilitare la gestione degli indirizzi IP a livello aziendale con AWS Organizations, creare un IPAM e pianificare l'utilizzo degli indirizzi IP.
- Gestione dello spazio degli indirizzi IP in IPAM: Passaggi per gestire IPAM, ambiti, pool e assegnazioni.
- Monitoraggio dell'utilizzo dell'indirizzo IP in IPAM: Passaggi per monitorare e tracciare l'utilizzo degli indirizzi IP con IPAM.
- Tutorial per Amazon VPC IP Address Manager: step-by-step Tutorial dettagliati per creare un IPAM e pool CIDRs, allocare un VPC e trasferire il proprio indirizzo IP pubblico in IPAM. CIDRs

Funzionamento di IPAM

Questo argomento spiega alcuni dei concetti chiave per aiutarti ad iniziare a utilizzare IPAM.

Il diagramma seguente mostra una gerarchia di pool IPAM per più AWS regioni all'interno di un pool IPAM di primo livello. Ogni pool AWS regionale include due pool di sviluppo IPAM, un pool per la preproduzione e un pool di risorse di produzione. Per ulteriori informazioni su IPAM, consultare le descrizioni sotto il diagramma.



Per utilizzare IP Address Manager di Amazon VPC, è necessario creare per prima cosa un IPAM.

Quando crei l'IPAM, scegli in quale AWS regione crearlo. Quando si crea un IPAM, AWS VPC IPAM crea automaticamente due ambiti per l'IPAM. Gli ambiti, insieme a pool e assegnazioni, sono componenti chiave del tuo IPAM.

- Un ambito è il container di più alto livello all'interno di IPAM. Quando crei un IPAM, vengono creati in automatico un ambito privato e un ambito pubblico predefiniti. Ogni ambito rappresenta lo spazio IP per una singola rete. L'ambito privato è destinato a tutti gli indirizzi IP che non possono essere pubblicizzati su Internet. L'ambito pubblico è generalmente destinato a tutti gli indirizzi IP dai quali è possibile pubblicizzare su Internet. AWS Tieni presente che quando fornisci BYOIPv6 indirizzi a un pool IPAM, puoi configurare gli indirizzi in modo che non siano pubblicizzabili pubblicamente sebbene siano di dominio pubblico. Gli ambiti consentono di riutilizzare gli indirizzi IP su più reti non connesse senza causare sovrapposizioni o conflitti di indirizzi IP. All'interno di un ambito, si creano pool IPAM.
- Un pool è una raccolta di intervalli di indirizzi IP contigui (o). CIDRs I pool IPAM consentono di organizzare gli indirizzi IP in base alle esigenze di routing e sicurezza. Puoi avere più pool all'interno di un pool di livello superiore. Ad esempio, se si hanno esigenze di routing e sicurezza

separate per le applicazioni di sviluppo e produzione, è possibile creare un pool per ciascuna. All'interno dei pool IPAM, l'allocazione CIDRs viene effettuata in base alle risorse. AWS

- Un'allocazione è un incarico CIDR da un pool IPAM a un'altra risorsa o pool IPAM. Quando si crea un VPC e si sceglie un pool IPAM per il CIDR del VPC, il CIDR viene allocato dal CIDR su cui è stato effettuato il provisioning al pool IPAM. È possibile monitorare e gestire l'assegnazione con IPAM.

IPAM può gestire e monitorare lo spazio pubblico e privato. IPv6 Per ulteriori informazioni sugli IPv6 indirizzi pubblici e privati, consulta IPv6 gli indirizzi nella Amazon VPC User Guide.

Per iniziare e creare un IPAM, consulta Nozioni di base su IPAM.

Nozioni di base su IPAM

Segui la procedura riportata in questo tutorial per iniziare a utilizzare IPAM. Questa sezione ha lo scopo di aiutarti a iniziare rapidamente a usare IPAM, ma il risultato dei passaggi in questa sezione potrebbe non soddisfare le tue esigenze. Per informazioni sui diversi modi per utilizzare IPAM, vedi Pianificare il provisioning degli indirizzi IP e Tutorial per Amazon VPC IP Address Manager.

In questa sezione, il primo passaggio è accedere a IPAM e decidere se delegare un account IPAM. Alla fine di questa sezione, avrai creato un IPAM, creato più pool di indirizzi IP e assegnato un CIDR in un pool a un VPC.

Attività

- Accedi a IPAM
- Configura le opzioni di integrazione per IPAM
- Crea un IPAM
- Pianificare il provisioning degli indirizzi IP
- Allocazione CIDRs da un pool IPAM

Accedi a IPAM

Come con altri AWS servizi, puoi creare, accedere e gestire il tuo IPAM utilizzando i seguenti metodi:

- AWS Console di gestione: fornisce un'interfaccia web che è possibile utilizzare per creare e gestire l'IPAM. Per informazioni, consulta https://console.aws.amazon.com/ipam/.
- AWS Interfaccia a riga di comando (AWS CLI): fornisce comandi per un'ampia gamma di AWS servizi, tra cui Amazon VPC. La AWS CLI è supportata su Windows, macOS e Linux. Per ottenere la AWS CLI, consulta. AWS Command Line Interface
- AWS SDKs: Fornisci informazioni specifiche per la lingua APIs. AWS SDKsSi occupano di molti dettagli di connessione, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta AWS SDKs.
- API della query: fornisce operazioni API di basso livello accessibili tramite richieste HTTPS. L'utilizzo dell'API della query è il modo più diretto di accedere a IPAM. Tuttavia, richiede che l'applicazione gestisca dettagli di basso livello, come la generazione dell'hash per firmare la richiesta e la gestione degli errori. Per ulteriori informazioni, consulta le azioni di Amazon IPAM nell'Amazon EC2 API Reference.

Questa guida si concentra principalmente sull'uso della console di AWS gestione per creare, accedere e gestire il tuo IPAM. In ogni descrizione su come completare un processo nella console, includiamo collegamenti alla documentazione della AWS CLI che mostra come eseguire la stessa operazione utilizzando la AWS CLI.

Se utilizzi IPAM per la prima volta, consulta Funzionamento di IPAM per conoscere il ruolo di IPAM in Amazon VPC e quindi continua con le istruzioni in Configura le opzioni di integrazione per IPAM.

Configura le opzioni di integrazione per IPAM

Questa sezione descrive le opzioni su come integrare IPAM con AWS Organizations, altri AWS account o utilizzarlo con un singolo AWS account.

Prima di iniziare a utilizzare IPAM, è necessario scegliere una delle opzioni in questa sezione per consentire a IPAM di monitorare le risorse di EC2 rete e CIDRs archiviare le metriche:

- Per consentire l'integrazione di IPAM con AWS Organizations il servizio IPAM di Amazon VPC per gestire e monitorare le risorse di rete create da tutti gli account membri di AWS Organizations, consulta. Integrare IPAM con gli account di un'organizzazione AWS
- Dopo l'integrazione con AWS Organizations, per integrare IPAM con account esterni all'organizzazione, consulta. Come integrare IPAM con account esterni alla tua organizzazione
- Per utilizzare un singolo AWS account con IPAM e abilitare il servizio IPAM di Amazon VPC per gestire e monitorare le risorse di rete create con il singolo account, consulta. Utilizza IPAM con un singolo account

Se non scegli una di queste opzioni, puoi comunque creare risorse IPAM come ad esempio i pool, ma non vedrai i parametri nel pannello di controllo e non sarai in grado di monitorare lo stato delle risorse.

Indice

- Integrare IPAM con gli account di un'organizzazione AWS
- Come integrare IPAM con account esterni alla tua organizzazione
- Utilizza IPAM con un singolo account

Integrare IPAM con gli account di un'organizzazione AWS

Facoltativamente, puoi seguire i passaggi descritti in questa sezione per integrare IPAM con AWS Organizations e delegare un account membro come l'account IPAM.

L'account IPAM è responsabile della creazione e dell'utilizzo di un IPAM per gestire e monitorare l'uso dell'indirizzo IP.

L'integrazione di IPAM con AWS Organizations e la delega di un amministratore IPAM offre i seguenti vantaggi:

- Condividi i tuoi pool IPAM con la tua organizzazione: quando deleghi un account IPAM, IPAM consente agli altri account membri dell'organizzazione di allocare CIDRs dai pool IPAM condivisi utilizzando Resource Access Manager AWS (RAM). AWS Per ulteriori informazioni su come configurare un'organizzazione, consulta Cos'è AWS Organizations? nella Guida per l'utente di AWS Organizations.
- Monitora l'utilizzo degli indirizzi IP nella tua organizzazione: Quando si delega un account IPAM, viene concessa l'autorizzazione a IPAM per monitorare l'utilizzo dell'IP in tutti gli account. Di conseguenza, IPAM importa automaticamente in IPAM CIDRs ciò che viene utilizzato dagli account membri esistenti VPCs in altre AWS Organizations.

Se non delegate un account membro di AWS Organizations come account IPAM, IPAM monitorerà le risorse solo nell' AWS account che utilizzate per creare l'IPAM.

> **Note**
>
> Durante l'integrazione con AWS Organizations:
>
> - È necessario abilitare l'integrazione con AWS Organizations utilizzando IPAM nella console di AWS gestione o il comando enable-ipam-organization-adminCLI -account AWS . Ciò garantisce la creazione del ruolo collegato ai servizi `AWSServiceRoleForIPAM`. Se abiliti l'accesso affidabile con AWS Organizations utilizzando la console AWS Organizations o il comando register-delegated-administrator AWS CLI, il ruolo `AWSServiceRoleForIPAM` collegato al servizio non viene creato e non puoi gestire o monitorare le risorse all'interno dell'organizzazione.
> - L'account IPAM deve essere un account membro di AWS Organizations. Non è possibile utilizzare l'account di gestione AWS Organizations come account IPAM. Per verificare se il

tuo IPAM è già integrato con AWS Organizations, utilizza i passaggi seguenti e visualizza i dettagli dell'integrazione nelle impostazioni dell'organizzazione.

- IPAM addebita ogni indirizzo IP attivo monitorato negli account membri dell'organizzazione. Per ulteriori informazioni sui prezzi, consulta Prezzi di IPAM.
- È necessario disporre di un account in AWS Organizations e di un account di gestione configurato con uno o più account membro. Per ulteriori informazioni sui vari tipi di account, consultare Terminologia e concetti nella Guida per l'utente di AWS Organizations. Per ulteriori informazioni sulla configurazione di un'organizzazione, consultare Nozioni di base su AWS Organizations.
- L'account IPAM deve disporre di un ruolo IAM che ha una policy IAM collegata che consenta l'operazione `iam:CreateServiceLinkedRole`. Quando si crea l'IPAM, si crea automaticamente il ruolo collegato al servizio AWSService RoleFor IPAM.
- L'utente associato all'account di gestione AWS Organizations deve utilizzare un ruolo IAM a cui sono associate le seguenti azioni politiche IAM:
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`
  - `iam:CreateServiceLinkedRole`

  Per ulteriori informazioni sulla creazione di ruoli IAM, consulta Creazione di un ruolo per delegare le autorizzazioni a un utente IAM nella Guida per l'utente di IAM.
- L'utente associato all'account di gestione AWS Organizations può utilizzare un ruolo IAM a cui sono allegate le seguenti azioni politiche IAM per elencare gli amministratori delegati di AWS Org attuali: `organizations:ListDelegatedAdministrators`

AWS Management Console

Per selezionare un account IPAM

1. Utilizzando l'account di gestione AWS Organizations, apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nella Console di AWS gestione, scegli la AWS regione in cui desideri lavorare con IPAM.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione).

4. L'opzione Delegate è disponibile solo se hai effettuato l'accesso alla console come account di gestione AWS Organizations. Scegli Delega.
5. Inserisci l'ID dell' AWS account per un account IPAM. L'amministratore IPAM deve essere un account membro di AWS Organizations.
6. Scegli Save changes (Salva modifiche).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Per delegare un account amministratore IPAM utilizzando AWS CLI, usa il seguente comando: -account enable-ipam-organization-admin

Quando si delega un account membro di Organizations come account IPAM, IPAM creerà automaticamente un ruolo IAM collegato al servizio in tutti gli account membri dell'organizzazione. IPAM monitora l'utilizzo degli indirizzi IP in questi account assumendo il ruolo IAM collegato al servizio in ciascun account membro, individuando le risorse e le relative risorse e integrandole con IPAM. CIDRs Le risorse all'interno di tutti gli account membri saranno individuabili dall'IPAM indipendentemente dalla loro Unità Organizzativa. Se sono presenti account membri che hanno creato un VPC, ad esempio, vedrai il VPC e il relativo CIDR nella sezione Risorse della console IPAM.

> **Important**
>
> Il ruolo dell'account di AWS Organizations gestione che ha delegato l'amministratore IPAM è ora completo. Per continuare a utilizzare IPAM, l'account amministratore IPAM deve accedere all'IPAM di Amazon VPC e creare un IPAM.

Come integrare IPAM con account esterni alla tua organizzazione

Questa sezione spiega come integrare il tuo IPAM con account AWS esterni alla tua organizzazione. Per completare la procedura riportata in questa sezione, è necessario avere già completato la procedura descritta in Integrare IPAM con gli account di un'organizzazione AWS e avere già delegato un account IPAM.

L'integrazione di IPAM con account AWS esterni alla tua organizzazione consente di effettuare le seguenti operazioni:

- Gestisci indirizzi IP esterni alla tua organizzazione da un singolo account IPAM.
- Condividere pool IPAM con servizi di terzi ospitati da altri account AWS in altre AWS Organizations.

Una volta integrato un IPAM con account AWS esterni alla tua organizzazione, puoi condividere un pool IPAM direttamente con gli account desiderati di altre organizzazioni.

Indice

- Considerazioni e limitazioni
- Panoramica del processo

Considerazioni e limitazioni

Questa sezione include considerazioni e limitazioni per l'integrazione di IPAM con account esterni alla tua organizzazione:

- Quando condividi un rilevamento delle risorse con un altro account, gli unici dati che vengono scambiati sono l'indirizzo IP e i dati di monitoraggio dello stato dell'account. È possibile visualizzare questi dati prima di condividerli utilizzando i comandi get-ipam-discovered-resource-cidrs e get-ipam-discovered-accountsCLI o and. GetIpamDiscoveredResourceCidrsGetIpamDiscoveredAccounts APIs Per i rilevamenti delle risorse che monitorano le risorse in un'organizzazione, non vengono condivisi dati dell'organizzazione (ad esempio i nomi delle unità organizzative nella tua organizzazione).
- Quando crei un rilevamento delle risorse, il rilevamento delle risorse monitora tutte le risorse visibili nell'account del proprietario. Se l'account del proprietario è un AWS account di servizio di terze parti che crea risorse per più clienti propri, tali risorse verranno scoperte mediante l'individuazione delle risorse. Se l'account di AWS servizio di terze parti condivide l'individuazione delle risorse con un AWS account utente finale, l'utente finale avrà visibilità sulle risorse degli altri clienti del servizio di terze parti. AWS Per questo motivo, il AWS servizio di terze parti deve prestare attenzione nel creare e condividere le scoperte di risorse o utilizzare un account separato AWS per ogni cliente.

Panoramica del processo

Questa sezione spiega come integrare l'IPAM con AWS account esterni all'organizzazione. Si riferisce agli argomenti trattati in altre sezioni di questa guida. Lascia visibile questa pagina e apri gli argomenti con i link seguenti in una nuova finestra i in modo da poter tornare a questa pagina per ottenere assistenza.

Quando si integra IPAM con AWS account esterni all'organizzazione, il processo coinvolge 4 AWS account:

- Proprietario principale dell'organizzazione: l'account di AWS Organizations gestione dell'organizzazione 1.
- Account IPAM dell'organizzazione primaria: l'account amministratore delegato IPAM per l'organizzazione 1.
- Proprietario secondario dell'organizzazione: l'account di AWS Organizations gestione dell'organizzazione 2.
- Account amministratore dell'organizzazione secondaria: l'account amministratore delegato IPAM per l'organizzazione 2.

Fasi

1. Il proprietario dell'organizzazione primaria delega un membro della sua organizzazione come account IPAM dell'organizzazione primaria (consulta Integrare IPAM con gli account di un'organizzazione AWS).
2. L'account IPAM dell'organizzazione primaria crea un IPAM (consulta Crea un IPAM).
3. Il proprietario dell'organizzazione secondaria delega un membro della sua organizzazione come account amministratore dell'organizzazione secondaria (consulta Integrare IPAM con gli account di un'organizzazione AWS).
4. L'account di amministratore dell'organizzazione secondaria crea un rilevamento delle risorse e lo condivide con l'account IPAM dell'organizzazione principale utilizzando AWS RAM (vedi Crea un rilevamento di risorse da integrare con un altro IPAM eCondividi la scoperta di una risorsa con un altro AWS account). Il rilevamento delle risorse deve essere creato nella stessa regione di origine dell'IPAM dell'organizzazione primaria.
5. L'account IPAM dell'organizzazione principale accetta l'invito alla condivisione delle risorse utilizzando AWS RAM (vedi Accettazione e rifiuto degli inviti alla condivisione delle risorse nella Guida per l'AWS RAM utente).

6. L'account IPAM dell'organizzazione primaria associa il rilevamento delle risorse al suo IPAM (consulta Come associare un rilevamento delle risorse a un IPAM).
7. A questo punto, l'account IPAM dell'organizzazione primaria può monitorare e/o gestire le risorse IPAM create dagli account nell'organizzazione secondaria.
8. (Facoltativo) L'account IPAM dell'organizzazione primaria condivide i pool IPAM con gli account dei membri nell'organizzazione secondaria (consulta Condivisione di un pool IPAM tramite AWS RAM).
9. (Facoltativo) Se l'account IPAM dell'organizzazione primaria desidera interrompere il rilevamento delle risorse nell'organizzazione secondaria, può annullare l'associazione del rilevamento delle risorse all'IPAM (consulta Come annullare l'associazione di un rilevamento delle risorse).
10. (Facoltativo) Se l'account amministratore dell'organizzazione secondaria desidera interrompere la partecipazione all'IPAM dell'organizzazione primaria, può annullare la condivisione del rilevamento delle risorse condivisa (consulta Come aggiornare una condivisione di risorse AWS RAM nella Guida per l'utente di AWS RAM) o eliminare il rilevamento delle risorse (consulta Come eliminare un rilevamento delle risorse).

Utilizza IPAM con un singolo account

Se scegli di non farloIntegrare IPAM con gli account di un'organizzazione AWS, puoi utilizzare IPAM con un unico AWS account.

Quando crei un IPAM nella sezione successiva, viene creato automaticamente un ruolo collegato al servizio IPAM di Amazon VPC in (IAM). AWS Identity and Access Management

I ruoli collegati ai servizi sono un tipo di ruolo IAM che consente ai servizi di accedere ad altri AWS servizi per tuo conto. AWS Semplificano il processo di gestione delle autorizzazioni creando e gestendo automaticamente le autorizzazioni necessarie affinché AWS servizi specifici possano eseguire le azioni richieste, semplificando la configurazione e l'amministrazione di questi servizi.

IPAM utilizza il ruolo collegato ai servizi per monitorare e archiviare le metriche associate alle risorse di rete. CIDRs EC2 Per ulteriori informazioni sul ruolo collegato al servizio e su come IPAM ne fa uso, consulta Ruoli collegati al servizio per IPAM.

> **Important**
>
> Se si utilizza IPAM con un singolo AWS account, è necessario assicurarsi che l' AWS account utilizzato per creare l'IPAM utilizzi un ruolo IAM a cui è associata una policy

che consenta l'azione. `iam:CreateServiceLinkedRole` Quando crei l'IPAM, crei automaticamente il ruolo collegato al AWSService RoleFor servizio IPAM. Per maggiori informazioni sulla gestione di una policy IAM, consultare Creazione di policy IAM nella Guida per l'utente di IAM.

Una volta che l' AWS account singolo ha l'autorizzazione a creare il ruolo collegato al servizio IPAM, vai a. Crea un IPAM

Crea un IPAM

Per creare un IPAM, segui i passaggi descritti in questa sezione. Se è stato delegato un amministratore IPAM, questi passaggi devono essere completati dall'account IPAM.

Important

Quando crei un IPAM, ti verrà chiesto di permettere a IPAM di replicare i dati dagli account fonte in un account IPAM delegato. Per integrare IPAM con AWS Organizations, IPAM richiede l'autorizzazione dell'utente per replicare i dettagli sull'utilizzo delle risorse e degli IP tra account (dagli account membro all'account membro IPAM delegato) e tra AWS regioni (dalle regioni operative alla regione di origine dell'IPAM). Per gli utenti IPAM con account singolo, è necessaria l'autorizzazione per replicare i dettagli di utilizzo delle risorse e dell'IP tra Regioni operative nella Regione di origine dell'IPAM.

Quando si crea l'IPAM, si scelgono le AWS regioni in cui l'IPAM è autorizzato a gestire l'indirizzo IP. CIDRs Queste AWS regioni sono chiamate regioni operative. IPAM rileva e monitora le risorse solo nelle AWS regioni selezionate come regioni operative. IPAM non archivia dati al di fuori delle Regioni operative selezionate.

La gerarchia di esempio seguente mostra come le AWS regioni assegnate al momento della creazione dell'IPAM influiranno sulle regioni che saranno disponibili per i pool creati in seguito.

- IPAM che opera nella AWS Regione 1 e nella Regione 2 AWS
  - Ambito privato
    - Pool IPAM di alto livello
      - Pool IPAM Regionale nella Regione AWS 2

- Pool di sviluppo
  - Assegnazione per un VPC nella Regione AWS 2

Puoi creare un solo IPAM. Per ulteriori informazioni su come aumentare le quote relative all'IPAM, consulta Quote per l'IPAM.

AWS Management Console

Per creare un IPAM

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nella console di AWS gestione, scegli la AWS regione in cui desideri creare l'IPAM. Crea l'IPAM nella tua Regione operativa principale.
3. Nella home page del servizio, scegli Crea IPAM.
4. Seleziona Consenti a IP Address Manager di Amazon VPC di replicare i dati dagli account sorgente verso l'account IPAM delegato. Se non si seleziona questa opzione, non sarà possibile creare un IPAM.
5. Scegli un IPAM tier (Livello IPAM). Per ulteriori informazioni sulle funzionalità disponibili in ogni livello e sui costi associati ai livelli, consulta la scheda IPAM nella pagina dei prezzi di Amazon VPC.
6. In Regioni operative, seleziona le AWS regioni in cui questo IPAM può gestire e scoprire le risorse. La AWS regione in cui si sta creando l'IPAM è selezionata come una delle regioni operative per impostazione predefinita. Ad esempio, se stai creando questo IPAM in AWS Regione `us-east-1` ma desideri creare successivamente pool IPAM regionali che lo CIDRs forniscano VPCs `us-west-2`, seleziona qui. `us-west-2` Se si dimentica una Regione operativa, sarà possibile ritornarvi in un secondo momento e modificare le impostazioni IPAM.

> **Note**
>
> Se stai creando un IPAM nel livello gratuito, puoi selezionare più regioni operative per il tuo IPAM, ma l'unica funzionalità IPAM che sarà disponibile nelle regioni operative è Informazioni sugli IP pubblici. Non puoi utilizzare altre funzionalità nel livello gratuito, come BYOIP, nelle regioni operative dell'IPAM. Puoi utilizzarle solo nella regione di origine dell'IPAM. Per utilizzare tutte le funzionalità IPAM nelle regioni operative, crea un IPAM nel livello avanzato.

7. Scegli se vuoi abilitare il GUA privato IPv6 . CIDRs Per ulteriori informazioni su questa opzione, consulta Abilita il provisioning GUA privato IPv6 CIDRs.
8. Scegli se vuoi abilitare la modalità di misurazione. Per ulteriori informazioni su questa opzione, consulta Abilita la distribuzione dei costi.
9. Scegli Create IPAM (Crea IPAM).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti AWS CLI comandi per creare, modificare e visualizzare i dettagli relativi al tuo IPAM:

1. Crea l'IPAM: create-ipam
2. Visualizza l'IPAM che hai creato: describe-ipams
3. Visualizza gli ambiti creati automaticamente: describe-ipam-scopes
4. Modificare un IPAM esistente: modify-ipam

Dopo aver completato questi passaggi, IPAM avrà fatto quanto segue:

- Creato il tuo IPAM. È possibile visualizzare l'IPAM e le regioni operative attualmente selezionate selezionando IPAMs nel riquadro di navigazione a sinistra della console.
- Creato un ambito privato e uno pubblico. È possibile visualizzare gli ambiti scegliendo Ambiti nel pannello di navigazione. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.

Pianificare il provisioning degli indirizzi IP

Segui la procedura descritta in questa sezione per pianificare il provisioning dell'indirizzo IP utilizzando i pool IPAM. Se hai configurato un account IPAM, questi passaggi dovrebbero essere completati da tale account. Il processo di creazione del pool è diverso per i pool in ambito pubblico e privato. Questa sezione include i passaggi per la creazione di un pool regionale in ambito privato. Per i tutorial su BYOIP e BYOASN, vedi Tutorial.

> **Important**
>
> Per utilizzare i pool IPAM tra AWS account, è necessario integrare IPAM con AWS Organizations o alcune funzionalità potrebbero non funzionare correttamente. Per ulteriori informazioni, consulta Integrare IPAM con gli account di un'organizzazione AWS.

In IPAM, un pool è una raccolta di intervalli di indirizzi IP contigui (o). CIDRs I pool IPAM consentono di organizzare gli indirizzi IP in base alle esigenze di routing e sicurezza. È possibile creare pool per AWS regioni esterne alla propria regione IPAM. Ad esempio, se si hanno esigenze di routing e sicurezza separate per le applicazioni di sviluppo e produzione, è possibile creare un pool per ciascuna.

Nel primo passaggio di questa sezione creerai un pool di livello superiore. Quindi, creerai un pool Regionale all'interno del pool di livello superiore. All'interno del pool Regionale è possibile creare pool aggiuntivi in base alle esigenze, come ad esempio pool di ambienti di produzione e sviluppo. Per impostazione predefinita, puoi creare pool fino a una profondità di 10. Per informazioni sulle quote IPAM, consulta Quote per l'IPAM.

> **Note**
>
> I termini effettuare il provisioning e assegnare sono utilizzati in questa guida per l'utente e nella console IPAM. Effettuare il provisioning viene utilizzato quando si aggiunge un CIDR a un pool IPAM. Assegnare viene utilizzato quando si associa un CIDR da un pool IPAM a una risorsa.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare completando i passaggi contenuti in questa sezione:

- IPAM che opera nella AWS Regione 1 e AWS nella Regione 2
  - Ambito privato
    - Pool di livello superiore
      - Pool regionale nella AWS Regione 1
        - Pool di sviluppo
          - Assegnazione per un VPC

Questa struttura è un esempio di come si potrebbe voler utilizzare IPAM, ma è possibile utilizzare IPAM per soddisfare le esigenze della propria organizzazione. Per ulteriori informazioni sulle best practice, consulta Best practice di Amazon VPC IP Address Manager.

Se stai creando un unico pool IPAM, completa i passaggi descritti in Creare un pool di primo livello IPv4 , quindi passa a Allocazione CIDRs da un pool IPAM.

Indice

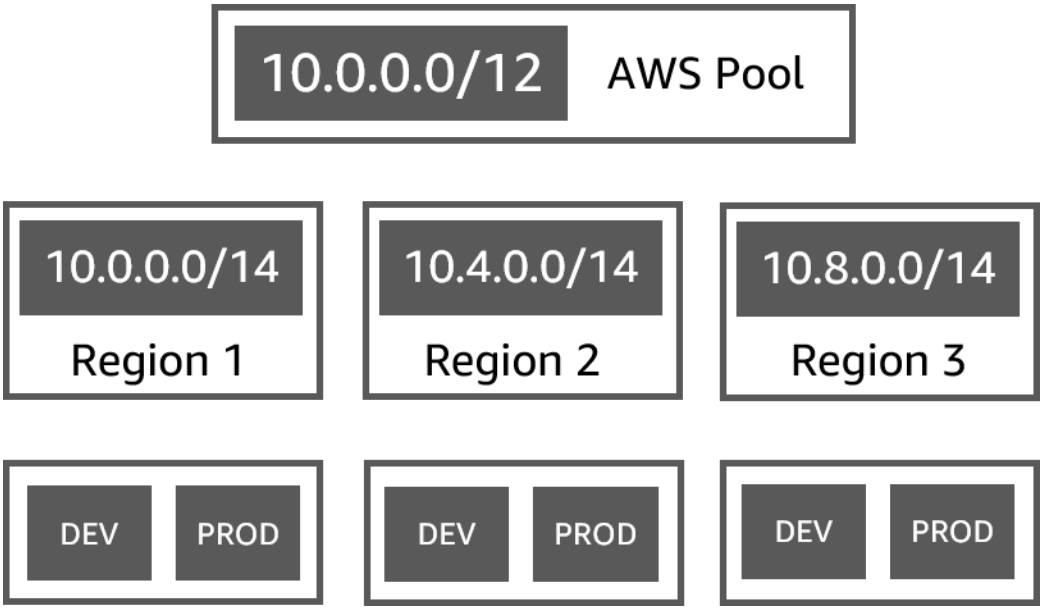
- Esempio di piani di pool IPAM
- Crea IPv4 pool
- Crea pool di IPv6 indirizzi nel tuo IPAM

Esempio di piani di pool IPAM

Puoi usare IPAM per soddisfare le esigenze della tua organizzazione. In questa sezione vengono forniti esempi su come organizzare gli indirizzi IP.

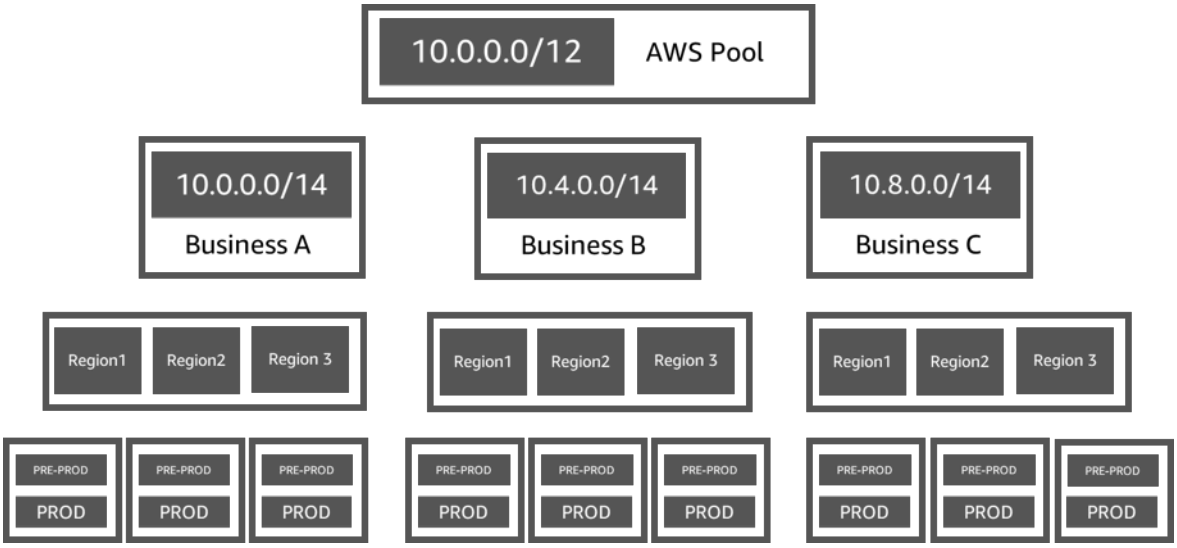
IPv4 pool in più AWS regioni

L'esempio seguente mostra una gerarchia di pool IPAM per più AWS regioni all'interno di un pool di primo livello. Ogni pool AWS regionale include due pool di sviluppo IPAM, un pool per le risorse di sviluppo e un pool per le risorse di produzione.



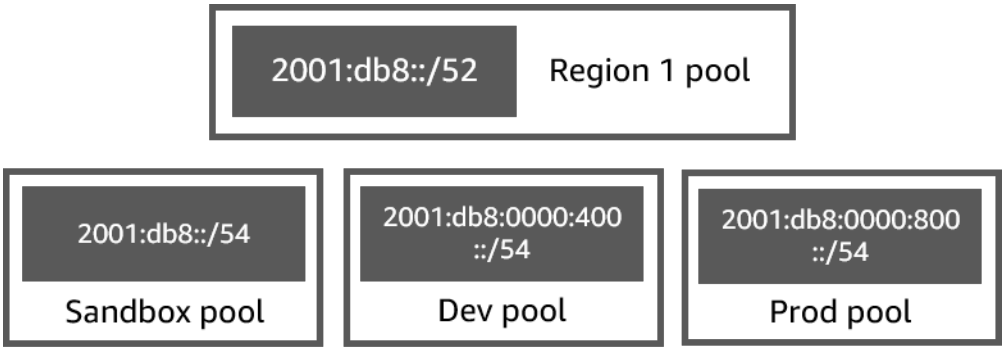
IPv4 pool per più linee di business

L'esempio seguente mostra una gerarchia di pool IPAM per più linee di business all'interno di un pool di livello superiore. Ogni pool per ogni linea di attività contiene tre pool AWS regionali. Ogni pool Regionale ha due pool di sviluppo IPAM al suo interno, un pool per la pre-produzione e uno per la produzione di risorse.



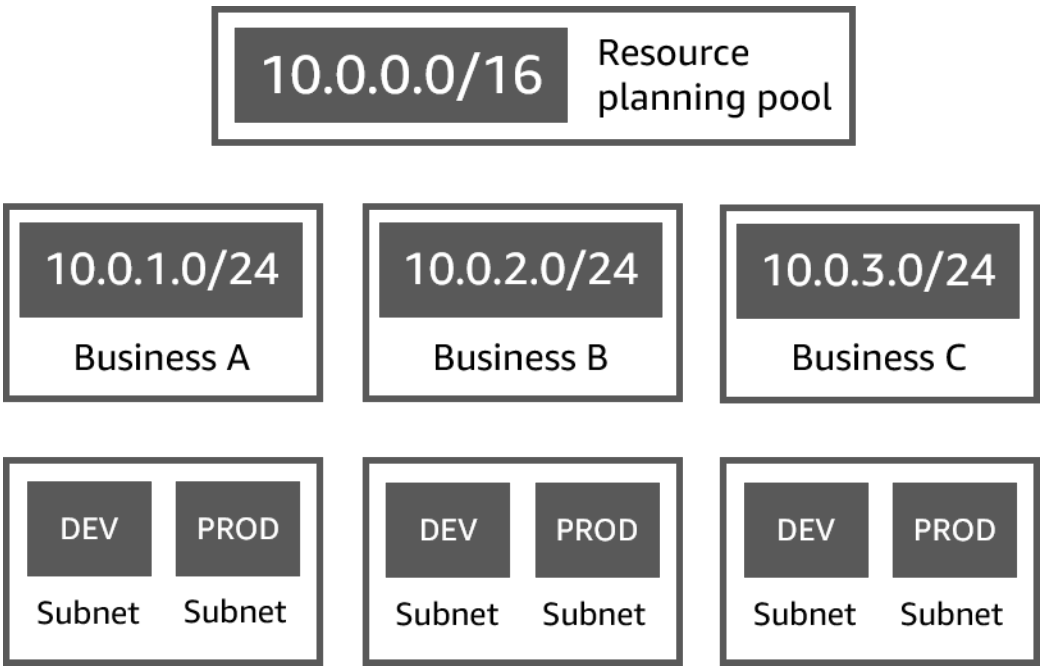
IPv6 pool in una AWS regione

L'esempio seguente mostra una gerarchia di IPv6 pool IPAM per più linee di business all'interno di un pool regionale. Ogni pool regionale include tre pool IPAM, un pool per l'ambiente di sperimentazione (sandbox) delle risorse, uno per le risorse di sviluppo e uno per le risorse di produzione.



Pool di sottoreti per più linee di business

L'esempio seguente mostra una gerarchia di pool di pianificazione delle risorse per più linee di business e pool di sottoreti di sviluppo / di produzione. Per ulteriori informazioni sulla pianificazione dello spazio degli indirizzi IP della sottorete utilizzando IPAM, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.



Crea IPv4 pool

Segui i passaggi di questa sezione per creare una gerarchia di pool IPv4 IPAM.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare con le istruzioni contenute in questa guida. In questa sezione, si sta creando una gerarchia di pool IPv4 IPAM:

- IPAM che opera nella AWS Regione 1 e nella Regione 2 AWS
  - Ambito privato
    - Pool di livello superiore (10.0.0.0/8)
      - Pool regionale nella AWS Regione 2 (10.0.0.0/16)
        - Pool di sviluppo (10.0.0.0/24)
          - Allocazione per un VPC (10.0.0.0/25)

Nell'esempio precedente, quelli utilizzati sono solo CIDRs esempi. Essi mostrano che ogni pool all'interno del pool di alto livello è dotato di una parte del CIDR di alto livello.

Indice

- Creare un pool di primo livello IPv4
- Crea un IPv4 pool regionale

- Crea un IPv4 pool di sviluppo

Creare un pool di primo livello IPv4

Segui i passaggi di questa sezione per creare un pool IPAM IPv4 di primo livello. Quando crei il pool, effettui il provisioning di un CIDR per il pool da utilizzare. Assegna, quindi, tale spazio a un'allocazione. Un'allocazione è un'assegnazione CIDR da un pool IPAM a un'altra risorsa o pool IPAM.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare con le istruzioni contenute in questa guida. In questa fase stai creando un pool Regionale IPAM:

- IPAM che opera nella AWS Regione 1 e nella Regione 2 AWS
  - Ambito privato
    - Pool di livello superiore (10.0.0.0/8)
      - Pool regionale nella AWS Regione 1 (10.0.0.0/16)
        - Pool di sviluppo per attività non produttive (10.0.0.0/24) VPCs
          - Allocazione per un VPC (10.0.0.0/25)

Nell'esempio precedente, quelli utilizzati sono solo esempi. CIDRs Essi mostrano che ogni pool all'interno del pool di alto livello è dotato di una parte del CIDR di alto livello.

Quando si crea un pool IPAM, è possibile configurare le regole per le assegnazioni effettuate all'interno del pool IPAM.

Le regole di assegnazione consentono di configurare quanto segue:

- Se IPAM deve importare automaticamente CIDRs nel pool IPAM se li trova all'interno dell'intervallo CIDR di questo pool
- La lunghezza della netmask richiesta per le assegnazioni all'interno del pool
- I tag richiesti per le risorse all'interno del pool
- La località richiesta per le risorse all'interno del pool. La locale è la AWS regione in cui è disponibile un pool IPAM per le allocazioni.

Le regole di assegnazione determinano se le risorse sono conformi o non conformi. Per ulteriori informazioni sulla conformità, consulta Monitoraggio dell'utilizzo del CIDR per risorsa.

> **Important**
>
> Esiste una regola implicita aggiuntiva che non viene visualizzata nelle regole di assegnazione. Se la risorsa si trova in un pool IPAM che è una risorsa condivisa in AWS Resource Access Manager (RAM), il proprietario della risorsa deve essere configurato come principale nella AWS RAM. Per ulteriori informazioni sulla condivisione di pool con RAM, consulta Condivisione di un pool IPAM tramite AWS RAM.

L'esempio seguente mostra come utilizzare le regole di assegnazione per controllare l'accesso a un pool IPAM:

Example

Quando crei i pool in base alle esigenze di routing e sicurezza, potresti voler permettere solo a determinate risorse di utilizzare un pool. In questi casi è possibile impostare una regola di assegnazione che indica che qualsiasi risorsa che desidera un CIDR da questo pool deve avere un tag che corrisponda ai requisiti del tag della regola di assegnazione. Ad esempio, è possibile impostare una regola di allocazione che stabilisca che solo VPCs con il tag prod può accedere CIDRs a un pool IPAM. È inoltre possibile impostare una regola che stabilisca che l' CIDRs allocazione da questo pool non può essere maggiore di /24. In questo caso, la creazione di una risorsa utilizzando un CIDR maggiore di /24 da questo pool viola una regola di allocazione sul pool e la creazione non riesce. Le risorse esistenti con un CIDR maggiore di /24 vengono contrassegnate come non conformi.

> **Important**
>
> Questo argomento spiega come creare un IPv4 pool di primo livello con un intervallo di indirizzi IP fornito da. AWS Se si desidera portare il proprio intervallo di IPv4 indirizzi a AWS (BYOIP), esistono dei prerequisiti. Per ulteriori informazioni, consulta Tutorial: trasferisci i tuoi indirizzi IP su IPAM.

AWS Management Console

Per creare un pool

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.

3. Scegli Crea pool.
4. Sotto la voce Ambito IPAM scegli l'ambito privato che vuoi utilizzare. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.

   Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. I pool nell'ambito privato devono essere IPv4 pool. Le piscine in ambito pubblico possono essere le IPv4 nostre IPv6 piscine. L'ambito pubblico è destinato a tutti gli spazi pubblici.
5. (Facoltativo) Aggiungi un Tag nome e una descrizione per il pool.
6. In Source (Origine), scegli IPAM scope (Ambito IPAM).
7. In Famiglia di indirizzi, scegli IPv4.
8. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
9. Per la Località, scegli Nessuna. Imposterai la località sul pool Regionale.

   La lingua è la AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni. Ad esempio, è possibile assegnare un CIDR per un VPC solo da un pool IPAM che condivide una lingua con la Regione del VPC. Tieni presente che dopo aver scelto una lingua per un pool, questa non può essere modificata. Se la regione di origine dell'IPAM non è disponibile a causa di un'interruzione e il pool è in una località differente dalla regione di origine dell'IPAM, il pool può essere ancora utilizzato per assegnare gli indirizzi IP.
10. (Facoltativo) Puoi creare un pool senza CIDR, ma non potrai utilizzare il pool per le allocazioni fino a quando non avrai eseguito il provisioning di un CIDR per tale pool. Per effettuare il provisioning di un CIDR, scegli Aggiungi nuovo CIDR. Inserite un IPv4 CIDR per il provisioning del pool. Se desideri aggiungere il tuo intervallo di indirizzi IPv6 IP IPv4 o il tuo intervallo di indirizzi IP, AWS ci sono dei prerequisiti. Per ulteriori informazioni, consulta Tutorial: trasferisci i tuoi indirizzi IP su IPAM.
11. Scegli le regole di assegnazione facoltative per questo pool:

    - Importazione automatica delle risorse rilevale: questa opzione non è disponibile se la Località è impostata su Nessuna. Se selezionato, IPAM cercherà continuamente le risorse all'interno dell'intervallo CIDR di questo pool e le importerà automaticamente come assegnazioni nel tuo IPAM. Tieni presente quanto segue:

- Le risorse CIDRs che verranno allocate per queste risorse non devono essere già assegnate ad altre risorse affinché l'importazione abbia esito positivo.
- IPAM importerà un CIDR indipendentemente dalla conformità con le regole di allocazione del pool, in modo che una risorsa possa essere importata e successivamente contrassegnata come non conforme.
- Se IPAM ne rileva più di uno CIDRs che si sovrappone, IPAM importerà solo il CIDR più grande.
- Se IPAM ne rileva più di uno CIDRs con corrispondenza CIDRs, IPAM ne importerà in modo casuale solo uno.

> ⚠ Warning
>
> - Dopo aver creato un IPAM, quando crei un VPC, scegli l'opzione di blocco CIDR allocato dall'IPAM. In caso contrario, il CIDR scelto per il VPC potrebbe sovrapporsi a un'allocazione CIDR IPAM.
> - Se hai già un cloud VPC allocato in un pool IPAM, un cloud VPC con un CIDR sovrapposto non può essere importato automaticamente. Ad esempio, se hai un VPC con CIDR 10.0.0.0/26 allocato in un pool IPAM, non puoi importare un VPC con CIDR 10.0.0.0/23 (che si sovrapporrebbe al CIDR 10.0.0.0/26).
> - L'importazione automatica in IPAM delle allocazioni CIDR dei VPC esistenti richiede tempo.

- Lunghezza minima della netmask: la lunghezza minima della netmask richiesta affinché le assegnazioni CIDR in questo pool IPAM siano conformi e il blocco CIDR di dimensioni maggiori che può essere assegnato dal pool. La lunghezza minima della netmask deve essere inferiore alla lunghezza massima della netmask. Le lunghezze possibili delle maschere di rete per gli indirizzi sono comprese tra 0 e 32. IPv4 Le lunghezze possibili delle maschere di rete per IPv6 gli indirizzi sono comprese tra 0 e 128.
- Lunghezza di default della netmask: lunghezza di default della netmask per le assegnazioni aggiunte a questo pool. Ad esempio, se il CIDR di cui è stato eseguito il provisioning in questo pool è **`10.0.0.0/8`** e qui inserisci **`16`**, per tutte le nuove allocazioni in questo pool verrà ripristinata l'impostazione predefinita della lunghezza della maschera di rete /16.
- Lunghezza massima della netmask: la lunghezza massima della netmask richiesta per le assegnazioni CIDR in questo pool. Questo valore determina il blocco CIDR di dimensioni più piccole che può essere assegnato dal pool.

- Requisiti per l'assegnazione di tag: i tag necessari alle risorse per assegnare spazio dal pool. Se i tag delle risorse sono stati modificati dopo aver assegnato spazio o se le regole di assegnazione di tag di allocazione vengono modificate nel pool, la risorsa potrebbe essere contrassegnata come non conforme.
- Locale: la versione locale che sarà richiesta per le risorse utilizzate CIDRs da questo pool. Le risorse importate automaticamente che non dispongono di questa località saranno contrassegnate come non conformi. Le risorse che non vengono importate automaticamente nel pool non saranno autorizzate ad assegnare spazio dal pool a meno che non si trovino in questa località.

> **Note**
>
> Le regole di allocazione si applicano solo alle risorse gestite all'interno di quel pool. Le regole non si applicano alle risorse nei pool all'interno di un pool.

12. (Facoltativo) Scegli Tag per il pool.
13. Scegli Crea pool.
14. Consultare Crea un IPv4 pool regionale.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti AWS CLI comandi per creare o modificare un pool di primo livello nel tuo IPAM:

1. Crea un pool:. create-ipam-pool
2. Modifica il pool dopo averlo creato per modificare le regole di allocazione: modify-ipam-pool.

Crea un IPv4 pool regionale

Segui i passaggi in questa sezione per creare un pool Regionale all'interno del tuo pool di livello superiore. Se hai bisogno solo di un pool di livello superiore e non di pool aggiuntivi Regionali e di sviluppo, vai a Allocazione CIDRs da un pool IPAM.

> **Note**
>
> Il processo di creazione del pool è diverso per i pool in ambito pubblico e privato. Questa sezione include i passaggi per la creazione di un pool regionale in ambito privato. Per i tutorial su BYOIP e BYOASN, vedi Tutorial.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare con le istruzioni contenute in questa guida. In questa fase stai creando un pool Regionale IPAM:

- IPAM che opera nella AWS Regione 1 e AWS nella Regione 2
  - Ambito privato
    - Pool di livello superiore (10.0.0.0/8)
      - Pool regionale nella AWS Regione 1 (10.0.0.0/16)
        - Pool di sviluppo per attività non produttive (10.0.0.0/24) VPCs
          - Allocazione per un VPC (10.0.0.0/25)

Nell'esempio precedente, quelli utilizzati sono solo esempi. CIDRs Essi mostrano che ogni pool all'interno del pool di livello superiore è dotato di una parte del CIDR di livello superiore.

AWS Management Console

Per creare un pool Regionale all'interno di un pool di livello superiore

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli Crea pool.
4. Sotto la voce Pool scegli lo stesso ambito utilizzato al momento della creazione dei pool di livello superiore. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
5. (Facoltativo) Aggiungi un Tag nome e una descrizione per il pool.
6. In Source (Origine), scegli IPAM pool (Pool IPAM). Quindi scegli il pool di livello superiore creato nella sezione precedente.
7. Se stai creando questo pool in ambito pubblico, vedrai un'opzione per Famiglia di indirizzi. Scegli IPv4.

8. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
9. Scegli la località per il pool. La scelta di una località garantisce che non vi siano dipendenze interregionali tra il pool e le risorse da esso assegnate. Le opzioni qui disponibili provengono dalle Regioni operative scelte al momento della creazione dell'IPAM.

   La lingua è la AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni. Ad esempio, è possibile assegnare un CIDR per un VPC solo da un pool IPAM che condivide una lingua con la Regione del VPC. Tieni presente che dopo aver scelto una lingua per un pool, questa non può essere modificata. Se la regione di origine dell'IPAM non è disponibile a causa di un'interruzione e il pool è in una località differente dalla regione di origine dell'IPAM, il pool può essere ancora utilizzato per assegnare gli indirizzi IP.

   > **Note**
   >
   > Se stai creando un pool nel livello gratuito, puoi scegliere solo la locale corrispondente alla regione di origine del tuo IPAM. Per utilizzare tutte le funzionalità IPAM nelle locale, esegui l'upgrade al livello avanzato.

10. Se stai creando questo pool in ambito pubblico, vedrai un'opzione per Servizio. Scegli EC2(EIP/VPC). Il servizio selezionato determina il servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione è EC2 (EIP/VPC), il che significa che quanto CIDRs allocato da questo pool sarà pubblicizzabile per il EC2 servizio Amazon (per indirizzi IP elastici) e il servizio Amazon VPC (per associato a). CIDRs VPCs
11. (Facoltativo) Scegliere un CIDR su cui effettuare il provisioning per il pool. Puoi creare un pool senza CIDR, ma non sarai in grado di utilizzare il pool per le assegnazioni fino a quando non avrai eseguito il provisioning di un CIDR. Puoi aggiungere qualcosa CIDRs a un pool in qualsiasi momento modificando il pool.
12. Qui hai a disposizione le stesse opzioni delle regole di assegnazione rispetto a quando hai creato il pool Regionale di alto livello. Consulta Creare un pool di primo livello IPv4 per una spiegazione delle opzioni disponibili durante la creazione di pool. Le regole di allocazione per il pool Regionale non vengono ereditate dal pool di primo livello. Se non si applica alcuna regola, non verranno impostate regole di assegnazione per il pool.
13. (Facoltativo) Scegli Tag per il pool.

14. Quando hai finito di configurare il pool, scegli Crea pool.
15. Per informazioni, consulta Crea un IPv4 pool di sviluppo.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Usa i seguenti AWS CLI comandi per creare un pool regionale nel tuo IPAM:

1. Ottieni l'ID dell'ambito in cui desideri creare il pool: describe-ipam-scopes
2. Ottieni l'ID del pool in cui vuoi creare il pool: describe-ipam-pools
3. Crea il pool: create-ipam-pool
4. Visualizza il nuovo pool: describe-ipam-pools

Ripeti questi passaggi per creare pool aggiuntivi all'interno del pool di livello superiore, secondo necessità.

Crea un IPv4 pool di sviluppo

Segui i passaggi in questa sezione per creare un pool di sviluppo all'interno del tuo pool regionale. Se hai bisogno solo di un pool di alto livello e regionale e non di un pool di sviluppo, vai a Allocazione CIDRs da un pool IPAM.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare con le istruzioni contenute in questa guida. In questa fase stai creando un pool di sviluppo IPAM:

- IPAM che opera nella AWS Regione 1 e AWS nella Regione 2
  - Ambito privato
    - Pool di livello superiore (10.0.0.0/8)
      - Pool regionale nella AWS Regione 1 (10.0.0.0/16)
        - Pool di sviluppo per attività non produttive (10.0.0.0/24) VPCs
          - Allocazione di un VPC (10.0.1.0/25)

Nell'esempio precedente, quelli utilizzati sono solo esempi. CIDRs Essi mostrano che ogni pool all'interno del pool di alto livello è dotato di una parte del CIDR di alto livello.

AWS Management Console

Per creare un pool di sviluppo all'interno di un pool regionale

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli Crea pool.
4. Sotto la voce Pool scegli lo stesso ambito utilizzato al momento della creazione dei pool regionali e di livello superiore. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
5. (Facoltativo) Aggiungi un Tag nome e una descrizione per il pool.
6. In Source (Origine), scegli IPAM pool (Pool IPAM). Quindi scegli il pool regionale.
7. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
8. (Facoltativo) Scegliere un CIDR su cui effettuare il provisioning per il pool. È possibile effettuare il provisioning solo di un CIDR su cui è stato eseguito il provisioning al pool di livello superiore. Puoi creare un pool senza CIDR, ma non sarai in grado di utilizzare il pool per le assegnazioni fino a quando non avrai eseguito il provisioning di un CIDR. È possibile aggiungere qualcosa CIDRs a un pool in qualsiasi momento modificando il pool.
9. Qui hai a disposizione le stesse opzioni delle regole di assegnazione rispetto a quando hai creato il pool regionale di alto livello. Consulta Creare un pool di primo livello IPv4 per una spiegazione delle opzioni disponibili durante la creazione di pool. Le regole di assegnazione per il pool non vengono ereditate dal pool sopra di esso nella gerarchia. Se qui non si applica alcuna regola, non verranno impostate regole di assegnazione per il pool.
10. (Facoltativo) Scegli Tag per il pool.
11. Quando hai finito di configurare il pool, scegli Crea pool.
12. Per informazioni, consulta Allocazione CIDRs da un pool IPAM.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Usa i seguenti AWS CLI comandi per creare un pool regionale nel tuo IPAM:

1. Ottieni l'ID dell'ambito in cui desideri creare il pool: describe-ipam-scopes
2. Ottieni l'ID del pool in cui vuoi creare il pool: describe-ipam-pools
3. Crea il pool: create-ipam-pool
4. Visualizza il nuovo pool: describe-ipam-pools

Ripeti questi passaggi per creare pool di sviluppo aggiuntivi all'interno del pool regionale, secondo necessità.

Crea pool di IPv6 indirizzi nel tuo IPAM

AWS offre IPv6 connettività attraverso molti dei suoi servizi EC2, tra cui VPC e S3, consentendoti di utilizzare lo spazio di indirizzi maggiore e le funzionalità di sicurezza avanzate di. IPv6 IPv6è stato progettato per risolvere questa limitazione fondamentale di. IPv4 Passando a uno spazio di indirizzi a 128 bit, IPv6 offre un gran numero di indirizzi IP unici. Questa massiccia espansione degli indirizzi consente la continua proliferazione di tecnologie connesse, da smartphone e dispositivi IoT all'infrastruttura cloud.

Inoltre, puoi utilizzare IPAM per assicurarti di utilizzare contiguous per la creazione di IPv6 CIDRs VPC. Le allocazioni contigue sono quelle allocate in sequenza CIDRs . CIDRs Consentono di semplificare le regole di sicurezza e di rete; IPv6 CIDRs possono essere aggregate in un'unica voce attraverso costrutti di rete e sicurezza come elenchi di controllo degli accessi, tabelle di routing, gruppi di sicurezza e firewall.

Segui i passaggi in questa sezione per creare una gerarchia di pool IPv6 IPAM. Quando crei il pool, puoi eseguire il provisioning di un CIDR che il pool deve utilizzare. Il pool assegna spazio all'interno di tale CIDR alle allocazioni all'interno del pool. Un'allocazione è un incarico CIDR da un pool IPAM a un'altra risorsa o pool IPAM.

> **Note**
>
> L' IPv6 indirizzamento pubblico e privato è disponibile in. AWS AWS considera gli indirizzi IP pubblici quelli da cui vengono pubblicizzati su Internet AWS, mentre gli indirizzi IP privati non lo sono e non possono essere pubblicizzati su Internet da. AWS Se desideri che le tue reti private supportino IPv6 e non hai intenzione di indirizzare il traffico da questi indirizzi a

Internet, crea il tuo IPv6 pool in un ambito privato. Per ulteriori informazioni sugli IPv6 indirizzi pubblici e privati, consulta IPv6gli indirizzi nella Amazon VPC User Guide.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare con le istruzioni contenute in questa guida. In questa sezione, stai creando una gerarchia di pool IPv6 IPAM:

- IPAM che opera nella AWS Regione 1 e nella Regione 2 AWS
  - Ambito
    - Pool regionale nella AWS Regione 1 (2001:db8: :/52)
      - Pool di sviluppo (2001:db8::/54)
        - Allocazione per un VPC (2001:db8::/56)

Nell'esempio precedente, quelli utilizzati sono solo esempi. CIDRs In particolare, mostrano che il provisioning di ogni pool di sviluppo nel pool regionale è stato eseguito con una parte del CIDR del pool regionale.

Indice

- Crea un pool di IPv6 indirizzi regionali nel tuo IPAM
- Crea un pool di IPv6 indirizzi di sviluppo nel tuo IPAM

Crea un pool di IPv6 indirizzi regionali nel tuo IPAM

Segui i passaggi di questa sezione per creare un pool IPAM IPv6 regionale. Quando esegui il provisioning di un blocco IPv6 CIDR fornito da Amazon in un pool, è necessario assegnarlo a un pool con una locale (AWS Regione) selezionata. Quando crei il pool, puoi eseguire il provisioning di un CIDR per il pool da utilizzare o aggiungerlo in un secondo momento. A questo punto, assegna tale spazio a un'allocazione. Un'allocazione è un'assegnazione CIDR da un pool IPAM a un'altra risorsa o pool IPAM.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare con le istruzioni contenute in questa guida. In questa fase, stai creando il pool IPAM regionale: IPv6

- IPAM che opera nella AWS Regione 1 e AWS nella Regione 2
  - Ambito
    - Pool regionale nella AWS Regione 1 (2001:db8: :/52)

- Pool di sviluppo (2001:db8::/54)
  - Allocazione per un VPC (2001:db8::/56)

Nell'esempio precedente, quelli utilizzati sono solo esempi. CIDRs Illustrano che ogni pool all'interno del pool IPv6 regionale è dotato di una parte del IPv6 CIDR regionale.

Quando crei un pool IPAM, puoi configurare le regole per le allocazioni eseguite nel pool IPAM.

Le regole di assegnazione consentono di configurare quanto segue:

- La lunghezza della netmask richiesta per le assegnazioni all'interno del pool
- I tag richiesti per le risorse all'interno del pool
- La località richiesta per le risorse all'interno del pool. Il locale è la AWS regione in cui è disponibile un pool IPAM per le allocazioni.

Le regole di assegnazione determinano se le risorse sono conformi o non conformi. Per ulteriori informazioni sulla conformità, consulta Monitoraggio dell'utilizzo del CIDR per risorsa.

> **Note**
>
> Esiste una regola implicita aggiuntiva che non viene visualizzata nelle regole di assegnazione. Se la risorsa si trova in un pool IPAM che è una risorsa condivisa in AWS Resource Access Manager (RAM), il proprietario della risorsa deve essere configurato come principale nella AWS RAM. Per ulteriori informazioni sulla condivisione di pool con RAM, consulta Condivisione di un pool IPAM tramite AWS RAM.

L'esempio seguente mostra come utilizzare le regole di assegnazione per controllare l'accesso a un pool IPAM:

Example

Quando crei i pool in base alle esigenze di routing e sicurezza, potresti voler permettere solo a determinate risorse di utilizzare un pool. In questi casi è possibile impostare una regola di assegnazione che indica che qualsiasi risorsa che desidera un CIDR da questo pool deve avere un tag che corrisponda ai requisiti del tag della regola di assegnazione. Ad esempio, è possibile impostare una regola di allocazione che stabilisca che solo VPCs con il tag prod può accedere CIDRs a un pool IPAM.

Note

- Questo argomento spiega come creare un pool IPv6 regionale con un intervallo di IPv6 indirizzi fornito da AWS o con un intervallo privato. IPv6 Se desideri portare i tuoi intervalli di indirizzi pubblici IPv4 o IPv6 IP a AWS (BYOIP), ci sono dei prerequisiti. Per ulteriori informazioni, consulta Tutorial: trasferisci i tuoi indirizzi IP su IPAM.
- Se si crea un IPv6 pool in un ambito privato, è possibile utilizzare un intervallo IPv6 GUA o ULA privato. Per utilizzare un intervallo GUA privato, deve prima essere abilitata l'opzione sull'IPAM (vedi Abilita il provisioning GUA privato IPv6 CIDRs).

AWS Management Console

Per creare un pool

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli Crea pool.
4. Sotto la voce Ambito IPAM, scegli l'ambito pubblico o privato. Se desideri che le tue reti private supportino IPv6 e non hai intenzione di indirizzare il traffico da questi indirizzi a Internet, scegli un ambito privato. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.

   Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default.
5. (Facoltativo) Aggiungi un Tag nome e una descrizione per il pool.
6. In Source (Origine), scegli IPAM scope (Ambito IPAM).
7. Per Famiglia di indirizzi, seleziona IPv6. Se stai creando questo pool a uso pubblico, tutto il pool CIDRs in esso contenuto sarà pubblicizzabile pubblicamente.
8. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
9. Scegli la Locale per il pool. Se desideri effettuare il provisioning di un blocco IPv6 CIDR fornito da Amazon in un pool, devi assegnarlo a un pool con una locale (AWS Regione)

selezionata. La scelta di una località garantisce che non vi siano dipendenze interregionali tra il pool e le risorse da esso assegnate. Le opzioni disponibili provengono dalle regioni operative scelte al momento della creazione dell'IPAM. Puoi aggiungere altre regioni operative in qualunque momento.

La locale è la AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni. Ad esempio, è possibile assegnare un CIDR per un VPC solo da un pool IPAM che condivide una lingua con la Regione del VPC. Tieni presente che dopo aver scelto una lingua per un pool, questa non può essere modificata. Se la regione di origine dell'IPAM non è disponibile a causa di un'interruzione e il pool è in una località differente dalla regione di origine dell'IPAM, il pool può essere ancora utilizzato per assegnare gli indirizzi IP.

> **Note**
>
> Se stai creando un pool nel livello gratuito, puoi scegliere solo la locale corrispondente alla regione di origine del tuo IPAM. Per utilizzare tutte le funzionalità IPAM nelle locale, esegui l'upgrade al livello avanzato.

10. (Facoltativo) Se state creando un IPv6 pool nell'ambito pubblico, in Servizio, scegliete EC2(EIP/VPC). Il servizio selezionato determina il servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione è EC2 (EIP/VPC), il che significa che quanto CIDRs allocato da questo pool sarà pubblicizzabile per il EC2 servizio Amazon (per indirizzi IP elastici) e il servizio Amazon VPC (per associato a). CIDRs VPCs
11. (Facoltativo) Se stai creando un IPv6 pool in ambito pubblico, nell'opzione di origine IP pubblico, scegli Amazon owned per AWS fornire un intervallo di IPv6 indirizzi per questo pool. Come indicato nella parte superiore di questa pagina, questo argomento spiega come creare un pool IPv6 regionale con un intervallo di indirizzi IP fornito da AWS. Se desideri aggiungere il tuo intervallo di IPv6 indirizzi IPv4 o il tuo intervallo di indirizzi a AWS (BYOIP), ci sono dei prerequisiti. Per ulteriori informazioni, consulta Tutorial: trasferisci i tuoi indirizzi IP su IPAM.
12. (Facoltativo) Puoi creare un pool senza CIDR, ma non potrai utilizzare il pool per le allocazioni fino a quando non avrai eseguito il provisioning di un CIDR per tale pool. Per eseguire il provisioning di un CIDR, effettua una delle seguenti operazioni:

    - Se stai creando un IPv6 pool in ambito pubblico con origine IP pubblica di proprietà di Amazon, per effettuare il provisioning di un CIDR, in to provisioning, scegli Aggiungi CIDR di proprietà di Amazon e scegli la dimensione della maschera di rete compresa tra /40 e /52 per il CIDR. CIDRs Quando scegli la lunghezza di una netmask nel menu a discesa,

vedi la lunghezza della netmask e il numero di /56 che la netmask rappresenta. CIDRs Per impostazione predefinita, puoi aggiungere un blocco IPv6 CIDR fornito da Amazon al pool regionale. Per informazioni sull'incremento del limite predefinito, consulta Quote per l'IPAM.

- Se stai creando un IPv6 pool in un ambito privato, puoi utilizzare un intervallo IPv6 GUA o ULA privato:
  - Per dettagli importanti sull' IPv6 indirizzamento privato, IPv6 consulta Indirizzi privati nella Amazon VPC User Guide.
  - Per utilizzare un intervallo IPv6 ULA privato, nella sezione CIDRsDa fornire, scegli Aggiungi ULA CIDR per maschera di rete e scegli la dimensione della maschera di rete oppure scegli Inserisci IPv6 CIDR privato e inserisci un intervallo ULA. Lo spazio IPv6 ULA valido è qualsiasi cosa inferiore a fd00: :/8 che non si sovrappone all'intervallo riservato di Amazon fd00: :/16.
  - Per utilizzare un intervallo IPv6 GUA privato, devi prima aver abilitato l'opzione sul tuo IPAM (vedi). Abilita il provisioning GUA privato IPv6 CIDRs Dopo aver abilitato il IPv6 GUA privato CIDRs, inserisci un IPv6 GUA in Input private IPv6 CIDR.

13. Scegli le regole di assegnazione facoltative per questo pool:

- Lunghezza minima della netmask: la lunghezza minima della netmask richiesta affinché le assegnazioni CIDR in questo pool IPAM siano conformi e il blocco CIDR di dimensioni maggiori che può essere assegnato dal pool. La lunghezza minima della netmask deve essere inferiore alla lunghezza massima della netmask. Le lunghezze possibili delle maschere di rete per IPv6 gli indirizzi sono comprese tra 0 e 128.
- Lunghezza di default della netmask: lunghezza di default della netmask per le assegnazioni aggiunte a questo pool. Ad esempio, se il CIDR di cui è stato eseguito il provisioning in questo pool è `2001:db8::/52` e qui inserisci 56, per tutte le nuove allocazioni in questo pool verrà ripristinata l'impostazione predefinita della lunghezza della maschera di rete /56.
- Lunghezza massima della netmask: la lunghezza massima della netmask richiesta per le assegnazioni CIDR in questo pool. Questo valore determina il blocco CIDR di dimensioni più piccole che può essere assegnato dal pool. Ad esempio, se si immette /56 qui, la lunghezza minima della maschera di rete che può essere allocata da questo pool è /56. CIDRs
- Requisiti per l'assegnazione di tag: i tag necessari alle risorse per assegnare spazio dal pool. Se i tag delle risorse sono stati modificati dopo aver assegnato spazio o se le regole di assegnazione di tag di allocazione vengono modificate nel pool, la risorsa potrebbe essere contrassegnata come non conforme.

- Locale: la versione locale che sarà richiesta per le risorse utilizzate da questo pool. CIDRs Le risorse importate automaticamente che non dispongono di questa località saranno contrassegnate come non conformi. Le risorse che non vengono importate automaticamente nel pool non saranno autorizzate ad assegnare spazio dal pool a meno che non si trovino in questa località.

14. (Facoltativo) Scegli Tag per il pool.
15. Scegli Crea pool.
16. Per informazioni, consulta Crea un pool di IPv6 indirizzi di sviluppo nel tuo IPAM.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Usa i seguenti AWS CLI comandi per creare o modificare un pool IPv6 regionale nel tuo IPAM:

1. Se desideri abilitare il provisioning IPv6 GUA privato CIDRs, modifica l'IPAM con modify-ipam e includi l'opzione to. `enable-private-gua` Per ulteriori informazioni, consulta Abilita il provisioning GUA privato IPv6 CIDRs.
2. Crea un pool con. create-ipam-pool
3. Fornisci un CIDR al pool: provision-ipam-pool-cidr.
4. Modifica il pool dopo averlo creato per modificare le regole di allocazione:. modify-ipam-pool

Crea un pool di IPv6 indirizzi di sviluppo nel tuo IPAM

Segui i passaggi di questa sezione per creare un pool di sviluppo all'interno del tuo pool IPv6 regionale. Se hai bisogno solo di un pool regionale e non ti occorre di pool di sviluppo, passa a Allocazione CIDRs da un pool IPAM.

L'esempio seguente mostra la gerarchia della struttura del pool che è possibile creare con le istruzioni contenute in questa guida. In questa fase stai creando un pool di sviluppo IPAM:

- IPAM che opera nella AWS Regione 1 e AWS nella Regione 2
  - Ambito
    - Pool regionale nella AWS Regione 1 (2001:db8: :/52)

- Pool di sviluppo (2001:db8::/54)
  - Allocazione per un VPC (2001:db8::/56)

Nell'esempio precedente, quelli utilizzati sono solo esempi. CIDRs Essi mostrano che ogni pool all'interno del pool di alto livello è dotato di una parte del CIDR di alto livello.

AWS Management Console

Per creare un pool di sviluppo all'interno di un pool IPv6 regionale

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli Crea pool.
4. Sotto la voce Ambito IPAM, scegliere un ambito. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
5. (Facoltativo) Aggiungi un Tag nome e una descrizione per il pool.
6. In Source (Origine), scegli IPAM pool (Pool IPAM). Quindi, in Source pool, scegli il pool IPv6 regionale.
7. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
8. (Facoltativo) Scegliere un CIDR su cui effettuare il provisioning per il pool. È possibile effettuare il provisioning solo di un CIDR su cui è stato eseguito il provisioning al pool di livello superiore. Puoi creare un pool senza CIDR, ma non sarai in grado di utilizzare il pool per le assegnazioni fino a quando non avrai eseguito il provisioning di un CIDR. Puoi aggiungerlo CIDRs a un pool in qualsiasi momento modificando il pool.
9. Qui hai le stesse opzioni di regole di allocazione che avevi quando hai creato il pool IPv6 regionale. Consulta Crea un pool di IPv6 indirizzi regionali nel tuo IPAM per una spiegazione delle opzioni disponibili durante la creazione di pool. Le regole di assegnazione per il pool non vengono ereditate dal pool sopra di esso nella gerarchia. Se qui non si applica alcuna regola, non verranno impostate regole di assegnazione per il pool.
10. (Facoltativo) Scegli Tag per il pool.
11. Quando hai finito di configurare il pool, scegli Crea pool.
12. Per informazioni, consulta Allocazione CIDRs da un pool IPAM.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Usa i seguenti AWS CLI comandi per creare un pool IPv6 regionale nel tuo IPAM:

1. Ottieni l'ID dell'ambito in cui desideri creare il pool: describe-ipam-scopes
2. Ottieni l'ID del pool in cui vuoi creare il pool: describe-ipam-pools
3. Crea il pool: create-ipam-pool
4. Visualizza il nuovo pool: describe-ipam-pools

Ripeti questi passaggi per creare pool di sviluppo aggiuntivi all'interno del pool IPv6 regionale, se necessario.

Allocazione CIDRs da un pool IPAM

Una funzionalità importante di IPAM è la capacità di assegnare e gestire lo spazio degli indirizzi IP. Quando si crea un VPC, è necessario specificare un blocco CIDR di indirizzi IP, che definisce l'intervallo di indirizzi IP disponibili per quel VPC. IPAM semplifica questo processo fornendo una visione globale dell'intero inventario degli indirizzi IP, aiutandoti ad assegnare e riutilizzare strategicamente i prefissi IP su più prefissi IP. VPCs

Questa assegnazione dello spazio degli indirizzi è fondamentale per garantire che non vi siano intervalli IP sovrapposti, che potrebbero causare conflitti di routing e problemi di connettività. IPAM consente inoltre di riservare lo spazio degli indirizzi IP per le future espansioni del VPC, evitando la necessità di complesse rinumerazioni successive.

Per assegnare un CIDR da un pool IPAM a una risorsa, seguire la procedura descritta in questa sezione.

> **Note**
>
> I termini effettuare il provisioning e assegnare sono utilizzati in questa guida per l'utente e nella console IPAM. Effettuare il provisioning viene utilizzato quando si aggiunge un CIDR a un pool IPAM. Assegnare viene utilizzato quando si associa un CIDR da un pool IPAM a una risorsa.

È possibile effettuare l'allocazione CIDRs da un pool IPAM nei seguenti modi:

- Utilizza un AWS servizio integrato con IPAM, come Amazon VPC, e seleziona l'opzione per utilizzare un pool IPAM per il CIDR. IPAM crea automaticamente l'assegnazione nel pool per te.
- Alloca manualmente un CIDR all'interno di un pool IPAM per riservarlo per un uso successivo con un AWS servizio integrato con IPAM, come Amazon VPC.

Questa sezione illustra entrambe le opzioni: come utilizzare i AWS servizi integrati con IPAM per fornire un pool IPAM CIDR e come prenotare manualmente lo spazio degli indirizzi IP.

Indice

- Creare un VPC che utilizza un CIDR del pool IPAM
- Assegna manualmente un CIDR a un pool per riservare lo spazio degli indirizzi IP

Creare un VPC che utilizza un CIDR del pool IPAM

Con Amazon Virtual Private Cloud (Amazon VPC), puoi avviare AWS risorse in una rete virtuale logicamente isolata che hai definito. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'infrastruttura scalabile di AWS.

Un cloud privato virtuale (VPC) è una rete virtuale dedicata al tuo AWS account. Il VPC è isolato a livello logico dalle altre reti virtuali del cloud AWS . Puoi specificare un intervallo di indirizzi IP per il VPC, aggiungere sottoreti e associare gruppi di sicurezza.

Segui i passaggi descritti in Crea un VPC nella Amazon VPC User Guide. Quando raggiungi la fase di scelta di un CIDR per il VPC, avrai la possibilità di utilizzare un CIDR da un pool IPAM.

Se si sceglie l'opzione di utilizzare un pool IPAM quando si crea il VPC AWS , alloca un CIDR nel pool IPAM. È possibile visualizzare l'assegnazione in IPAM scegliendo un pool nel riquadro dei contenuti della console IPAM e visualizzando la scheda Risorse per il pool.

> **Note**
>
> Per istruzioni complete sull'uso della AWS CLI, inclusa la creazione di un VPC, consulta la sezione. Tutorial per Amazon VPC IP Address Manager

Assegna manualmente un CIDR a un pool per riservare lo spazio degli indirizzi IP

Per assegnare manualmente un CIDR a un pool, segui i passaggi descritti in questa sezione. È possibile fare ciò per prenotare un CIDR all'interno di un pool IPAM ad un uso successivo. È inoltre possibile riservare spazio nel pool IPAM per rappresentare una rete on-premise. IPAM gestirà la prenotazione per te e indicherà eventuali CIDRs sovrapposizioni con lo spazio IP locale.

AWS Management Console

Per allocare manualmente un CIDR

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, selezionare Pool.
3. Per impostazione predefinita è selezionato l'ambito privato di default. Se non si desidera utilizzare l'ambito privato di default, scegliere l'ambito che si desidera utilizzare dal menu a tendina nella parte superiore del riquadro dei contenuti. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Nel riquadro dei contenuti, seleziona un pool.
5. Scegli Actions (Operazioni) > Create custom allocation (Crea allocazione personalizzata).
6. Scegli se aggiungere un CIDR specifico da allocare (ad esempio, per IPv4 o `10.0.0.0/24` `2001:db8::/52` per IPv6) o aggiungere un CIDR in base alla dimensione scegliendo solo la lunghezza della maschera di rete (ad esempio, `/24` per o per). IPv4 `/52` IPv6
7. Scegli Alloca.
8. È possibile visualizzare l'assegnazione in IPAM selezionando Pool nel pannello di navigazione, scegliendo un pool e visualizzando la scheda Assegnazioni per il pool.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per allocare manualmente un CIDR a un pool:

1. Ottieni l'ID del pool IPAM in cui desideri creare l'allocazione:. describe-ipam-pools

2. Crea l'allocazione:. allocate-ipam-pool-cidr
3. Visualizza l'allocazione:. get-ipam-pool-allocations

Per rilasciare un CIDR assegnato manualmente, consulta Rilasciare un'assegnazione.

Gestione dello spazio degli indirizzi IP in IPAM

Le attività in questa sezione sono facoltative. Ricorda che questa sezione è un raggruppamento di procedure tutte relative all'utilizzo di IPAM. Le procedure sono elencate in ordine alfabetico.

Se si desidera completare le attività in questa sezione e si è delegato un account IPAM, le attività dovranno essere completate dall'amministratore IPAM.

Segui i passaggi riportati in questa sezione per gestire lo spazio degli indirizzi IP in IPAM.

Indice

- Modifica lo stato di monitoraggio del VPC CIDRs
- Crea ambiti aggiuntivi
- Elimina un IPAM
- Elimina un pool
- Elimina un ambito
- Deapprovvigionamento CIDRs da un pool
- Modifica un pool IPAM
- Abilita la distribuzione dei costi
- Abilita il provisioning GUA privato IPv6 CIDRs
- Implementa l'uso di IPAM per la creazione di VPC con SCPs
- Escludi unità organizzative da IPAM
- Modifica un livello IPAM
- Modifica le regioni operative IPAM
- Fornitura CIDRs a un pool
- Sposta il VPC CIDRs tra gli ambiti
- Rilasciare un'assegnazione
- Condivisione di un pool IPAM tramite AWS RAM
- Lavora con il rilevamento delle risorse

Modifica lo stato di monitoraggio del VPC CIDRs

Per modificare lo stato di monitoraggio di un CIDR VPC, segui la procedura descritta in questa sezione. Puoi modificare un CIDR VPC dallo stato Monitorato a Ignorato, se non vuoi che IPAM gestisca o controlli la risorsa e consenta al CIDR assegnato al VPC di essere disponibile per l'uso. È possibile modificare un CIDR VPC dallo stato Ignorato a Monitorato se desideri che IPAM gestisca e monitori il CIDR VPC.

> **Note**
>
> - Non puoi ignorare il VPC CIDRs nell'ambito pubblico.
> - Se un CIDR viene ignorato, ti verranno comunque addebitati gli indirizzi IP attivi nel CIDR. Per ulteriori informazioni, consulta Prezzi per IPAM.
> - Se un CIDR viene ignorato, sarà comunque possibile visualizzare la cronologia degli indirizzi IP nel CIDR. Per ulteriori informazioni, consulta Visualizzazione della cronologia degli indirizzi IP.

È possibile modificare lo stato di monitoraggio di un CIDR VPC su Monitorato o Ignorato:

- Monitorato: il VPC CIDR è stato rilevato da IPAM e viene monitorato per verificare la sovrapposizione con altre CIDRs regole di allocazione.
- Ignorato: il CIDR VPC è stato scelto per non essere incluso nel monitoraggio. I CIDRs VPC ignorati non vengono valutati per verificarne la sovrapposizione con CIDRs altri sistemi o con la conformità alle regole di allocazione. Una volta che un CIDR VPC viene scelto per essere ignorato, qualsiasi spazio assegnato da un pool IPAM viene restituito al pool e la risorsa non verrà di nuovo importata tramite l'importazione automatica (se la regola di assegnazione dell'importazione automatica è impostata sul pool).

AWS Management Console

Modifica dello stato di monitoraggio di un CIDR assegnato a un VPC

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di spostamento seleziona Resources (Risorse).

3. Dal menu a discesa nella parte superiore del pannello dei contenuti, scegli l'ambito privato che desideri utilizzare.
4. Nel riquadro dei contenuti, scegli il VPC e visualizzane i dettagli.
5. In VPC CIDRs, seleziona uno dei file CIDRs allocati al VPC e scegli Azioni > Contrassegna come ignorato o Deseleziona come ignorato.
6. Scegli Contrassegna come ignorato o Non contrassegnare come ignorato.

Command line

Utilizza i seguenti AWS CLI comandi per modificare lo stato di monitoraggio di un VPC CIDR:

1. Ottieni un ID di ambito: describe-ipam-scopes
2. Visualizza lo stato di monitoraggio corrente per il VPC CIDR: get-ipam-resource-cidrs
3. Cambia lo stato del VPC CIDR: modify-ipam-resource-cidr
4. Visualizza il nuovo stato di monitoraggio per il VPC CIDR: get-ipam-resource-cidrs

Crea ambiti aggiuntivi

Per creare un ambito aggiuntivo, segui le fasi descritte in questa sezione.

Un ambito è il container di più alto livello all'interno di IPAM. Quando crei un IPAM, verranno creati due ambiti di default per te. Ogni ambito rappresenta lo spazio IP per una singola rete. L'ambito privato è destinato a tutti gli spazi privati. L'ambito pubblico è destinato a tutti gli spazi pubblici. Gli ambiti consentono di riutilizzare gli indirizzi IP su più reti non connesse senza causare sovrapposizioni o conflitti di indirizzi IP.

Quando crei un IPAM, vengono creati ambiti di default (uno privato e uno pubblico). È possibile creare ambiti privati aggiuntivi. Non è possibile creare ambiti pubblici aggiuntivi.

È possibile creare ambiti privati aggiuntivi se si richiede il supporto per più reti private disconnesse. Ambiti privati aggiuntivi permettono di creare pool e gestire risorse che utilizzano lo stesso spazio IP.

> **Important**
>
> Se IPAM rileva risorse private IPv4 o private IPv6 CIDRs, le risorse CIDRs vengono importate nell'ambito privato predefinito e non vengono visualizzate in nessun ambito privato aggiuntivo

creato. È possibile passare CIDRs dall'ambito privato predefinito a un altro ambito privato. Per informazioni, consultare Sposta il VPC CIDRs tra gli ambiti.

AWS Management Console

Per creare un ulteriore ambito privato

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, scegliere Ambiti.
3. Scegli Crea ambito.
4. Scegliere l'IPAM a cui si desidera aggiungere l'ambito.
5. Aggiungi una descrizione per l'ambito.
6. Scegli Crea ambito.
7. È possibile visualizzare l'ambito in IPAM scegliendo Ambiti nel pannello di navigazione.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per creare un ambito privato aggiuntivo:

1. Visualizza gli ambiti attuali: describe-ipam-scopes
2. Crea un nuovo ambito privato: create-ipam-scope
3. Visualizza gli ambiti attuali per visualizzare il nuovo ambito: describe-ipam-scopes

Elimina un IPAM

È possibile eliminare un IPAM se non è più necessario, se è necessario rivedere la gestione degli indirizzi IP o se si desidera ricominciare da capo con una nuova configurazione IPAM. L'eliminazione di un IPAM può contribuire a semplificare la gestione degli indirizzi IP e ad allinearsi con i requisiti aziendali oppure operativi in continua evoluzione.

Per eliminare un IPAM, segui i passaggi descritti in questa sezione. Per informazioni su come aumentare il numero predefinito IPAMs di dati disponibili anziché eliminare un IPAM esistente, vedere. Quote per l'IPAM

> **Note**
>
> L'eliminazione di un IPAM rimuove tutti i dati monitorati associati all'IPAM, inclusi i dati storici di. CIDRs

AWS Management Console

Per eliminare un IPAM

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, scegli IPAMs.
3. Nel riquadro dei contenuti, seleziona il tuo IPAM.
4. Seleziona Azioni > Elimina IPAM.
5. Esegui una di queste operazioni:

   - Scegli Cascade delete (Elimina a cascata) per eliminare l'IPAM, gli ambiti privati, i pool negli ambiti privati e le allocazioni nei pool negli ambiti privati. Se è presente un pool nell'ambito pubblico, con questa opzione non è possibile eliminare l'IPAM. Se utilizzi questa opzione, l'IPAM effettua le seguenti operazioni:
     - Dealloca tutte le risorse CIDRs allocate a VPC (ad esempio VPCs) nei pool in ambiti privati.

       > **Note**
       >
       > Nessuna risorsa VPC viene eliminata a seguito dell'abilitazione di questa opzione. Il CIDR associato alla risorsa non sarà più allocato da un pool IPAM, ma il CIDR stesso rimarrà invariato.

     - Annulla il IPv4 CIDRs provisioning di tutti i pool IPAM in ambiti privati.
     - Elimina tutti i pool IPAM negli ambiti privati.
     - Elimina tutti gli ambiti privati non predefiniti nell'IPAM.
     - Elimina gli ambiti pubblici e privati predefiniti e l'IPAM.

- Se non selezioni la casella di controllo Cascade delete (Elimina a cascata), prima di eliminare un IPAM devi eseguire le seguenti operazioni:
  - Rilasciare le assegnazioni all'interno dei pool IPAM. Per ulteriori informazioni, consulta Rilasciare un'assegnazione.
  - CIDRs Deprovisioning fornito ai pool all'interno dell'IPAM. Per ulteriori informazioni, consulta Deapprovvigionamento CIDRs da un pool.
  - Eliminare eventuali ambiti aggiuntivi non di default. Per ulteriori informazioni, consulta Elimina un ambito.
  - Eliminare i pool IPAM. Per ulteriori informazioni, consulta Elimina un pool.

6. Immetti **`delete`**, quindi scegli Elimina.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per eliminare un IPAM:

1. Visualizza corrente IPAMs: describe-ipams
2. Elimina un IPAM: delete-ipam
3. Visualizza il tuo aggiornamento: describe-ipams IPAMs

Per creare un nuovo IPAM, consulta Crea un IPAM.

Elimina un pool

Un pool IPAM AWS rappresenta un intervallo definito di indirizzi IP che possono essere allocati e gestiti all'interno di un AWS ambiente o di un'organizzazione specifici. I pool vengono utilizzati per organizzare lo spazio degli indirizzi IP, per consentirne la gestione automatizzata e per applicare le policy di governance degli indirizzi IP nell'infrastruttura cloud.

Potresti voler eliminare un pool IPAM per rimuovere lo spazio degli indirizzi IP inutilizzato o non necessario e recuperarlo per altri scopi. Non è possibile eliminare un pool di indirizzi IP se vi sono assegnazioni. È necessario rilasciare le assegnazioni e Deapprovvigionamento CIDRs da un pool prima di poter eliminare il pool.

Per eliminare un pool IPAM, segui i passaggi descritti in questa sezione.

AWS Management Console

Per eliminare un pool

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Dal menu a tendina nella parte superiore del riquadro dei contenuti, scegliere l'ambito che si desidera utilizzare. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Nel riquadro dei contenuti, scegliere il pool di cui si desidera eliminare il CIDR.
5. Seleziona Azioni > Elimina pool.
6. Immetti **`delete`**, quindi scegli Elimina.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per eliminare un pool:

1. Visualizza i pool e ottieni un ID del pool IPAM: describe-ipam-pools
2. Eliminare un pool: delete-ipam-pool
3. Visualizza i tuoi pool: describe-ipam-pools

Per creare un nuovo pool, consulta Creare un pool di primo livello IPv4 .

Elimina un ambito

È possibile eliminare un ambito IPAM se non serve più allo scopo previsto, ad esempio quando si ristruttura la rete, si consolidano le regioni o si modifica l'assegnazione degli indirizzi IP. L'eliminazione degli ambiti non utilizzati può aiutare a semplificare la configurazione IPAM e ottimizzare la gestione degli indirizzi IP in AWS.

> **Note**
>
> Non è possibile eliminare un ambito se si verifica una delle seguenti condizioni:
>
> - L'ambito è un ambito di default. Quando crei un IPAM, due ambiti di default (uno pubblico e uno privato) vengono creati automaticamente e non possono essere eliminati. Per vedere se un ambito è quello di default, visualizza il Tipo di ambito nei dettagli dell'ambito.
> - Ci sono uno o più pool nell'ambito. Bisogna anzitutto Elimina un pool prima di poter eliminare l'ambito.

AWS Management Console

Per eliminare un ambito

1. Aprire la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, seleziona Ambiti.
3. Nel riquadro dei contenuti, scegli l'ambito che desideri eliminare.
4. Seleziona Azioni > Elimina ambito.
5. Inserisci **`delete`**, quindi scegli Elimina.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per eliminare un ambito:

1. Visualizza gli ambiti: describe-ipam-scopes
2. Eliminare un ambito: delete-ipam-scope
3. Visualizza gli ambiti aggiornati: describe-ipam-scopes

Per creare un nuovo ambito, consulta Crea ambiti aggiuntivi. Per eliminare l'IPAM, consulta Elimina un IPAM.

Deapprovvigionamento CIDRs da un pool

È possibile eseguire il deprovisioning del CIDR di un pool per liberare spazio degli indirizzi IP, semplificare la gestione degli indirizzi IP, prepararsi alle modifiche di rete o soddisfare i requisiti di conformità. Il deprovisioning del CIDR di un pool consente un migliore controllo e una migliore ottimizzazione delle assegnazioni degli indirizzi IP all'interno di IPAM, permettendo così di recuperare lo spazio IP inutilizzato e di riutilizzarlo in futuro. Non è possibile eseguire il deprovisioning del CIDR se sono presenti assegnazioni nel pool. Per rimuovere le assegnazioni, consulta the section called “Rilasciare un'assegnazione”.

Segui i passaggi descritti in questa sezione per eseguire il deprovisioning CIDRs da un pool IPAM. Quando si esegue il deprovisioning di tutto il pool CIDRs, il pool non può più essere utilizzato per le allocazioni. È necessario innanzitutto effettuare il provisioning di un nuovo CIDR nel pool prima di poter utilizzare il pool per le assegnazioni.

AWS Management Console

Per revocare un CIDR del pool

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Dal menu a tendina nella parte superiore del riquadro dei contenuti, scegliere l'ambito che si desidera utilizzare. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Nel riquadro dei contenuti, scegliete il pool di cui CIDRs desiderate effettuare il deprovisioning.
5. Scegliere la scheda CIDRs.
6. Selezionane uno o più CIDRs e scegli CIDRsDeprovisioning.
7. Scegli Revoca CIDR.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Usa i seguenti AWS CLI comandi per eseguire il deprovisioning di un pool CIDR:

1. Ottieni un ID del pool IPAM: describe-ipam-pools

2. Visualizza la tua corrente CIDRs per il pool: get-ipam-pool-cidrs
3. Deprovisioning CIDRs: deprovision-ipam-pool-cidr
4. Visualizza i tuoi aggiornamenti: CIDRs get-ipam-pool-cidrs

Per effettuare il provisioning di un nuovo CIDR nel pool, consulta Deapprovvigionamento CIDRs da un pool. Se desideri eliminare il pool, consulta Elimina un pool.

Modifica un pool IPAM

È possibile modificare un pool eseguendo una delle seguenti operazioni:

- Modifica le regole di assegnazione per il pool. Per ulteriori informazioni sulle regole di assegnazione, consulta Creare un pool di primo livello IPv4 .
- Modifica il nome, la descrizione o altri metadati del pool per migliorare l'organizzazione e la visibilità all'interno di IPAM.
- Modifica le opzioni del pool, come l'importazione automatica delle risorse scoperte, per ottimizzare la gestione automatizzata degli indirizzi IP di IPAM.

Per modificare un pool IPAM, segui i passaggi riportati in questa sezione.

AWS Management Console

Per modificare un pool

1. Aprire la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, selezionare Pool.
3. Per impostazione predefinita è selezionato l'ambito privato di default. Se non si desidera utilizzare l'ambito privato di default, scegliere l'ambito che si desidera utilizzare dal menu a tendina nella parte superiore del riquadro dei contenuti. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM
4. Nel riquadro dei contenuti, scegliere il pool di cui si desidera modificare il CIDR.
5. Scegli Operazioni > Modifica.
6. Apportare tutte le modifiche di cui si ha bisogno ai pool. Per ulteriori informazioni sulle opzioni di configurazione del pool, consulta Creare un pool di primo livello IPv4 .
7. Scegli Aggiorna.

Command line

Utilizzate i seguenti AWS CLI comandi per modificare un pool:

1. Ottieni un ID del pool IPAM: describe-ipam-pools
2. Modifica il pool: modify-ipam-pool

Abilita la distribuzione dei costi

Quando si abilita la distribuzione dei costi, si distribuiscono gli addebiti per gli indirizzi IP attivi agli account che utilizzano gli indirizzi IP anziché al proprietario IPAM. Ciò è utile per le grandi organizzazioni in cui l'amministratore IPAM delegato gestisce gli indirizzi IP a livello centrale utilizzando IPAM e ogni account è responsabile del proprio utilizzo, eliminando la necessità di calcoli di fatturazione manuali.

L'opzione di distribuzione dei costi è disponibile quando si crea un IPAM o si modifica un IPAM in modalità Metering, dove:

- Proprietario IPAM (impostazione predefinita): all' AWS account proprietario dell'IPAM vengono addebitati tutti gli indirizzi IP attivi gestiti in IPAM.
- Proprietario della risorsa: all' AWS account che possiede l'indirizzo IP viene addebitato l'indirizzo IP attivo.

Requisiti

- Il tuo IPAM deve essere integrato con AWS Organizations.
- L'IPAM deve essere stato creato dall'amministratore IPAM delegato dell'organizzazione. AWS
- La regione di origine dell'IPAM deve essere una regione abilitata per impostazione predefinita. Non può essere una regione che accetta l'iscrizione.

Come funziona la ricarica

- Anche se è possibile distribuire i costi relativi agli indirizzi IP all'interno di un'organizzazione, tutti gli addebiti IPAM vengono consolidati sul conto pagante dell'organizzazione tramite AWS Organizations consolidated billing.

- Quando la distribuzione dei costi è abilitata, gli account dei membri dell'organizzazione possono comunque visualizzare l'utilizzo e gli addebiti individuali dell'IPAM nelle fatture dei rispettivi account.
- L'ARN IPAM verrà visualizzato nelle fatture dei singoli account quando è abilitata la distribuzione dei costi, il che consente ai proprietari delle risorse di tenere traccia dell'utilizzo dell'IP attivo IPAM. Se si utilizza Esportazioni di dati AWS, gli addebiti IPAM vengono visualizzati con l'ARN IPAM associato nelle fatture dei conti consolidate e individuali.
- Solo gli account all'interno dell'organizzazione dell'amministratore delegato possono ricevere addebiti per le risorse di cui sono proprietari. I costi degli indirizzi IP esterni all'organizzazione vengono addebitati al proprietario dell'IPAM.

Restrizioni temporali

- Hai 24 ore di tempo per annullare l'iscrizione dopo aver abilitato la distribuzione dei costi. Dopo 24 ore, non è possibile modificare l'impostazione per 7 giorni. Dopo 7 giorni, è possibile disattivare la distribuzione dei costi.

Abilita il provisioning GUA privato IPv6 CIDRs

Se desideri che le tue reti private supportino IPv6 e non hai intenzione di indirizzare il traffico da questi indirizzi a Internet, puoi fornire un intervallo IPv6 ULA o GUA privato a un pool IPAM in ambito privato.

Per dettagli importanti sull' IPv6 indirizzamento privato, IPv6 consulta Indirizzi privati nella Amazon VPC User Guide.

Esistono due tipi di IPv6 indirizzi privati:

- IPv6 Intervalli ULA: IPv6 indirizzi come definiti in RFC4193. Questi intervalli di indirizzi iniziano sempre con “fc” o “fd”, il che li rende facilmente identificabili. Lo spazio IPv6 ULA valido è qualsiasi cosa inferiore a fd00: :/8 che non si sovrappone all'intervallo riservato di Amazon fd00: :/16.
- IPv6 Intervalli GUA: indirizzi come definiti in. IPv6 RFC3587 L'opzione per utilizzare gli intervalli IPv6 GUA come IPv6 indirizzi privati è disabilitata per impostazione predefinita e deve essere abilitata prima di poterla utilizzare.

Per utilizzare gli intervalli di indirizzi IPv6 ULA, si sceglie l' IPv6 opzione quando si fornisce un CIDR a un pool IPAM e si inserisce l'intervallo IPv6 ULA. Per utilizzare i propri intervalli IPv6 GUA come IPv6 indirizzi privati, tuttavia, è necessario prima completare i passaggi descritti in questa sezione. Per impostazione predefinita, l'opzione è disabilitata.

> **Note**
>
> - Quando utilizzi intervalli IPv6 GUA privati, richiediamo che tu utilizzi intervalli IPv6 GUA di tua proprietà.
> - IPAM rileva risorse con indirizzi IPv6 ULA e GUA e monitora i pool per individuare la sovrapposizione degli spazi di indirizzi IPv6 ULA e GUA.
> - Se desideri connetterti a Internet da una risorsa con un IPv6 indirizzo privato, puoi farlo, ma per farlo devi indirizzare il traffico attraverso una risorsa in un'altra sottorete con un indirizzo pubblico. IPv6
> - Se disponi di un intervallo IPv6 GUA privato assegnato a un VPC, non puoi utilizzare uno spazio GUA IPv6 pubblico che si sovrappone allo spazio GUA IPv6 privato nello stesso VPC.
> - È supportata la comunicazione tra risorse con intervalli di indirizzi IPv6 ULA e GUA privati (ad esempio tramite Direct Connect). Peering VPC, gateway di transito o connessioni VPN).
> - Un IPv6 intervallo GUA privato non può essere convertito in un intervallo GUA pubblicizzato pubblicamente IPv6 .

AWS Management Console

Per abilitare il provisioning di GUA privati IPv6 CIDRs

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, scegli IPAMs.
3. Scegli l'IPAM e seleziona Operazioni > Modifica.
4. In IPv6 GUA privato CIDRs, scegli Abilita il provisioning dello spazio GUA CIDR in pool IPAM privati IPv6 .
5. Scegli Save changes (Salva modifiche).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per abilitare il provisioning di GUA privati IPv6 : CIDRs

1. Visualizza la corrente IPAMs con describe-ipams
2. Modifica l'IPAM con modify-ipam e includi l'opzione per `enable-private-gua`.

Una volta abilitata l'opzione per il provisioning di un IPv6 GUA privato CIDRs, è possibile fornire un IPv6 GUA CIDR privato a un pool. Per ulteriori informazioni, consulta Fornitura CIDRs a un pool.

Implementa l'uso di IPAM per la creazione di VPC con SCPs

> **Note**
>
> Questa sezione è applicabile solo se hai abilitato l'integrazione con IPAM. AWS Organizations Per ulteriori informazioni, consulta Integrare IPAM con gli account di un'organizzazione AWS.

Questa sezione descrive come creare una politica di controllo del servizio AWS Organizations che richieda ai membri dell'organizzazione di utilizzare IPAM quando creano un VPC. Le politiche di controllo del servizio (SCPs) sono un tipo di politica organizzativa che consente di gestire le autorizzazioni all'interno dell'organizzazione. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

Applica l'IPAM durante la creazione VPCs

Segui i passaggi di questa sezione per richiedere ai membri della tua organizzazione di utilizzare IPAM durante la creazione. VPCs

Per creare una SCP e limitare la creazione di VPC a IPAM

1. Segui i passaggi descritti in Creare una politica di controllo del servizio nella Guida per l'AWS Organizations utente e inserisci il seguente testo nell'editor JSON:

JSON

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

2. Allega la policy a una o più unità organizzative della tua organizzazione. Per ulteriori informazioni, consulta Allega policy e Detach policies nella Guida per l'AWS Organizations utente.

Applica un pool IPAM durante la creazione VPCs

Segui i passaggi di questa sezione per richiedere ai membri dell'organizzazione di utilizzare un pool IPAM specifico durante la creazione. VPCs

Per creare un SCP e limitare la creazione di VPC a un pool IPAM

1. Segui i passaggi descritti in Creare una politica di controllo del servizio nella Guida per l'AWS Organizations utente e inserisci il seguente testo nell'editor JSON:

   JSON

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

```
            "StringNotEquals": {
                "ec2:Ipv4IpamPoolId": "ipam-pool-0123456789abcdefg"
            }
          }
    }]
}
```

2. Cambia il valore di `ipam-pool-0123456789abcdefg` esempio IPv4 con l'ID del pool a cui desideri limitare gli utenti.
3. Allega la policy a una o più unità organizzative della tua organizzazione. Per ulteriori informazioni, consulta Allach policies e Detach Policies nella Guida per l'AWS Organizations utente.

Applica l'IPAM per tutti tranne un determinato elenco di OUs

Segui i passaggi di questa sezione per applicare l'IPAM a tutte le unità organizzative tranne un determinato elenco (). OUs La politica descritta in questa sezione è obbligatoria all' OUs interno dell'organizzazione, ad eccezione di OUs quella specificata in per l'utilizzo di IPAM `aws:PrincipalOrgPaths` per la creazione e l'espansione. VPCs Gli elencati OUs possono utilizzare IPAM durante la creazione VPCs o specificare manualmente un intervallo di indirizzi IP.

Per creare un SCP e applicare l'IPAM per tutti tranne un determinato elenco di OUs

1. Segui i passaggi descritti in Creare una politica di controllo del servizio nella Guida per l'AWS Organizations utente e inserisci il seguente testo nell'editor JSON:

   JSON

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

```
                "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/",
                "o-a1b2c3d4e5/r-ab12/ou-ab13-22222222/ou-ab13-33333333/"
            ]
          }
        }
    }]
}
```

2. Rimuovi i valori di esempio (come`o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/`) e aggiungi i percorsi delle entità AWS Organizations di OUs cui desideri avere l'opzione (ma non obbligatoria) di utilizzare IPAM. Per ulteriori informazioni sul percorso dell'entità, consulta Understand the AWS Organizations entity path e aws: PrincipalOrgPaths nella IAM User Guide.
3. Collega la policy alla root dell'organizzazione. Per ulteriori informazioni, consulta Allach policies e Detach policies nella AWS Organizations User Guide.

Escludi unità organizzative da IPAM

Se il tuo IPAM è integrato con AWS Organizations, puoi escludere un'unità organizzativa (OU) dalla gestione da parte di IPAM. Quando si esclude un'unità organizzativa, IPAM non gestirà gli indirizzi IP negli account di quell'unità organizzativa. Questa funzionalità offre una maggiore flessibilità nella modalità di utilizzo di IPAM.

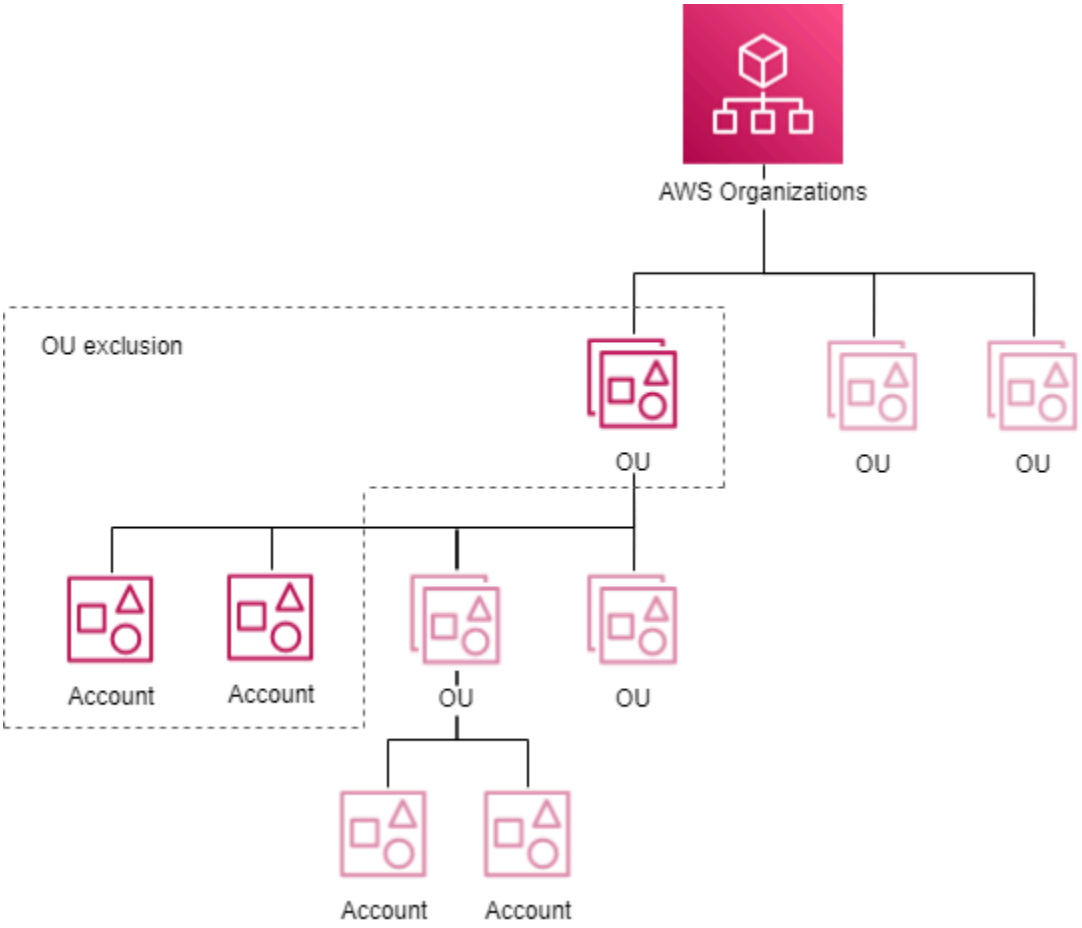
Puoi utilizzare le esclusioni delle unità organizzative nei seguenti modi:

- Abilita IPAM per parti specifiche dell'attività: se hai più unità aziendali o filiali in AWS Organizations, ora puoi utilizzare IPAM solo per quelle che ne hanno bisogno.
- Tieni separati gli account sandbox: puoi escludere gli account sandbox da IPAM concentrandoti solo su quelli realmente importanti per la gestione della proprietà intellettuale.

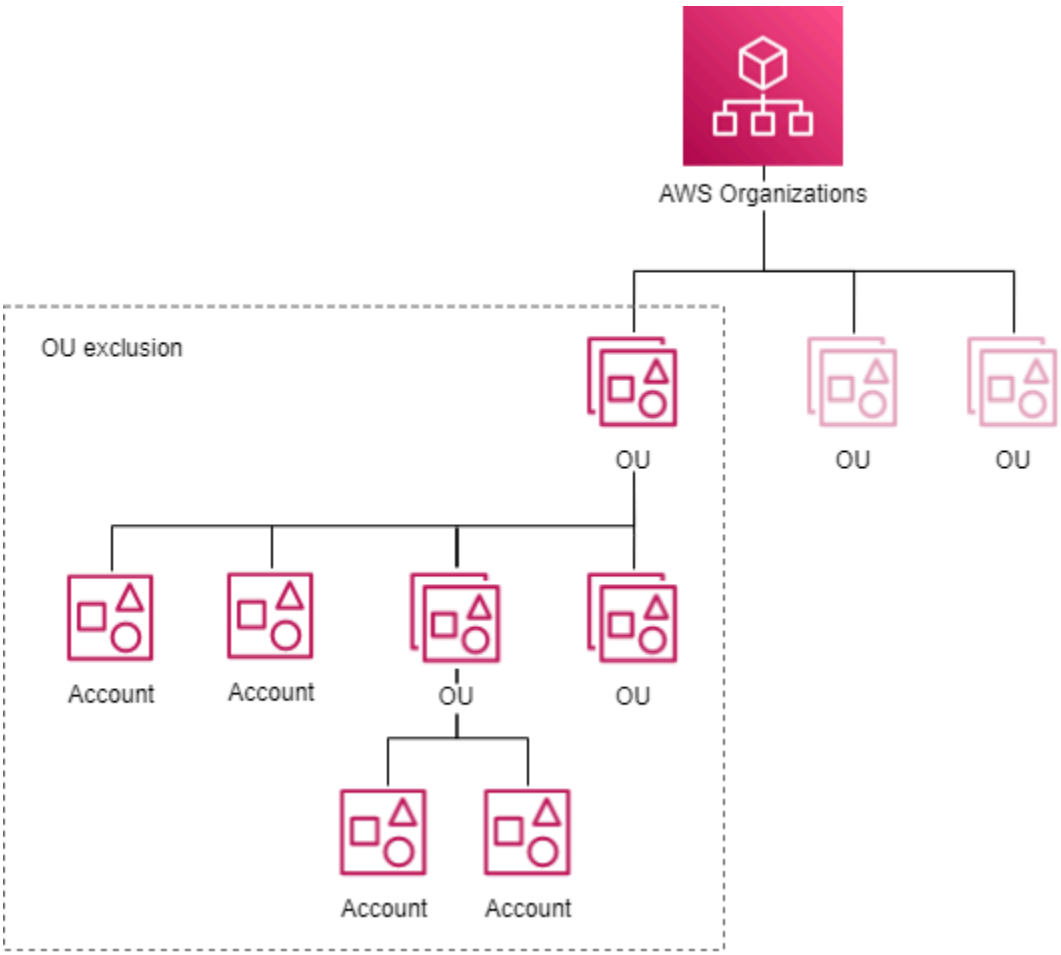
Come funzionano le esclusioni delle unità organizzative

I diagrammi di questa sezione mostrano due casi d'uso per aggiungere esclusioni di unità organizzative in IPAM.

Il primo diagramma mostra l'impatto dell'aggiunta di un'esclusione solo su un'unità organizzativa principale. In questo caso, IPAM non gestirà gli indirizzi IP negli account dell'unità organizzativa principale. IPAM gestirà gli indirizzi IP degli account degli altri account al di fuori dell'esclusione. OUs



Il secondo diagramma mostra l'impatto dell'aggiunta dell'esclusione di un'unità organizzativa (OU) su un'unità organizzativa principale e su tutti i figli. OUs Di conseguenza, IPAM non gestirà gli indirizzi IP negli account dell'unità organizzativa principale o negli account di alcun figlio. OUs IPAM gestirà gli indirizzi IP negli account OUs al di fuori dell'esclusione.



Aggiungi o rimuovi esclusioni di unità organizzative

Completa i passaggi descritti in questa sezione per aggiungere o rimuovere esclusioni delle unità organizzative.

> **Note**
>
> - L'account amministratore IPAM delegato non è escluso neanche se si trova all'interno di un'unità organizzativa esclusa.
> - L'IPAM deve essere integrato con AWS Organizations per aggiungere un'esclusione dell'unità organizzativa. L'organizzazione deve averla OUs dentro.
> - È necessario essere l'amministratore IPAM delegato per poter visualizzare, aggiungere o rimuovere le esclusioni delle unità organizzative.
> - IPAM impiega tempo per scoprire le unità organizzative create di recente.

- Esiste una quota predefinita per il numero di esclusioni che puoi aggiungere per ogni rilevamento di risorse. Per ulteriori informazioni, vedi Esclusioni di unità organizzative per rilevamento di risorse in Quote per l'IPAM.
- Se si condivide l'individuazione di una risorsa con un altro account, tale account può visualizzare le esclusioni dell'unità organizzativa su tale account, che contiene informazioni come l'ID di organizzazione, l'ID radice e l'unità organizzativa IDs dell'organizzazione del proprietario della risorsa.

AWS Management Console

Per aggiungere o rimuovere esclusioni delle unità organizzative

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di navigazione, scegli Rilevamenti delle risorse.
3. Scegli il rilevamento di risorse predefinito.
4. Scegli Modifica.
5. Alla voce Esclusioni di unità organizzative, procedi come segue:
   - Per aggiungere l'esclusione di un'unità organizzativa:
     - Se si desidera escludere l'unità organizzativa e tutti i relativi elementi OUs secondari:
       - Trova l'unità organizzativa nella tabella e seleziona la casella di controllo. Tutti i figli OUs vengono selezionati automaticamente.
     - Se desideri escludere solo gli account delle unità organizzative principali:
       - Trova l'unità organizzativa nella tabella e seleziona la casella di controllo. Tutti i bambini OUs vengono selezionati automaticamente. Deseleziona tutti i bambini OUs.
     - In alternativa, puoi utilizzare la colonna Azioni per selezionare solo un'unità organizzativa principale o un genitore e un figlio OUs:
       - Seleziona tutto il figlio OUs: includi qualsiasi bambino OUs nell'esclusione. Dopo aver scelto un'unità organizzativa, questa viene aggiunta sullo schermo. Ogni unità organizzativa contiene l'ID e il percorso entità della sua esclusione.
       - Seleziona solo questa unità organizzativa: inserisci solo questa unità nell'esclusione. Dopo aver scelto un'unità organizzativa, questa viene aggiunta sullo schermo. Ogni unità organizzativa contiene l'ID e il percorso entità della sua esclusione.

- Copia il percorso dell'entità OU: copia il percorso dell' AWS Organizations entità da utilizzare secondo necessità.

- Se conosci già il percorso dell'entità AWS Organizations o desideri crearlo:
  - Scegli Inserisci esclusione dell'unità organizzativa e inserisci il percorso entità per tale esclusione. Crea il percorso per le unità organizzative utilizzando AWS Organizzazioni IDs separate da a/. Includi tutti i bambini OUs terminando il percorso con/*.
    - Esempio 1
      - Percorso per un'unità organizzativa secondaria: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
      - In questo esempio, `o-a1b2c3d4e5` è l'ID dell'organizzazione, `r-f6g7h8i9j0example` è l'ID radice, `ou-ghi0-awsccccc` è un ID OU ed `ou-jkl0-awsddddd` è un ID OU figlio.
      - IPAM non gestirà gli indirizzi IP negli account dell'unità organizzativa secondaria.
    - Esempio 2
      - Percorso in cui tutti i bambini OUs faranno parte dell'esclusione: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
      - In questo esempio, IPAM non gestirà gli indirizzi IP negli account dell'unità organizzativa (`ou-ghi0-awsccccc`) o negli account di altri OUs che sono figli dell'unità organizzativa.
  - Per rimuovere l'esclusione di un'unità organizzativa:
    - Seleziona X accanto a un'unità organizzativa già aggiunta. L'ID /* successivo all'unità organizzativa indica che si tratta di un'unità organizzativa principale e che il figlio fa OUs parte dell'esclusione dell'unità organizzativa.

6. Scegli Save changes (Salva modifiche).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

1. Visualizza i dettagli relativi all'individuazione delle risorse per ottenere l'ID dell'individuazione delle risorse predefinita per la fase successiva. describe-ipam-resource-discoveries

   Input:

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

Output:

```
{

    "IpamResourceDiscoveries": [

        {

            "OwnerId": "111122223333",

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

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

            "OperatingRegions": [

                {

                    "RegionName": "us-east-1"

                },

                {

                    "RegionName": "us-west-1"

                },

                {

                    "RegionName": "us-west-2"

                }

            ],

            "IsDefault": true,
```

```
            "State": "modify-complete",

            "Tags": []

        }

    ]

}
```

2. Aggiungi o rimuovi l'esclusione di un'unità organizzativa dall'individuazione di risorse con modify-ipam-resource-discoverye le `--remove-organizational-unit-exclusions` opzioni `--add-organizational-unit-exclusions` or. Dovrai inserire un percorso dell'entità AWS Organizations. Crea il percorso per le unità organizzative utilizzando AWS Organizzazioni IDs separate da a`/`. Includi tutti i bambini OUs terminando il percorso con`/*`. Non puoi includere lo stesso percorso dell'entità più di una volta nei parametri di aggiunta o rimozione.

   - Esempio 1
     - Percorso per un'unità organizzativa secondaria: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
     - In questo esempio, `o-a1b2c3d4e5` è l'ID dell'organizzazione, `r-f6g7h8i9j0example` è l'ID radice, `ou-ghi0-awsccccc` è un ID OU ed `ou-jkl0-awsddddd` è un ID OU figlio.
     - IPAM non gestirà gli indirizzi IP negli account dell'unità organizzativa secondaria.
   - Esempio 2
     - Percorso in cui tutti i bambini OUs faranno parte dell'esclusione: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
     - In questo esempio, IPAM non gestirà gli indirizzi IP negli account dell'unità organizzativa (`ou-ghi0-awsccccc`) o negli account di altri OUs che sono figli dell'unità organizzativa.

   > **Note**
   >
   > L'insieme di esclusioni risultante non deve «sovrapporsi», il che significa che due o più esclusioni di unità organizzative non devono escludere la stessa unità organizzativa.

Esempio di percorsi di entità non sovrapposti:

- Percorso 1 ="o-1/r-1/ou-1/»
- Percorso 2 ="o-1/r-1/ou-1/ou-2/»

Questi percorsi non si sovrappongono perché Path 1 esclude solo gli account sotto ou-1 e Path 2 esclude solo gli account sotto ou-2.
Esempio di percorsi di entità sovrapposti:

- Percorso 1 ="o-1/r-1/ou-1/*»
- Percorso 2 ="o-1/r-1/ou-1/ou-2/»

Questi percorsi si sovrappongono perché il Percorso 1 rappresenta sia «o-1/r-1/ou-1/» che «o-1/r-1/ou-1/ou-2/» e «o-1/r-1/ou-1/ou-2/» si sovrappone al Percorso 2.

Input:

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

Output:

```
{
    "IpamResourceDiscovery": {
        "OwnerId": "111122223333",
        "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-resource-
discovery/ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryRegion": "us-east-1",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
```

```
        ],
        "IsDefault": false,
        "State": "modify-in-progress",
        "OrganizationalUnitExclusions": [
            {
                "OrganizationsEntityPath": "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-
ghi0-awscccccc/*"
            }
        ]
    }
}
```

Modifica un livello IPAM

IPAM offre due livelli: livello gratuito e livello avanzato. Il passaggio al livello avanzato di Gestione indirizzi IP di Amazon VPC offre un controllo più granulare sugli indirizzi IP. Ciò può essere utile man mano che la complessità della rete aumenta, perché consente di ottimizzare e gestire meglio lo spazio degli indirizzi IP. Per ulteriori informazioni sulle funzionalità disponibili in ogni livello gratuito e sui costi associati al livello avanzato, consulta la scheda IPAM nella pagina dei prezzi di Amazon VPC.

> **Note**
>
> Prima di poter passare dal livello avanzato al livello gratuito, devi:
>
> - Eliminare i pool con ambito privato.
> - Eliminare ambiti privati non predefiniti.
> - Eliminare i pool con locali diverse dalla regione di origine IPAM.
> - Eliminare le associazioni di rilevamento risorse non predefinite.
> - Eliminare le allocazioni dei pool agli account diversi da quello del proprietario IPAM.

AWS Management Console

Modifica del livello IPAM

1. Aprire la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, scegli IPAMs.

3. Nel riquadro dei contenuti, seleziona il tuo IPAM.
4. Scegli Operazioni > Modifica.

> **Note**
>
> Se utilizzi il piano gratuito, vedrai che il numero di IP attivi totali IPAM stimato è... . Il numero totale di IP attivi è il numero di indirizzi IP attivi nel tuo IPAM che ti verrebbero addebitati se passassi dal piano gratuito al livello avanzato. Un indirizzo IP attivo è definito come un indirizzo IP o un prefisso associato a un'interfaccia di rete elastica (ENI) collegata a una risorsa come un'istanza. EC2
>
> - Questa metrica è disponibile solo per i clienti del piano gratuito.
> - Se il tuo IPAM è integrato con AWS Organizations, il conteggio IP attivo copre tutti gli account dell'organizzazione.
> - Non è possibile visualizzare una suddivisione del numero di IP attivi per tipo di IP (public/private) or class (IPv4/IPv6).
> - IPAM conta solo gli account IPs di ENIs proprietà degli account monitorati. Il conteggio potrebbe quindi essere impreciso a causa delle sottoreti condivise. Gli indirizzi IP sono esclusi se il proprietario della sottorete o dell'ENI non è coperto dall'IPAM.

5. Scegli il livello IPAM da utilizzare per l'IPAM.
6. Scegli Save changes (Salva modifiche).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per visualizzare e modificare un livello IPAM:

1. Visualizza corrente IPAMs: describe-ipams
2. Modifica il livello IPAM: modify-ipam
3. Visualizza il tuo aggiornamento: describe-ipams IPAMs

Modifica le regioni operative IPAM

Le regioni operative sono AWS regioni in cui l'IPAM è autorizzato a gestire l'indirizzo CIDRs IP. IPAM rileva e monitora solo le risorse nelle AWS regioni selezionate come regioni operative.

L'aggiunta di una regione operativa a un IPAM consente di gestire lo spazio degli indirizzi IP su più regioni. AWS Così è possibile migliorare l'utilizzo degli indirizzi IP, consentire la segmentazione regionale e supportare un'infrastruttura geograficamente distribuita. L'espansione dell'ambito regionale di IPAM offre maggiore flessibilità e controllo sulla gestione complessiva degli indirizzi IP.

AWS Management Console

Modifica delle regioni operative IPAM

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, scegli IPAMs.
3. Nel riquadro dei contenuti, seleziona il tuo IPAM.
4. Scegli Operazioni > Modifica.
5. In IPAM settings (Impostazioni IPAM), scegli le Operating Regions (Regioni operative) da utilizzare per l'IPAM.
6. Scegli Save changes (Salva modifiche).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per visualizzare e modificare le regioni operative IPAM:

1. Visualizza corrente IPAMs: describe-ipams
2. Aggiungere o rimuovere regioni operative IPAM: modify-ipam
3. Visualizza il tuo aggiornamento: describe-ipams IPAMs

Fornitura CIDRs a un pool

Segui i passaggi descritti in questa sezione per effettuare il provisioning CIDRs a un pool. Se hai già effettuato il provisioning di un CIDR quando hai creato il pool, potresti dover effettuare un provisioning aggiuntivo CIDRs se un pool è prossimo all'allocazione completa. Per monitorare l'utilizzo del pool, consulta Monitora l'utilizzo del CIDR con il pannello di controllo IPAM.

> **Note**
>
> I termini effettuare il provisioning e assegnare sono utilizzati in questa guida per l'utente e nella console IPAM. Effettuare il provisioning viene utilizzato quando si aggiunge un CIDR a un pool IPAM. Utilizza Alloca quando associ un CIDR da un pool IPAM a un VPC o un indirizzo IP elastico.

AWS Management Console

Per effettuare il provisioning di un pool CIDRs

1. Aprire la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, selezionare Pool.
3. Per impostazione predefinita è selezionato l'ambito privato di default. Se non si desidera utilizzare l'ambito privato di default, scegliere l'ambito che si desidera utilizzare dal menu a tendina nella parte superiore del riquadro dei contenuti. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Nel riquadro dei contenuti, scegliere il pool a cui si desidera aggiungere un CIDR.
5. Scegliete Azioni > Fornitura CIDRs.
6. Esegui una di queste operazioni:
   - Se stai effettuando il provisioning di un CIDR a un pool di ambito pubblico, inserisci la Maschera di rete.
   - Se stai fornendo un CIDR a un IPv4 pool nell'ambito privato, inserisci il CIDR.
   - Se stai fornendo un CIDR a un IPv6 pool nell'ambito privato, tieni presente quanto segue:
     - Per dettagli importanti sull' IPv6 indirizzamento privato, IPv6 consulta Indirizzi privati nella Amazon VPC User Guide.

- Per utilizzare un intervallo IPv6 ULA privato, nella sezione CIDRsDa fornire, scegli Aggiungi ULA CIDR per maschera di rete e scegli la dimensione della maschera di rete oppure scegli Inserisci IPv6 CIDR privato e inserisci un intervallo ULA. Gli intervalli validi per l' IPv6 ULA privato sono compresi tra /9 e /60 a partire da fd80: :/9.
- Per utilizzare un intervallo IPv6 GUA privato, devi prima aver abilitato l'opzione sul tuo IPAM (vedi). Abilita il provisioning GUA privato IPv6 CIDRs Dopo aver abilitato il IPv6 GUA privato CIDRs, inserisci un IPv6 GUA in Input private IPv6 CIDR.

> **Note**
>
> - Per impostazione predefinita, puoi aggiungere un blocco IPv6 CIDR fornito da Amazon a un pool regionale. Per informazioni sull'incremento del limite predefinito, consulta Quote per l'IPAM.
> - Il CIDR di cui si desidera effettuare il provisioning deve essere disponibile nell'ambito.
> - Se esegui il provisioning CIDRs a un pool all'interno di un pool, lo spazio CIDR che desideri fornire deve essere disponibile nel pool.

7. Scegli Provision (Esegui il provisioning).
8. È possibile visualizzare il CIDR in IPAM scegliendo Pool nel pannello di navigazione, scegliendo un pool e visualizzando la CIDRs scheda relativa al pool.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per effettuare il provisioning CIDRs a un pool:

1. Ottieni l'ID di un pool IPAM: describe-ipam-pools
2. Ottieni quelli CIDRs che vengono forniti al pool: get-ipam-pool-cidrs
3. Fornisci un nuovo CIDR al pool: provision-ipam-pool-cidr
4. Ottieni CIDRs i dati forniti al pool e visualizza il nuovo CIDR: get-ipam-pool-cidrs

Sposta il VPC CIDRs tra gli ambiti

Il CIDRs passaggio da un ambito all'altro consente di ottimizzare l'allocazione degli indirizzi IP, organizzarli per regione, separare le preoccupazioni, applicare la conformità e adattarsi ai cambiamenti dell'infrastruttura. Questa flessibilità aiuta a gestire lo spazio degli indirizzi IP in modo efficiente man mano che i carichi di lavoro si evolvono.

Per spostare un CIDR VPC da un ambito a un altro, segui la procedura descritta in questa sezione.

⚠ Important

- Puoi spostare solo i VPC CIDRs. Quando sposti un CIDR VPC, anche la sottorete CIDRs del VPC viene spostata automaticamente.
- Puoi spostare il VPC solo CIDRs da un ambito privato a un altro. Non è possibile spostare il VPC CIDRs da un ambito pubblico a un ambito privato o da un ambito privato a un ambito pubblico.
- Lo stesso AWS account deve possedere entrambi gli ambiti.
- Se un CIDR VPC è attualmente allocato da un pool in un ambito privato, la richiesta di spostamento ha esito positivo, ma il CIDR non verrà spostato fino a quando non si rilascia l'allocazione dal pool corrente. Per informazioni sul rilascio di un'allocazione, consulta Rilascio di un'allocazione.

AWS Management Console

Spostamento di un CIDR assegnato a un VPC

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di spostamento seleziona Resources (Risorse).
3. Dal menu a tendina nella parte superiore del riquadro dei contenuti, scegliere l'ambito che si desidera utilizzare.
4. Nel riquadro dei contenuti, scegli un VPC e visualizzane i dettagli.
5. In VPC CIDRs, seleziona una delle risorse CIDRs allocate alla risorsa e scegli Azioni > Sposta CIDR in un ambito diverso.
6. Seleziona l'ambito in cui desideri spostare il CIDR VPC.
7. Scegli Move CIDR to different scope (Sposta CIDR in un ambito diverso).

Command line

Usa i seguenti AWS CLI comandi per spostare un CIDR VPC:

1. Ottieni un VPC CIDR nell'ambito corrente: get-ipam-resource-cidrs
2. Sposta un CIDR VPC: modify-ipam-resource-cidr
3. Ottieni un VPC CIDR nell'altro ambito: get-ipam-resource-cidrs

Rilasciare un'assegnazione

Se si prevede di eliminare un pool, potrebbe essere necessario rilasciare un'assegnazione del pool. Un'assegnazione è un incarico CIDR da un pool IPAM a un'altra risorsa o pool IPAM.

Non è possibile eliminare i pool se i pool sono stati CIDRs assegnati e non è possibile eseguire il deprovisioning CIDRs se CIDRs sono allocati a risorse.

Note

- Per rilasciare un'allocazione manuale, utilizza i passaggi in questa sezione o chiama l'API. ReleaseIpamPoolAllocation
- Per rilasciare un'allocazione in un ambito privato, è necessario ignorare o eliminare il CIDR della risorsa. Per ulteriori informazioni, consulta Modifica lo stato di monitoraggio del VPC CIDRs. Dopo un po' di tempo, Amazon VPC IPAM rilascerà automaticamente l'allocazione per tuo conto.

  Example

  Esempio

  Se si dispone di un CIDR VPC in un ambito privato, per rilasciare l'allocazione è necessario ignorare o eliminare il CIDR VPC. Dopo un po' tempo, Amazon VPC IPAM rilascerà automaticamente l'allocazione CIDR VPC dal pool IPAM.
- Per rilasciare un'allocazione in un ambito pubblico, è necessario eliminare il CIDR della risorsa. Non puoi ignorare le risorse CIDRs pubbliche. Per ulteriori informazioni, consultare Cleanup in Porta il tuo IPv4 CIDR pubblico su IPAM usando solo la CLI AWS o Cleanup in Porta il tuo IPv6 CIDR su IPAM usando solo la CLI AWS. Dopo un po 'di tempo, Amazon VPC IPAM rilascerà automaticamente l'allocazione per tuo conto.

Per consentire ad Amazon VPC IPAM di rilasciare le allocazioni per tuo conto, tutte le autorizzazioni dell'account devono essere configurate correttamente per uso di un account singolo o uso con più account.

Quando si rilascia un CIDR gestito da IPAM, Amazon VPC IPAM ricicla il CIDR in un pool IPAM. Se si utilizza IPAM nel livello avanzato, sono necessari alcuni minuti perché il CIDR diventi disponibile per le assegnazioni future. Se si utilizza IPAM nel piano gratuito, sono necessarie fino a 48 ore perché il CIDR diventi disponibile per le assegnazioni future. Per ulteriori informazioni sui pool e le assegnazioni, consulta Funzionamento di IPAM.

AWS Management Console

Per rilasciare un'assegnazione di pool

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, seleziona Pool.
3. Dal menu a tendina nella parte superiore del riquadro dei contenuti, scegliere l'ambito che si desidera utilizzare. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Nel riquadro dei contenuti, scegli il pool in cui si trova l'assegnazione.
5. Scegli la scheda Assegnazioni.
6. Seleziona una o più allocazioni. È possibile identificare le allocazioni in base al tipo di risorsa:
   - personalizzata: un'allocazione personalizzata.
   - vpc: un'allocazione VPC.
   - ipam-pool: un'allocazione di pool IPAM.
   - ec2-public-ipv4-pool: allocazione di un pool pubblico. IPv4
   - subnet: l'allocazione di una sottorete.
7. Scegli Actions (Operazioni) > Release custom allocation (Rilascia allocazione personalizzata).
8. Scegli De-assegna CIDR.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizzate i seguenti AWS CLI comandi per rilasciare l'allocazione di un pool:

1. Ottieni un ID del pool IPAM: describe-ipam-pools
2. Visualizza le tue attuali allocazioni nel pool: get-ipam-pool-allocations
3. Rilascia un'allocazione: release-ipam-pool-allocation
4. Visualizza le allocazioni aggiornate: get-ipam-pool-allocations

Per aggiungere una nuova assegnazione, consulta Allocazione CIDRs da un pool IPAM.
Per eliminare il pool dopo aver rilasciato le assegnazioni, è necessario innanzitutto eseguire Deapprovvigionamento CIDRs da un pool.

Condivisione di un pool IPAM tramite AWS RAM

Segui i passaggi di questa sezione per condividere un pool IPAM utilizzando AWS Resource Access Manager (RAM). Quando condividi un pool IPAM con RAM, i «responsabili» possono allocare CIDRs dal pool alle AWS risorse VPCs, ad esempio dai rispettivi account. Un principal è un concetto in RAM che indica qualsiasi AWS account, ruolo IAM o unità organizzativa in AWS Organizations. Per ulteriori informazioni, consulta Condivisione AWS delle risorse nella AWS RAM User Guide.

Note

- Puoi condividere un pool IPAM con AWS RAM solo se hai integrato IPAM con Organizations AWS . Per ulteriori informazioni, consulta Integrare IPAM con gli account di un'organizzazione AWS. Non puoi condividere un pool IPAM con AWS RAM se sei un utente IPAM con account singolo.
- È necessario abilitare la condivisione delle risorse con AWS Organizations in AWS RAM. Per ulteriori informazioni, consulta Enable resource sharing within AWS Organizations nella AWS RAM User Guide.
- La condivisione della RAM è disponibile solo nella AWS regione di origine del tuo IPAM. È necessario creare la condivisione nella AWS regione in cui si trova l'IPAM, non nella regione del pool IPAM.

- L'account che crea ed elimina le condivisioni di risorse del pool IPAM deve disporre delle seguenti autorizzazioni nella policy IAM collegata al rispettivo ruolo IAM:
  - `ec2:PutResourcePolicy`
  - `ec2:DeleteResourcePolicy`
- È possibile aggiungere più pool IPAM a una condivisione RAM.
- Sebbene sia possibile condividere i pool IPAM con qualsiasi AWS account esterno a un' AWS organizzazione, IPAM monitorerà gli indirizzi IP negli account esterni all'organizzazione solo se il proprietario dell'account ha completato il processo di condivisione delle proprie risorse con l'amministratore IPAM delegato, come descritto in. Come integrare IPAM con account esterni alla tua organizzazione

AWS Management Console

Per condividere un pool IPAM utilizzando RAM

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, selezionare Pool.
3. Per impostazione predefinita è selezionato l'ambito privato di default. Se non si desidera utilizzare l'ambito privato di default, scegliere l'ambito che si desidera utilizzare dal menu a tendina nella parte superiore del riquadro dei contenuti. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Nel riquadro dei contenuti, seleziona il pool da condividere e scegli Operazioni > Visualizza dettagli.
5. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. Di conseguenza, si apre la console AWS RAM. Creerai il pool condiviso nella AWS RAM.
6. Selezionare Create a resource share (Crea una condivisione di risorse).
7. Aggiungi un Nome per la risorsa condivisa.
8. Alla voce Seleziona il tipo di risorsa, seleziona i pool IPAM e scegli uno o più pool IPAM.
9. Scegli Next (Successivo).
10. Scegli una delle autorizzazioni per la condivisione di risorse:
    - AWSRAMDefaultPermissionsIpamPool: Scegli questa autorizzazione per consentire ai principali di visualizzare le allocazioni CIDRs e nel pool IPAM condiviso e di CIDRs allocare/rilasciare nel pool.

- AWSRAMPermissionIpamPoolByoipCidrImport: Scegli questa autorizzazione per consentire ai principali di importare BYOIP nel pool IPAM condiviso. CIDRs Avrai bisogno di questa autorizzazione solo se disponi di BYOIP esistente CIDRs e desideri importarli in IPAM e condividerli con i principali. Per ulteriori informazioni su CIDRs BYOIP to IPAM, vedere. Tutorial: trasferimento di un IPv4 CIDR BYOIP a IPAM

11. Scegli i principal a cui è consentito accedere a questa risorsa. Se i principali importeranno il BYOIP CIDRs esistente in questo pool IPAM condiviso, aggiungi l'account proprietario CIDR BYOIP come principale.
12. Controlla le opzioni di condivisione delle risorse e i principal con cui condividere e scegli Crea.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. Qui troverai descrizioni dettagliate delle opzioni che puoi usare quando esegui i comandi.

Utilizzate i seguenti AWS CLI comandi per condividere un pool IPAM tramite RAM:

1. Ottieni l'ARN dell'IPAM: describe-ipam-pools
2. Crea la condivisione di risorse: create-resource-share
3. Visualizza la condivisione delle risorse: get-resource-shares

Come risultato della creazione della condivisione di risorse nella RAM, altri principali possono ora CIDRs allocare le risorse utilizzando il pool IPAM. Per informazioni sul monitoraggio delle risorse create dai principal, consulta Monitoraggio dell'utilizzo del CIDR per risorsa. Per ulteriori informazioni su come creare un VPC e allocare un CIDR da un pool IPAM condiviso, consulta Create a VPC nella Amazon VPC User Guide.

Lavora con il rilevamento delle risorse

Un rilevamento di risorse è un componente IPAM che consente a IPAM di gestire e monitorare le risorse appartenenti all'account proprietario del rilevamento. Ciò consente a IPAM di mantenere un up-to-date inventario dell'utilizzo degli indirizzi IP tra i carichi di lavoro, facilitando la gestione e la pianificazione degli indirizzi IP.

Per impostazione predefinita, quando crei un IPAM viene creato un rilevamento delle risorse. Puoi creare un rilevamento delle risorse anche indipendentemente da un IPAM e integrarlo con un IPAM

di proprietà di un altro account o un'altra organizzazione. Se il proprietario del rilevamento delle risorse è l'amministratore delegato di un'organizzazione, IPAM monitorerà le risorse per tutti i membri dell'organizzazione.

> **Note**
>
> La creazione, la condivisione e l'associazione di rilevamenti delle risorse fa parte del processo di integrazione di IPAM con account esterni alle tue organizzazioni (consulta Come integrare IPAM con account esterni alla tua organizzazione). Se non crei un IPAM e non lo integri con account esterni alla tua organizzazione, non è necessario creare, condividere o associare rilevamenti delle risorse.

Ricorda che questa sezione è un raggruppamento di procedure tutte relative all'utilizzo del rilevamento di risorse.

Indice

- Crea un rilevamento di risorse da integrare con un altro IPAM
- Come visualizzare i dettagli del rilevamento delle risorse
- Condividi la scoperta di una risorsa con un altro AWS account
- Come associare un rilevamento delle risorse a un IPAM
- Come annullare l'associazione di un rilevamento delle risorse
- Come eliminare un rilevamento delle risorse

Crea un rilevamento di risorse da integrare con un altro IPAM

Questa sezione spiega come creare un rilevamento delle risorse. Per impostazione predefinita, quando crei un IPAM viene creato un rilevamento delle risorse. La quota predefinita per i rilevamenti delle risorse per ogni regione è 1. Per ulteriori informazioni sulle quote IPAM, consulta Quote per l'IPAM.

> **Note**
>
> La creazione, la condivisione e l'associazione dei rilevamenti delle risorse fa parte del processo di integrazione di IPAM con account esterni alle tue organizzazioni (consulta Come integrare IPAM con account esterni alla tua organizzazione). Se non crei un IPAM e non lo

integri con account esterni alla tua organizzazione, non è necessario creare, condividere o associare rilevamenti delle risorse.

Se integri un IPAM con account esterni alle tue organizzazioni, questo passaggio è obbligatorio e deve essere completato dall'account amministratore dell'organizzazione secondaria. Per ulteriori informazioni sui ruoli coinvolti in questa procedura, consulta Panoramica del processo.

AWS Management Console

Come creare un rilevamento delle risorse

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di navigazione, scegli Rilevamenti delle risorse.
3. Scegli Crea individuazione delle risorse.
4. Seleziona Consenti a IP Address Manager di Amazon VPC di replicare i dati dagli account sorgente verso l'account IPAM delegato. Se non selezioni questa opzione, non puoi creare un rilevamento delle risorse.
5. (Facoltativo) Aggiungi un tag Nome al rilevamento delle risorse. Un tag è un'etichetta che si assegna a una AWS risorsa. Ciascun tag è formato da una chiave e da un valore facoltativo. Puoi utilizzare i tag per cercare e filtrare le tue risorse o tenere traccia AWS dei costi.
6. (Opzionale) Aggiungi una descrizione.
7. In Aree operative, seleziona le AWS regioni in cui verranno scoperte le risorse. La regione corrente verrà impostata automaticamente come una delle regioni operative. Se crei il rilevamento delle in modo da poterlo condividere con un IPAM nella regione operativa `us-east-1`, seleziona `us-east-1` qui. Se dimentichi una regione operativa, puoi tornare al passaggio suindicato in un secondo momento e modificare le impostazioni del rilevamento delle risorse.

   > **Note**
   >
   > Nella maggior parte dei casi, il rilevamento delle risorse deve avere le stesse regioni operative dell'IPAM, altrimenti il rilevamento delle risorse verrà eseguito solo in quest'unica regione.

8. (Facoltativo) Scegli un Tag aggiuntivo per il pool.
9. Scegli Create (Crea) .

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Crea una scoperta di risorse: create-ipam-resource-discovery

Come visualizzare i dettagli del rilevamento delle risorse

La visualizzazione dei dettagli di una scoperta di risorse in AWS IPAM può fornire informazioni preziose, come:

- Identificazione delle AWS risorse specifiche che sono state importate e delle relative allocazioni di indirizzi IP associate.
- Monitoraggio dello stato e del progresso del processo di rilevamento delle risorse.
- Risoluzione di eventuali problemi o discrepanze tra IPAM e le risorse rilevate.
- Analisi dell'utilizzo e delle tendenze degli indirizzi IP.

Queste informazioni possono aiutare a ottimizzare la gestione degli indirizzi IP e a garantire l'allineamento tra IPAM e l'effettiva implementazione delle risorse.

AWS Management Console

Come visualizzare i dettagli del rilevamento delle risorse

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di navigazione, scegli Rilevamenti delle risorse.
3. Scegli un rilevamento delle risorse.
4. In voce Dettagli sull'individuazione delle risorse visualizza i dettagli relativi al rilevamento delle risorse, ad esempio Predefinito, che indica se il rilevamento delle risorse è quello predefinito. Il rilevamento delle risorse predefinito è quello creato automaticamente quando crei un IPAM.
5. Nelle schede, visualizza i dettagli di un rilevamento delle risorse:

- Risorse rilevate: risorse monitorate con un rilevamento delle risorse. IPAM esegue il monitoraggio CIDRs dai seguenti tipi di risorse, IPv4 pool pubblici VPCs, sottoreti VPC e indirizzi IP elastici.
  - Nome (ID risorsa): ID del rilevamento delle risorse.
  - IPs allocato: la percentuale di spazio degli indirizzi IP in uso. Per convertire il decimale in percentuale, moltiplica il decimale per 100. Tieni presente quanto segue:
    - Per le risorse che lo sono VPCs, si tratta della percentuale di spazio degli indirizzi IP nel VPC occupata dalla sottorete. CIDRs
    - Per le risorse che sono sottoreti, se alla sottorete è assegnato un IPv4 CIDR, questa è la percentuale di spazio di IPv4 indirizzi nella sottorete in uso. Se alla sottorete è assegnato un IPv6 CIDR, la percentuale di spazio di indirizzi in uso non è rappresentata. IPv6 La percentuale di spazio degli IPv6 indirizzi in uso non può attualmente essere calcolata.
    - Per le risorse che sono IPv4 pool pubblici, questa è la percentuale di spazio di indirizzi IP nel pool che è stata allocata agli indirizzi IP elastici (EIPs).
  - CIDR: CIDR della risorsa.
  - Regione: regione della risorsa.
  - ID proprietario: ID del proprietario della risorsa.
  - Tempo di campionamento: l'ultima volta in cui il rilevamento delle risorse è riuscito.
- Account scoperti: AWS account monitorati durante l'individuazione di risorse. Se hai integrato IPAM con AWS Organizations, tutti gli account dell'organizzazione vengono scoperti account.
  - ID account: ID dell'account.
  - Regione: la AWS regione da cui vengono restituite le informazioni sull'account.
  - Ultima tentativo di rilevamento: l'ultima volta in cui è stato effettuato un tentativo di rilevamento delle risorse.
  - Ultimo rilevamento riuscito: l'ultima volta in cui il rilevamento delle risorse è riuscito.
  - Stato: motivo dell'errore del rilevamento delle risorse.
- Regioni operative: le regioni operative per il rilevamento delle risorse.
- Condivisione risorse: se il rilevamento delle risorse è stato condiviso, viene elencato l'ARN del rilevamento delle risorse.
  - ARN condivisione risorse: ARN della condivisione di risorse.

- Stato: lo stato corrente della condivisione di risorse. I valori possibili sono:
  - Attiva: la condivisione di risorse è attiva e utilizzabile.
  - Eliminata: la condivisione di risorse viene eliminata e non è più utilizzabile.
  - In sospeso: un invito ad accettare la condivisione di risorse è in attesa di risposta.
- Creato alle: l'ora in cui è stata creata la condivisione di risorse.

- Tag: un tag è un'etichetta che assegni a una AWS risorsa. Ciascun tag è formato da una chiave e da un valore facoltativo. È possibile utilizzare i tag per cercare e filtrare le risorse o monitorare i costi AWS .

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Visualizza i dettagli sulla scoperta delle risorse: describe-ipam-resource-discoveries

Condividi la scoperta di una risorsa con un altro AWS account

Segui i passaggi di questa sezione per condividere una scoperta di risorse utilizzando AWS Resource Access Manager. Per ulteriori informazioni in merito AWS RAM, consulta Condivisione AWS delle risorse nella Guida AWS RAM per l'utente.

> **Note**
>
> La creazione, la condivisione e l'associazione di rilevamenti delle risorse fa parte del processo di integrazione di IPAM con account esterni alle tue organizzazioni (consulta Come integrare IPAM con account esterni alla tua organizzazione). Se non crei un IPAM e non lo integri con account esterni alla tua organizzazione, non è necessario creare, condividere o associare rilevamenti delle risorse.

Quando crei un IPAM che monitora gli account esterni alla tua organizzazione, l'account amministratore dell'organizzazione secondaria condivide il rilevamento delle risorse con l'account IPAM dell'organizzazione primaria tramite AWS RAM. Affinché l'account IPAM dell'organizzazione primaria possa associare il rilevamento delle risorse al proprio IPAM, devi prima innanzitutto

condividere un rilevamento delle risorse con l'account IPAM dell'organizzazione primaria. Per ulteriori informazioni sui ruoli implicati in questo processo, consulta Panoramica del processo.

> **Note**
>
> - Quando si crea una condivisione di risorse utilizzando AWS RAM per condividere una scoperta di risorse, è necessario creare la condivisione di risorse nella regione di origine dell'IPAM dell'organizzazione primaria.
> - L'account che crea ed elimina una condivisione di risorse per un rilevamento delle risorse deve disporre delle seguenti autorizzazioni nella propria policy IAM:
>   - ec2: PutResourcePolicy
>   - ec2: DeleteResourcePolicy
> - Se condividi l'individuazione di una risorsa con un altro account, tale account può visualizzare tutte le esclusioni di unità organizzative relative all'account, che contiene informazioni come l'ID di organizzazione, l'ID root e l'unità organizzativa dell'organizzazione IDs del proprietario della ricerca delle risorse.

Se integri un IPAM con account esterni alle tue organizzazioni, questo passaggio è obbligatorio e deve essere completato dall'account amministratore dell'organizzazione secondaria.

AWS Management Console

Come condividere un rilevamento delle risorse

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di navigazione, scegli Rilevamenti delle risorse.
3. Scegli la scheda Condivisione risorse.
4. Seleziona Crea condivisione risorse. Si apre la AWS RAM console, nella quale verrà creata la condivisione delle risorse.
5. Nella AWS RAM console, scegli Impostazioni.
6. Scegli Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.
7. Selezionare Create a resource share (Crea una condivisione di risorse).
8. Aggiungi un Nome per la risorsa condivisa.

9. In Seleziona tipo di risorsa, seleziona Rilevamento risorse IPAM e scegli il rilevamento delle risorse.
10. Scegli Next (Successivo).
11. In Associa autorizzazioni, puoi visualizzare l'autorizzazione predefinita che verrà abilitata per i principali a cui è concesso l'accesso a questa condivisione di risorse:
    - AWSRAMPermissionIpamResourceDiscovery
    - Operazioni consentite da questa autorizzazione:
      - ec2: AssociateIpamResourceDiscovery
      - ec2: GetIpamDiscoveredAccounts
      - ec2: GetIpamDiscoveredPublicAddresses
      - ec2: GetIpamDiscoveredResourceCidrs
12. Specifica i principali a cui è consentito l'accesso alla risorsa condivisa. Per Principali scegli l'account IPAM dell'organizzazione principale, quindi scegli Aggiungi.
13. Scegli Next (Successivo).
14. Controlla le opzioni di condivisione di risorse e i principali con cui avverrà la condivisione. Seleziona, quindi, Crea condivisione risorse.
15. Una volta condiviso, un rilevamento delle risorse deve essere accettato dall'account IPAM dell'organizzazione primaria e poi associato a un IPAM dall'account IPAM dell'organizzazione primaria. Per ulteriori informazioni, consulta Come associare un rilevamento delle risorse a un IPAM.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

1. Crea la condivisione di risorse: create-resource-share
2. Visualizza la condivisione delle risorse: get-resource-shares

Come associare un rilevamento delle risorse a un IPAM

Questa sezione spiega come associare un rilevamento delle risorse a un IPAM. Quando si associa un rilevamento delle risorse a un IPAM, l'IPAM monitora tutte le risorse CIDRs e gli account rilevati

nell'ambito dell'individuazione delle risorse. Quando crei un IPAM, un rilevamento delle risorse predefinito per l'IPAM viene creato e associato automaticamente al tuo IPAM.

La quota predefinita per le associazioni del rilevamento delle risorse è 5. Per ulteriori informazioni (inclusa la modalità di modifica di questa quota), consulta Quote per l'IPAM.

> **Note**
>
> La creazione, la condivisione e l'associazione dei rilevamenti delle risorse fa parte del processo di integrazione di IPAM con account esterni alle tue organizzazioni (consulta Come integrare IPAM con account esterni alla tua organizzazione). Se non crei un IPAM e non lo integri con account esterni alla tua organizzazione, non è necessario creare, condividere o associare rilevamenti delle risorse.

Se integri un IPAM con account esterni alle tue organizzazioni, questo passaggio è obbligatorio e deve essere completato dall'account IPAM dell'organizzazione primaria. Per ulteriori informazioni sui ruoli implicati in questo processo, consulta Panoramica del processo.

AWS Management Console

Come associare un rilevamento delle risorse

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, scegli IPAMs.
3. Seleziona Rilevamenti associati e scegli Associa rilevamenti delle risorse.
4. In Rilevamenti delle risorse IPAM scegli un rilevamento delle risorse che l'account amministratore dell'organizzazione secondaria ha condiviso con te.
5. Selezionare Associate (Associa).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Associa una scoperta di risorse: associate-ipam-resource-discovery

Come annullare l'associazione di un rilevamento delle risorse

Questa sezione spiega come annullare l'associazione di un rilevamento delle risorse a un IPAM. Quando si dissocia un rilevamento delle risorse da un IPAM, l'IPAM non monitora più tutte le risorse CIDRs e gli account scoperti nell'ambito dell'individuazione delle risorse.

> **Note**
>
> Non puoi annullare l'associazione di un rilevamento delle risorse predefinito. Quando crei un IPAM, viene creata automaticamente un'associazione del rilevamento delle risorse predefinito. Tuttavia, l'associazione del rilevamento delle risorse predefinito viene eliminata se elimini l'IPAM.

Questo passaggio deve essere completato dall'account IPAM dell'organizzazione primaria. Per ulteriori informazioni sui ruoli implicati in questo processo, consulta Panoramica del processo.

AWS Management Console

Come annullare l'associazione di un rilevamento delle risorse

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, scegli IPAMs.
3. Seleziona Rilevamenti associati e scegli Annulla associazione rilevamenti delle risorse.
4. In voce Rilevamento delle risorse IPAM scegli un rilevamento delle risorse che l'account amministratore dell'organizzazione secondaria ha condiviso con te.
5. Scegli Dissocia.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Per dissociare l'individuazione di una risorsa: disassociate-ipam-resource-discovery

Come eliminare un rilevamento delle risorse

Questa sezione spiega come eliminare un rilevamento delle risorse.

> **Note**
>
> Non puoi eliminare un rilevamento delle risorse predefinito. Un rilevamento delle risorse predefinito è quello che viene creato automaticamente quando crei un IPAM. Il rilevamento delle risorse predefinito, tuttavia, viene eliminato se elimini l'IPAM.

Questo passaggio deve essere completato dall'account amministratore dell'organizzazione secondaria. Per ulteriori informazioni sui ruoli implicati in questo processo, consulta Panoramica del processo.

AWS Management Console

Come eliminare un rilevamento delle risorse

1. Aprire la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di navigazione, scegli Rilevamenti delle risorse.
3. Seleziona un rilevamento delle risorse e scegli Operazioni > Elimina rilevamento delle risorse.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Per eliminare una scoperta di risorse: delete-ipam-resource-discovery

Monitoraggio dell'utilizzo dell'indirizzo IP in IPAM

Gestione indirizzi IP di Amazon VPC offre funzionalità di monitoraggio dell'utilizzo degli indirizzi IP che possono essere utili a chiunque gestisca ambienti di rete complessi. IPAM offre visibilità sull'assegnazione, l'utilizzo e le tendenze di consumo degli indirizzi IP su AWS. Ciò consente di identificare gli indirizzi IP inutilizzati o utilizzati in modo inefficiente, di ottimizzare lo spazio degli indirizzi e di prevenire il potenziale esaurimento degli indirizzi IP.

IPAM tiene traccia dell'utilizzo degli indirizzi IP a livello di CIDR, ambito e IPAM, fornendo report e analisi dettagliati. Questo è molto utile per le implementazioni su larga scala, le configurazioni multi-account e i requisiti di rete in evoluzione.

Sfruttando il monitoraggio dell'utilizzo di IPAM, è possibile prendere decisioni informate, migliorare la gestione degli indirizzi IP e garantire un utilizzo efficiente delle risorse IP.

> **Note**
>
> Le attività descritte in questa sezione sono facoltative. Se si desidera completare le attività in questa sezione e si è delegato un account IPAM, le attività dovranno essere completate dall'account IPAM.

Indice

- Monitora l'utilizzo del CIDR con il pannello di controllo IPAM
- Monitoraggio dell'utilizzo del CIDR per risorsa
- Monitora l'IPAM con Amazon CloudWatch
- Visualizzazione della cronologia degli indirizzi IP
- Visualizzazione di informazioni dettagliate relative agli indirizzi IP pubblici

Monitora l'utilizzo del CIDR con il pannello di controllo IPAM

La dashboard di IPAM in Gestione indirizzi IP di Amazon VPC consente di monitorare l'utilizzo del CIDR per diversi scenari chiave:

- Identifica lo spazio degli indirizzi IP inutilizzato o sottoutilizzato: la dashboard offre visibilità sull'utilizzo del CIDR, consentendoti di identificarti CIDRs con la capacità disponibile che può essere recuperata o riallocata.
- Ottimizza la gestione degli indirizzi IP: monitorando attentamente l'utilizzo del CIDR, è possibile prendere decisioni informate sull'espansione, la contrazione o la riassegnazione dei blocchi di indirizzi IP per soddisfare i requisiti aziendali e infrastrutturali in continuo cambiamento.
- Previeni l'esaurimento degli indirizzi IP: il monitoraggio dell'utilizzo del CIDR consente di prevedere quando potrebbe essere necessario acquisire spazio aggiuntivo per gli indirizzi IP, consentendo di pianificare ed evitare in modo proattivo le interruzioni del servizio dovute all'esaurimento degli indirizzi IP.
- Garantisci la conformità e la governance: la dashboard di IPAM può aiutarti a dimostrare gli schemi di utilizzo degli indirizzi IP per soddisfare i requisiti normativi o le policy interne relative alla gestione degli indirizzi IP.
- Risolvi i problemi di rete: i dati dettagliati sull'utilizzo del CIDR possono aiutare a identificare le cause principali dei problemi di connettività di rete o dei conflitti relativi alle risorse.

Monitorando attentamente l'utilizzo del CIDR tramite la dashboard di IPAM, è possibile migliorare l'efficienza, la resilienza e la conformità della gestione degli indirizzi IP in AWS.

AWS Management Console

Monitora l'utilizzo del CIDR con il pannello di controllo IPAM

1. Apri la console IPAM all'https://console.aws.amazon.com/ipam/indirizzo.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Per impostazione predefinita, quando viene visualizzato il pannello di controllo, l'ambito privato di default è selezionato. Se non si desidera utilizzare l'ambito privato di default, scegliere l'ambito che si desidera utilizzare dal menu a tendina nella parte superiore del riquadro dei contenuti. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. La dashboard presenta una panoramica dei pool IPAM e ne CIDRs rientra un ambito. Puoi aggiungere, rimuove, ridimensionare e spostare widget per personalizzare il pannello di controllo.

    - Ambito: I dettagli per questo ambito. Un ambito è il container di più alto livello all'interno di IPAM. Un IPAM contiene due ambiti predefiniti, uno privato e uno pubblico. Ogni ambito

rappresenta lo spazio IP per una singola rete. Puoi disporre di diversi ambiti privati, ma di un solo ambito pubblico.

- ID ambito: L'ID per questo ambito.
- Tipo di ambito: Il tipo di ambito.
- ID IPAM: ID dell'IPAM in cui si trova l'ambito.
- Pool IPAM di questo ambito: ID dell'IPAM in cui si trova l'ambito.
- Visualizza le risorse di rete di questo ambito: consente di accedere alla sezione Risorse della console IPAM.
- Cerca nella cronologia di un indirizzo IP in questo ambito: consente di accedere alla sezione Cerca nella cronologia IP della console IPAM.

- Tipi di risorse CIDR: i tipi di risorse inclusi CIDRs nell'ambito.
  - Subnet: il numero di CIDRs quattro sottoreti.
  - VPC: il numero di quattro. CIDRs VPCs
  - EIPs: Il numero CIDRs di indirizzi IP elastici.
  - IPv4 Piscine pubbliche: il numero CIDRs di IPv4 piscine pubbliche.
- Stato di gestione: lo stato di gestione di CIDRs.
  - Non gestita CIDRs: il numero di risorse CIDRs per le risorse non gestite in questo ambito.
  - Ignorato CIDRs: il numero di risorse CIDRs che hai scelto di esentare dal monitoraggio con IPAM nell'ambito. IPAM non valuta le risorse ignorate per la sovrapposizione o la conformità all'interno di un ambito. Una volta che una risorsa viene scelta per essere ignorata, qualsiasi spazio assegnato da un pool IPAM viene restituito al pool e la risorsa non verrà importata di nuovo tramite l'importazione automatica (se la regola di assegnazione dell'importazione automatica è impostata sul pool).
  - Gestito CIDRs: il numero di risorse CIDRs per risorse gestibili (VPCso IPv4 pool pubblici) allocate da un pool IPAM nell'ambito.
- Risorsa sovrapposta CIDRs: il numero di risorse sovrapposte e non sovrapposte. CIDRs La sovrapposizione può portare a un routing errato nel tuo CIDRs . VPCs
  - Sovrapposizione CIDRs: il numero di quelli CIDRs che attualmente si sovrappongono all'interno dei pool IPAM in questo ambito. La sovrapposizione CIDRs può portare a un routing errato nel tuo. VPCs
  - Nessuna sovrapposizione CIDRs: il numero di risorse CIDRs che non si sovrappongono all'interno dei pool IPAM in questo ambito.

- Risorsa conforme: il numero di risorse CIDRs conformi. CIDRs
  - Conforme CIDRs: il numero di risorse CIDRs conformi alle regole di allocazione per i pool IPAM nell'ambito.
  - Non conforme CIDRs: il numero di risorse CIDRs che non sono conformi alle regole di allocazione per i pool IPAM inclusi nell'ambito.
- Stato di sovrapposizione: il numero di tali sovrapposizioni nel tempo. CIDRs
  - OverlappingResourceCidrs: Il numero di tali sovrapposizioni all'interno dei pool IPAM in CIDRs questo ambito. La sovrapposizione CIDRs può portare a un routing errato nel tuo. VPCs
- Stato di conformità: il numero di CIDRs utenti conformi e non conformi alle regole di allocazione per i pool IPAM compresi nell'ambito di applicazione nel corso del tempo.
  - CompliantResourceCidrs: il numero di risorse conformi alle regole CIDRs di allocazione.
  - NoncompliantResourceCidrs: il numero di risorse CIDRs che non sono conformi alle regole di allocazione.
- Utilizzo VPC: VPCs (IPv4 e IPv6) con l'utilizzo IP più o meno elevato. Puoi utilizzare queste informazioni per configurare gli CloudWatch allarmi Amazon in modo che vengano avvisati in caso di superamento di una soglia di utilizzo dell'IP. Per ulteriori informazioni, consulta Parametri di utilizzo delle risorse IPAM.
- Utilizzo della sottorete: sottoreti (IPv4 solo) con l'utilizzo IP più o meno elevato. Puoi utilizzare queste informazioni per decidere se mantenere o eliminare le risorse sottoutilizzate. Per ulteriori informazioni, consulta Parametri di utilizzo delle risorse IPAM.
- VPCs con la massima IPs allocazione: quelle con la percentuale più alta VPCs di spazio di indirizzi IP allocato alle sottoreti. Ciò è utile per mostrare se è necessario fornire ulteriore spazio per indirizzi IP a. VPCs
- Sottoreti con l' IPsallocazione più alta: le sottoreti con la percentuale più alta di spazio di indirizzi IP allocato alle risorse. Questa informazione è utile a capire se hai bisogno di fornire spazio aggiuntivo alle sottoreti per gli indirizzi IP.
- Assegnazione del pool: la percentuale di spazio IP assegnato alle risorse e alle allocazioni manuali dell'ambito nel corso del tempo.
- Allocazione del pool: La percentuale dello spazio IP di un pool allocato ad altri pool dell'ambito nel corso del tempo.

Command line

Le informazioni visualizzate nella dashboard provengono da metriche archiviate in Amazon CloudWatch. Per ulteriori informazioni sulle metriche memorizzate in Amazon CloudWatch, consultaMonitora l'IPAM con Amazon CloudWatch. Utilizza le CloudWatch opzioni Amazon nella AWS CLI Reference per visualizzare le metriche per le allocazioni nei tuoi pool e ambiti IPAM.

Se ritieni che il CIDR fornito per un pool sia quasi completamente allocato, potresti dover effettuare un provisioning aggiuntivo. CIDRs Per ulteriori informazioni, consulta Fornitura CIDRs a un pool.

Monitoraggio dell'utilizzo del CIDR per risorsa

La visualizzazione Risorse in Amazon VPC IP Address Manager offre una panoramica centralizzata dell'utilizzo degli indirizzi IP tra le tue risorse. AWS Questo consente di identificare rapidamente quali risorse stanno consumando indirizzi IP, tenere traccia delle tendenze di assegnazione degli indirizzi e ottimizzare la gestione degli indirizzi IP per allinearla all'infrastruttura e alle esigenze aziendali in evoluzione.

In IPAM, una risorsa è un'entità di AWS servizio a cui viene assegnato un indirizzo IP o un blocco CIDR. IPAM gestisce alcune risorse, ma in altri casi si limita a monitorarle, quindi è importante comprendere la differenza tra i due tipi di risorse:

- Risorsa gestita: Una risorsa gestita ha un CIDR assegnato da un pool IPAM. IPAM monitora il CIDR per rilevare eventuali sovrapposizioni di indirizzi IP con altri CIDRs membri del pool e monitora la conformità del CIDR alle regole di allocazione del pool. IPAM supporta la gestione del seguente tipo di risorse:
  - Indirizzi IP elastici
  - IPv4 Piscine pubbliche

    > **Note**
    >
    > I IPv4 pool pubblici e i pool IPAM sono gestiti da risorse distinte in AWS. I IPv4 pool pubblici sono risorse con account singolo che consentono di convertire gli indirizzi IP di proprietà pubblica in indirizzi IP CIDRs elastici. I pool IPAM possono essere utilizzati per allocare lo spazio pubblico ai pool pubblici. IPv4

  - VPCs

- Risorsa monitorata: se una risorsa è monitorata da IPAM, la risorsa è stata rilevata da IPAM ed è possibile visualizzare i dettagli sul CIDR della risorsa quando si utilizza con `get-ipam-resource-cidrs` la AWS CLI o quando si visualizzano le risorse nel riquadro di navigazione. IPAM supporta il monitoraggio delle seguenti risorse:
  - Indirizzi IP elastici
  - Piscine pubbliche IPv4
  - VPCs
  - Sottoreti VPC

AWS Management Console

Per monitorare dell'utilizzo del CIDR per risorsa

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel riquadro di spostamento seleziona Resources (Risorse).
3. Dal menu a discesa IP nella parte superiore del riquadro dei contenuti, scegli il protocollo di indirizzo IP che desideri utilizzare: IPv4 oppure. IPv6
4. Dal menu a tendina degli ambiti nella parte superiore del riquadro dei contenuti, scegli l'ambito che desideri utilizzare. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
5. Utilizza la mappa CIDR delle risorse per visualizzare lo spazio di indirizzi IP disponibile, allocato e sovrapposto in un ambito:
   - Disponibile: un intervallo di indirizzi IP è disponibile per l'allocazione.
   - Conforme e non sovrapposta: un intervallo di indirizzi IP è assegnato a una risorsa gestita da IPAM.
   - Occupato: un intervallo di indirizzi IP è allocato a una risorsa.
   - Sovrapposto: un intervallo di indirizzi IP è stato allocato a più risorse e si sovrappone.
   - Non conforme: un intervallo di indirizzi IP non è conforme. Una risorsa che utilizza l'intervallo di indirizzi IP non è conforme alle regole di allocazione impostate per il pool.

   Nella parte inferiore della mappa CIDR scegli un blocco di indirizzi IP per visualizzare le risorse in blocchi CIDR più piccoli. Nella parte superiore della mappa scegli un blocco di indirizzi IP per visualizzare le risorse in blocchi CIDR più grandi.

6. Nella tabella puoi visualizzare i dettagli seguenti relativi alle risorse dell'ambito:

   - Nome (ID risorsa): il nome e l'ID della risorsa.
   - CIDR: Il CIDR associato alla risorsa.
   - Stato della gestione: Lo stato della risorsa.
     - Gestita: La risorsa ha un CIDR assegnato da un pool IPAM ed è monitorata da IPAM per la potenziale sovrapposizione CIDR e la conformità alle regole di assegnazione del pool.
     - Non gestita: La risorsa non ha un CIDR assegnato da un pool IPAM e non è monitorata da IPAM per la potenziale sovrapposizione CIDR e la conformità alle regole di assegnazione del pool. Il CIDR è monitorato per la sovrapposizione.
     - Ignorato: La risorsa è stata scelta per essere esente dal monitoraggio. Le risorse ignorate non vengono valutate per la sovrapposizione o la conformità alle regole di assegnazione. Una volta che una risorsa viene scelta per essere ignorata, qualsiasi spazio assegnato da un pool IPAM viene restituito al pool e la risorsa non verrà di nuovo importata tramite l'importazione automatica (se la regola di assegnazione dell'importazione automatica è impostata sul pool).
     - -: Questa risorsa non è uno dei tipi di risorse che IPAM è in grado di gestire.
   - Stato di conformità: Lo stato di conformità del CIDR.
     - Conforme: Una risorsa gestita è conforme alle regole di assegnazione del pool IPAM.
     - Non conforme: Il CIDR della risorsa non è conforme a una o più regole di assegnazione del pool IPAM.

       Example

       Se un VPC ha un CIDR che non soddisfa i parametri di lunghezza della maschera di rete del pool IPAM o se la risorsa non si trova nella stessa AWS regione del pool IPAM, verrà contrassegnata come non conforme.
     - Non gestita: La risorsa non ha un CIDR assegnato da un pool IPAM e non è monitorata da IPAM per la potenziale sovrapposizione CIDR e la conformità alle regole di assegnazione del pool. Il CIDR è monitorato per la sovrapposizione.
     - Ignorato: La risorsa è stata scelta per essere esente dal monitoraggio. Le risorse ignorate non vengono valutate per la sovrapposizione o la conformità alle regole di assegnazione. Una volta che una risorsa viene scelta per essere ignorata, qualsiasi spazio assegnato da un pool IPAM viene restituito al pool e la risorsa non verrà di

nuovo importata tramite l'importazione automatica (se la regola di assegnazione dell'importazione automatica è impostata sul pool).

- -: Questa risorsa non è uno dei tipi di risorse che IPAM è in grado di gestire.

- Stato di sovrapposizione: Lo stato di sovrapposizione del CIDR.
  - Non sovrapposto: Il CIDR della risorsa non si sovrappone a un altro CIDR nello stesso ambito.
  - Sovrapposto: Il CIDR della risorsa si sovrappone a un altro CIDR nello stesso ambito. Tieni presente che se un CIDR della risorsa si sovrappone, potrebbe sovrapporsi con un'assegnazione manuale.
  - Ignorato: La risorsa è stata scelta per essere esente dal monitoraggio. IPAM non valuta le risorse ignorate per la conformità alle regole di sovrapposizione o allocazione. Una volta che una risorsa viene scelta per essere ignorata, qualsiasi spazio assegnato da un pool IPAM viene restituito al pool e la risorsa non verrà di nuovo importata tramite l'importazione automatica (se la regola di assegnazione dell'importazione automatica è impostata sul pool).
  - -: Questa risorsa non è uno dei tipi di risorse che IPAM è in grado di gestire.
- IPs allocato: per le risorse che lo sono VPCs, questa è la percentuale di spazio degli indirizzi IP nel VPC occupata dalla sottorete. CIDRs Per le risorse che sono sottoreti, se alla sottorete è assegnato un IPv4 CIDR, questa è la percentuale di spazio degli IPv4 indirizzi nella sottorete in uso. Se alla sottorete è assegnato un IPv6 CIDR, la percentuale di spazio di indirizzi in uso non è rappresentata. IPv6 La percentuale di spazio degli IPv6 indirizzi in uso non può attualmente essere calcolata. Per le risorse che sono IPv4 pool pubblici, questa è la percentuale di spazio di indirizzi IP nel pool che è stata allocata agli indirizzi IP elastici (EIPs).
- Regione: la AWS regione della risorsa.
- ID proprietario: l'ID dell' AWS account della persona che ha creato questa risorsa.
- Tipo di risorsa: se la risorsa è un VPC, una sottorete, un indirizzo IP elastico o un pool pubblico. IPv4
- ID pool: ID del pool IPAM in cui si trova la risorsa.

7. Usa Filtra le risorse per filtrare la tabella delle risorse in base alla proprietà della colonna, come l'ID del VPC o lo stato di conformità.

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti AWS CLI comandi per monitorare l'utilizzo del CIDR per risorsa:

1. Ottieni l'ID dell'ambito: describe-ipam-scopes
2. Richiedi informazioni sulle risorse: get-ipam-resource-cidrs

Monitora l'IPAM con Amazon CloudWatch

IPAM memorizza automaticamente le metriche relative all'utilizzo degli indirizzi IP (come lo spazio degli indirizzi IP disponibile nei pool IPAM e il numero di risorse CIDRs conformi alle regole di allocazione) e all'utilizzo delle risorse nello spazio dei nomi `AWS/IPAM` CloudWatch Amazon nella regione di origine del tuo IPAM.

L'integrazione di IPAM con CloudWatch migliora la capacità di monitorare, analizzare e ottimizzare la gestione degli indirizzi IP all'interno. AWS

I casi d'uso includono:

- Monitoraggio delle tendenze di utilizzo degli indirizzi IP: CloudWatch può monitorare l'utilizzo del pool CIDR, l'allocazione degli ambiti e altre metriche IPAM, aiutandovi a identificare in modo proattivo i potenziali rischi di esaurimento degli indirizzi IP.
- Impostazione di avvisi basati sull'utilizzo: è possibile configurare CloudWatch allarmi per avvisare l'utente quando l'utilizzo del CIDR raggiunge soglie predeterminate, consentendo un intervento e un'ottimizzazione tempestivi.
- Monitoraggio degli eventi IPAM: CloudWatch può acquisire e analizzare gli eventi relativi all'IPAM, come allocazioni CIDR, deallocazioni e modifiche dell'ambito, fornendo visibilità sulle attività di gestione degli indirizzi IP.
- Generazione di dashboard personalizzate: combinando i dati IPAM con altre AWS metriche, è possibile creare dashboard complete per visualizzare e analizzare il panorama degli indirizzi IP insieme agli indicatori di infrastruttura e prestazioni correlati.

Indice

- Metriche IPAM
- Parametri di utilizzo delle risorse IPAM

Metriche IPAM

IPAM pubblica dati su IPAM, pool e ambiti su Amazon. CloudWatch È possibile utilizzare questi parametri per creare allarmi per i pool IPAM per notificare all'utente se i pool di indirizzi sono quasi esauriti o se le risorse non rispettano le regole di allocazione impostate su un pool. La creazione di allarmi e l'impostazione di notifiche con Amazon CloudWatch non rientrano nell'ambito di questa sezione. Per ulteriori informazioni, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

Le metriche e le dimensioni che IPAM invia ad Amazon CloudWatch sono elencate di seguito.

Metriche IPAM

Lo spazio dei nomi `AWS/IPAM` include le seguenti metriche IPAM.

Nome parametro	Descrizione
TotalActiveIpCount	Il numero totale di IP attivi è il numero di indirizzi IP attivi nel tuo IPAM che ti verranno addebitati se passi dal piano gratuito al livello avanzato. Un indirizzo IP attivo è definito come un indirizzo IP o un prefisso associato a un'interfaccia di rete elastica (ENI) collegata a una risorsa come un'istanza. EC2 • Questa metrica è disponibile solo per i clienti del piano gratuito. • Se il tuo IPAM è integrato con AWS Organizations, il conteggio IP attivo copre tutti gli account dell'organizzazione. • Non è possibile visualizzare una suddivisione del numero di IP attivi per tipo di IP (public/private) or class (IPv4/IPv6). • IPAM conta solo gli account IPs di ENIs proprietà degli account monitorati. Il conteggio potrebbe quindi essere impreciso a causa delle sottoreti condivise. Gli indirizzi IP sono esclusi se il proprietario della sottorete o dell'ENI non è coperto dall'IPAM.

Parametri del pool IPAM

Lo spazio dei nomi `AWS/IPAM` include le seguenti metriche dei pool per IPAM.

Nome parametro	Descrizione
CompliantResourceCidrs	Il numero di risorse gestite CIDRs conformi alle regole di allocazione del pool IPAM. Per ulteriori informazioni sulle regole di assegnazione, consulta Creare un pool di primo livello IPv4 .
NoncompliantResourceCidrs	Il numero di risorse gestite CIDRs che non sono conformi alle regole di allocazione del pool IPAM. Per ulteriori informazioni sulle regole di assegnazione, consulta Creare un pool di primo livello IPv4 .
PercentAllocated	La percentuale dello spazio IP di un pool allocato ad altri pool.
PercentAssigned	La percentuale dello spazio IP di un pool allocato alle risorse, incluse le allocazioni manuali.
PercentAvailable	La percentuale dello spazio IP di un pool non allocato ad altri pool o ad altre risorse.

Parametri dell'ambito IPAM

Lo spazio dei nomi `AWS/IPAM` include le seguenti metriche dell'ambito per IPAM.

Nome parametro	Descrizione
CompliantResourceCidrs	Il numero di risorse CIDRs conformi alle regole di allocazione per i pool IPAM nell'ambito.
ManagedResourceCidrs	Il numero di risorse CIDRs per risorse gestibili (VPCs o IPv4 pool pubblici) allocate da un pool IPAM nell'ambito.
NoncompliantResourceCidrs	Il numero di risorse CIDRs che non sono conformi alle regole di allocazione per i pool IPAM inclusi nell'ambito.

Nome parametro	Descrizione
OverlappingResourceCidrs	Il numero di risorse CIDRs che si sovrappongono nell'ambito.
UnmanagedResourceCidrs	Il numero di risorse CIDRs nell'ambito che sono attualmente associate a risorse gestibili ma non gestite da IPAM.

Metriche degli IP pubblici di IPAM

Lo spazio dei nomi `AWS/IPAM` include le seguenti metriche degli IP pubblici per IPAM.

Nome parametro	Descrizione
AmazonOwnedContigIPs	Il numero di indirizzi IP all'interno dei quali viene CIDRs fornito ai IPv4 pool pubblici contigui forniti da Amazon di proprietà dell'IPAM.
AllocatedAmazonOwnedContigIPs	Il numero di indirizzi IP che sono stati assegnati da un blocco CIDR del pool pubblico contiguo fornito da Amazon. IPv4
UnallocatedAmazonOwnedContigIPs	Il numero di indirizzi IP all'interno del blocco CIDR del IPv4 pool pubblico contiguo fornito da Amazon di proprietà dell'IPAM.
AssociatedAmazonOwnedContigIPs	Il numero di indirizzi IP elastici che sono stati allocati da un blocco CIDR di IPv4 pool pubblico contiguo fornito da Amazon e associato a un'interfaccia di rete elastica.
UnassociatedAmazonOwnedContigIPs	Il numero di indirizzi IP elastici che sono stati allocati da un blocco CIDR del IPv4 pool pubblico contiguo fornito da Amazon che non sono associati a un'interfaccia di rete elastica.

Dimensioni metrica

Per filtrare queste metriche IPAM, utilizza le seguenti dimensioni.

Dimensione	Descrizione
AddressFamily	La famiglia di indirizzi IP per la risorsa (o). CIDRs IPv4 IPv6
Locale	La AWS regione in cui è disponibile un pool IPAM per le allocazioni.
PoolID	L'ID di un pool.
ScopeID	L'ID di un ambito.

Per informazioni sul monitoraggio VPCs con Amazon CloudWatch, consulta i tuoi CloudWatch parametri VPCs nella Amazon Virtual Private Cloud User Guide.

Parametri di utilizzo delle risorse IPAM

IPAM pubblica su Amazon i parametri di utilizzo degli IP per le risorse monitorate dall'IPAM. CloudWatch Queste risorse includono:

- VPCs IPv4 IPv6(e)
- Sottoreti () IPv4
- Piscine pubbliche IPv4

IPAM calcola e pubblica le metriche di utilizzo degli IP separatamente per famiglia di indirizzi IP (o). IPv4 IPv6 L'utilizzo dell'IP di una risorsa viene calcolato su tutte le risorse della stessa famiglia di indirizzi CIDRs .

Per ogni tipo di risorsa e combinazione di famiglie di indirizzi, IPAM utilizza tre regole per determinare quali parametri pubblicare:

- Fino a 50 risorse con il massimo utilizzo IP. Puoi utilizzare queste informazioni per configurare gli allarmi e ricevere un avviso in caso di violazione di una soglia di utilizzo IP.
- Fino a 50 risorse con il minimo utilizzo IP. Puoi utilizzare queste informazioni per decidere se mantenere o eliminare le risorse sottoutilizzate.
- Fino a 50 altre risorse. Puoi utilizzare queste informazioni per tenere traccia in modo coerente dell'utilizzo IP delle risorse che potrebbero non essere comprese all'interno del gruppo ad alto o basso utilizzo.

- Fino a 50 VPCs contenenti un CIDR allocato da un pool IPAM (priorità in base alla dimensione totale dei blocchi CIDR).
- Fino a 50 sottoreti il cui VPC contiene un CIDR assegnato da un pool IPAM (con priorità in base alla dimensione totale dei blocchi CIDR).
- Fino a 50 IPv4 pool pubblici contenenti un CIDR allocato da un pool IPAM (con priorità in base alla dimensione totale dei blocchi CIDR).

Dopo aver applicato ogni regola, i parametri vengono aggregati e pubblicati con lo stesso nome parametro per ogni tipo di risorsa. Le informazioni dettagliate sui nomi parametri e sulle relative dimensioni sono fornite di seguito.

> **Important**
>
> Esiste un limite univoco per ogni tipo di risorsa, famiglia di indirizzi e combinazione di regole. Il valore predefinito di ogni limite è 50. È possibile modificare questi limiti contattando il AWS Support Center come descritto nelle quote di AWS servizio nel Riferimenti generali di AWS.

Example Esempio

Supponiamo che il tuo IPAM monitori 2.500 VPCs e 10.000 sottoreti, tutte con e. IPv4 IPv6 CIDRs IPAM pubblica i seguenti parametri di utilizzo IP:

- Fino a 150 parametri per l'utilizzo dell'IP IPv4 VPC, tra cui:
  - Le 50 VPCs con il più alto utilizzo dell'IP IPv4
  - I 50 VPCs con il minor utilizzo IPv4
  - Fino a 50 VPCs contenenti un IPv4 CIDR allocato da un pool IPAM
- Fino a 150 parametri per l'utilizzo del IPv6 VPC, tra cui:
  - Le 50 VPCs con il più alto utilizzo dell'IP IPv6
  - I 50 VPCs con il minor utilizzo IPv6
  - Fino a 50 VPCs contenenti un IPv6 CIDR allocato da un pool IPAM
- Fino a 150 parametri per l'utilizzo della IPv4 sottorete, tra cui:
  - Le 50 sottoreti con il massimo utilizzo dell'IP IPv4
  - Le 50 sottoreti con l'utilizzo IP più basso IPv4
  - Fino a 50 sottoreti il cui VPC contiene un IPv4 CIDR allocato da un pool IPAM

Parametri VPC

Il nome e la descrizione dei parametri VPC sono elencati di seguito.

Nome parametro	Descrizione
Vpc IPUsage	Il totale IPs coperto da CIDRs nelle sottoreti del VPC diviso per il totale IPs coperto dal VPC. CIDRs Questo viene calcolato su tutti i VPC CIDRs nello stesso ambito IPAM e separatamente per e. IPv4 IPv6 CIDRs

Di seguito sono elencate le dimensioni che puoi utilizzare per filtrare i parametri VPC.

Dimensione	Descrizione
AddressFamily	La famiglia di indirizzi IP per la risorsa CIDRs (IPv4 o IPv6).
OwnerID	L'ID del proprietario del VPC.
Regione	La AWS regione in cui si trova il VPC.
ScopeID	L'ID dell'ambito IPAM a cui appartiene il VPC.
VpcID	L'ID dell'VPC.

Parametri della sottorete

Il nome e la descrizione dei parametri della sottorete sono elencati di seguito.

Nome parametro	Descrizione
Sottorete IPUsage	Il numero di attivi IPs diviso per il totale IPs nel CIDR della sottorete. IPv4

Di seguito sono elencate le dimensioni che puoi utilizzare per filtrare i parametri della sottorete.

Dimensione	Descrizione
AddressFamily	La famiglia di indirizzi IP per la risorsa CIDRs (IPv4 solo).
OwnerID	L'ID del proprietario della sottorete.
Regione	La AWS regione in cui si trova la sottorete.
ScopeID	L'ID dell'ambito IPAM a cui appartiene la sottorete.
SubnetID	ID della sottorete.
VpcID	L'ID del VPC a cui appartiene la sottorete.

Metriche del IPv4 pool pubblico

Il nome e la descrizione della metrica del IPv4 pool pubblico sono elencati di seguito.

Nome parametro	Descrizione
Piscina pubblica IPv4 IPUsage	Il numero EIPs dei partecipanti alla IPv4 piscina pubblica diviso per il totale IPs del pool.

Le dimensioni che puoi utilizzare per filtrare le metriche del IPv4 pool pubblico sono elencate di seguito.

Dimensione	Descrizione
OwnerID	L'ID del proprietario del IPv4 pool pubblico.
ID della IPv4 piscina pubblica	L'ID del IPv4 pool pubblico.
Regione	La AWS regione in cui si trova la IPv4 piscina pubblica.
ScopeID	L'ID dell'ambito IPAM a cui appartiene il IPv4 pool pubblico.

Metriche di Informazioni sugli IP pubblici

I nomi e le descrizioni delle metriche di Informazioni sugli IP pubblici sono elencati di seguito.

Nome parametro	Descrizione
AmazonOwnedElasticIPs	Il numero di indirizzi IP elastici di proprietà di Amazon che hai fornito o assegnato alle risorse del tuo account. AWS
AssociatedAmazonOwnedElasticIPs	Il numero di indirizzi IP elastici di proprietà di Amazon che hai associato alle risorse del tuo AWS account.
AssociatedBringYourOwnIPs	Il numero di IPv4 indirizzi pubblici che hai AWS utilizzato Bring your own IP address (BYOIP) e che hai associato alle risorse del tuo account. AWS
BringYourOwnIPs	Il numero di IPv4 indirizzi pubblici che hai AWS utilizzato con Bring your own IP address (BYOIP).
EC2PubblicaIPs	Il numero di IPv4 indirizzi pubblici assegnati alle EC2 istanze quando le istanze sono state avviate in una sottorete predefinita o in una sottorete configurata per l'assegnazione automatica di un indirizzo pubblico. IPv4
ServiceManagedBringYourOwnIPs	Il numero di IPv4 indirizzi pubblici che hai portato a AWS utilizzare gli indirizzi Bring your own IP (BYOIP) forniti e gestiti da un servizio. AWS
ServiceManagedIPs	Il numero di IPv4 indirizzi pubblici forniti e gestiti da un servizio. AWS
UnassociatedAmazonOwnedElasticIPs	Il numero di indirizzi IP elastici di proprietà di Amazon che non hai associato alle risorse del tuo AWS account.
UnassociatedBringYourOwnIPs	Il numero di IPv4 indirizzi pubblici che hai AWS utilizzato con Bring your own IP address (BYOIP) e che non hai associato a nessuna risorsa del tuo account. AWS

Di seguito sono elencate le dimensioni che puoi utilizzare per filtrare le metriche di Informazioni sugli IP pubblici.

Dimensione	Descrizione
IpamId	L'ID dell'IPAM a cui appartiene l'indirizzo IP.
Regione	La AWS regione in cui si trova l'indirizzo IP pubblico.

Suggerimento rapido per la creazione di allarmi

Per creare rapidamente un CloudWatch allarme Amazon per risorse con un elevato utilizzo degli indirizzi IP, apri la CloudWatch console, scegli Metriche, Tutte le metriche, scegli la scheda Query, scegli il Namespace **`AWS/IPAM > VPC IP Usage Metrics`** oppure **`AWS/IPAM > Public IPv4 Pool IP Usage Metrics`** scegli il nome della metrica o **`MAX(VpcIPUsage) MAX(SubnetIPUsage)MAX(PublicIPv4PoolIPUsage)`**, e scegli Crea allarme. **`AWS/IPAM > Subnet IP Usage Metrics`** Per ulteriori informazioni, consulta Create allarmi sulle query di Metrics Insights nella Amazon CloudWatch User Guide.

Visualizzazione della cronologia degli indirizzi IP

Segui il passaggio descritto in questa sezione per visualizzare la cronologia di un indirizzo IP o di un CIDR in un ambito IPAM. È possibile utilizzare i dati cronologici per analizzare e verificare le policy di sicurezza e routing della rete. IPAM conserva automaticamente i dati di monitoraggio dell'indirizzo IP per un massimo di tre anni.

È possibile utilizzare i dati storici IP per cercare la modifica dello stato degli indirizzi IP o CIDRs per i seguenti tipi di risorse:

- VPCs
- Sottoreti VPC
- Indirizzi IP elastici
- EC2 istanze
- EC2 interfacce di rete collegate alle istanze

Important

Sebbene IPAM non monitori EC2 le istanze di Amazon o le interfacce di EC2 rete collegate alle istanze, puoi utilizzare la funzionalità di ricerca nella cronologia degli IP per cercare dati storici sull' EC2 istanza e sull'interfaccia di rete. CIDRs

Note

- Se si sposta una risorsa da un ambito IPAM a un altro, il registro della cronologia precedente termina e viene creato un nuovo registro della cronologia sotto il nuovo ambito. Per ulteriori informazioni, consulta Sposta il VPC CIDRs tra gli ambiti.
- Se elimini o trasferisci una risorsa su un AWS account non monitorato dal tuo IPAM, qualsiasi nuova cronologia relativa alla risorsa non sarà visibile e l'IPAM non monitorerà la risorsa. L'indirizzo IP della risorsa, tuttavia, sarà ancora ricercabile.
- Se tuCome integrare IPAM con account esterni alla tua organizzazione, il proprietario dell'IPAM, puoi visualizzare la cronologia degli indirizzi IP di tutte le risorse di CIDRs proprietà di tali account.

AWS Management Console

Per visualizzare la cronologia di un CIDR

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel riquadro di navigazione, scegli Cerca nella cronologia IP.
3. Inserisci un indirizzo IPv6 IP IPv4 o un CIDR. Deve trattarsi di un CIDR specifico per la risorsa.
4. Scegli un ID dell'ambito IPAM.
5. Scegli un intervallo di data/ora.
6. Se si desidera filtrare i risultati per VPC, immettere un ID VPC. Utilizzate questa opzione se il CIDR appare multiplo. VPCs
7. Selezionare Search (Cerca).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Visualizza la cronologia di un CIDR: get-ipam-address-history

Per vedere esempi di come è possibile utilizzare il AWS CLI per analizzare e controllare l'utilizzo degli indirizzi IP, vedere Tutorial: Visualizza la cronologia degli indirizzi IP utilizzando il AWS CLI.

I risultati della ricerca sono organizzati nelle seguenti colonne:

- Ora di fine campionata: ora di fine campionata dell' resource-to-CIDRassociazione nell'ambito IPAM. Le modifiche vengono rilevate in snapshot periodici, quindi l'orario di fine potrebbe essersi verificato prima di questo orario specifico.
- Ora di inizio campionata: ora di inizio campionata dell' resource-to-CIDRassociazione nell'ambito IPAM. Le modifiche vengono rilevate in snapshot periodici, quindi l'orario di inizio potrebbe essersi verificato prima di questo orario specifico.

  Example

  Per aiutarti a comprendere gli orari visualizzati in Orario di inizio campionato e Orario di fine campionato, diamo un'occhiata a un caso d'uso esemplificativo:

  Alle 14:00 è stato creato un VPC con CIDR 10.0.0.0/16. Alle 15:00, crei un pool IPAM e IPAM con CIDR 10.0.0.0/8 e selezioni l'opzione di importazione automatica per consentire a IPAM di rilevare e importare quelli che rientrano nell'intervallo di indirizzi IP 10.0.0.0/8. CIDRs Poiché IPAM rileva le modifiche apportate alle CIDRs istantanee periodiche, non rileva il CIDR VPC esistente fino alle 15:05. Quando cerchi l'ID di questo VPC utilizzando la funzione Cerca nella cronologia IP, l'Ora di inizio campionata per il VPC è 15:05, ovvero il momento in cui è stato rilevato da IPAM, non 14:00, ovvero il momento in cui è stato creato il VPC. Ora, supponiamo che si decida di eliminare il VPC alle 17:00. Quando il VPC viene eliminato, il CIDR 10.0.0.0/16 assegnato al VPC viene riciclato di nuovo nel pool IPAM. IPAM acquisisce lo snapshot periodico alle 17:05 e rileva il cambiamento. Quando cerchi l'ID di questo VPC in Cerca nella cronologia IP, l'Ora di fine di campionamento per il CIDR del VPC è 17:05, non 17:00, ovvero il momento in cui il VPC è stato eliminato.
- ID risorsa: L'ID generato quando la risorsa è stata associata al CIDR.

- Nome:: Il nome della risorsa (se applicabile).
- Stato di conformità: Lo stato di conformità del CIDR.
  - Conforme: Una risorsa gestita è conforme alle regole di assegnazione del pool IPAM.
  - Non conforme: Il CIDR della risorsa non è conforme a una o più regole di assegnazione del pool IPAM.

    Example

    Se un VPC ha un CIDR che non soddisfa i parametri di lunghezza della maschera di rete del pool IPAM o se la risorsa non si trova nella stessa AWS regione del pool IPAM, verrà contrassegnata come non conforme.
  - Non gestita: La risorsa non ha un CIDR assegnato da un pool IPAM e non è monitorata da IPAM per la potenziale sovrapposizione CIDR e la conformità alle regole di assegnazione del pool. Il CIDR è monitorato per la sovrapposizione.
  - Ignorata: La risorsa gestita è stata scelta per essere esente dal monitoraggio. Le risorse ignorate non vengono valutate per la sovrapposizione o la conformità alle regole di assegnazione. Una volta che una risorsa viene scelta per essere ignorata, qualsiasi spazio assegnato da un pool IPAM viene restituito al pool e la risorsa non verrà di nuovo importata tramite l'importazione automatica (se la regola di assegnazione dell'importazione automatica è impostata sul pool).
  - -: Questa risorsa non è uno dei tipi di risorse che IPAM è in grado di monitorare o gestire.
- Stato di sovrapposizione: Lo stato di sovrapposizione del CIDR.
  - Non sovrapposto: Il CIDR della risorsa non si sovrappone a un altro CIDR nello stesso ambito.
  - Sovrapposto: Il CIDR della risorsa si sovrappone a un altro CIDR nello stesso ambito. Tieni presente che se un CIDR della risorsa si sovrappone, potrebbe sovrapporsi con un'assegnazione manuale.
  - Ignorata: La risorsa gestita è stata scelta per essere esente dal monitoraggio. IPAM non valuta le risorse ignorate per la conformità alle regole di sovrapposizione o allocazione. Una volta che una risorsa viene scelta per essere ignorata, qualsiasi spazio assegnato da un pool IPAM viene restituito al pool e la risorsa non verrà di nuovo importata tramite l'importazione automatica (se la regola di assegnazione dell'importazione automatica è impostata sul pool).
  - -: Questa risorsa non è uno dei tipi di risorse che IPAM è in grado di monitorare o gestire.
- Tipo di risorsa
  - vpc: Il CIDR è associato a un VPC.
  - sottorete: Il CIDR è associato a una sottorete VPC.

  - eip: Il CIDR è associato a un indirizzo IP elastico.
  - istanza: Il CIDR è associato a un'istanza. EC2
  - rete-interfaccia: Il CIDR associato a un'interfaccia di rete.
- ID VPC: l'ID del VPC a cui appartiene la risorsa (se applicabile).
- Regione: la AWS regione di questa risorsa.
- ID proprietario: l'ID dell' AWS account dell'utente che ha creato questa risorsa (se applicabile).

Visualizzazione di informazioni dettagliate relative agli indirizzi IP pubblici

Puoi utilizzare Informazioni sugli IP pubblici per vedere quanto segue:

- Se il tuo IPAM è integrato con gli account di un' AWS organizzazione, puoi visualizzare tutti IPv4 gli indirizzi pubblici utilizzati dai servizi in tutte le AWS regioni per l'intera AWS organizzazione.
- Se il tuo IPAM è integrato con un singolo account, puoi visualizzare tutti gli IPv4 indirizzi pubblici utilizzati dai servizi in tutte le AWS regioni nel tuo account.

Un IPv4 indirizzo pubblico è un IPv4 indirizzo indirizzabile da Internet. Un IPv4 indirizzo pubblico è necessario affinché una risorsa sia direttamente raggiungibile da Internet tramite Internet. IPv4

> **Note**
>
> AWS costi per tutti gli IPv4 indirizzi pubblici, compresi gli IPv4 indirizzi pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda IPv4 Indirizzo pubblico nella pagina dei prezzi di Amazon VPC.

Puoi visualizzare informazioni dettagliate sui seguenti tipi di IPv4 indirizzi pubblici:

- Indirizzi IP elastici (EIPs): IPv4 indirizzi pubblici statici forniti da Amazon che puoi associare a un' EC2 istanza, un'interfaccia di rete elastica o una AWS risorsa.
- EC2 IPv4 indirizzi pubblici: IPv4 indirizzi pubblici assegnati a un' EC2 istanza da Amazon (se l' EC2 istanza viene avviata in una sottorete predefinita o se l'istanza viene avviata in una sottorete configurata per assegnare automaticamente un indirizzo pubblico IPv4).

- BYOIPv4 indirizzi: IPv4 indirizzi pubblici compresi nell'intervallo di IPv4 indirizzi che hai introdotto AWS utilizzando Bring your own IP address (BYOIP).
- IPv4 Indirizzi gestiti dal servizio: IPv4 indirizzi pubblici assegnati automaticamente AWS alle risorse e gestiti da un servizio. AWS Ad esempio, IPv4 indirizzi pubblici su Amazon ECS, Amazon RDS o Amazon. WorkSpaces

Public IP Insights mostra tutti gli IPv4 indirizzi pubblici utilizzati dai servizi in tutte le regioni. Puoi utilizzare queste informazioni per identificare l'utilizzo degli IPv4 indirizzi pubblici e visualizzare i consigli per rilasciare indirizzi IP elastici non utilizzati.

- Tipi di IP pubblici: il numero di IPv4 indirizzi pubblici organizzati per tipo.
  - Di proprietà di Amazon EIPs: indirizzi IP elastici che hai fornito o assegnato alle risorse del tuo account. AWS
  - EC2 public IPs: IPv4 indirizzi pubblici assegnati alle EC2 istanze quando le istanze sono state avviate in una sottorete predefinita o in una sottorete configurata per assegnare automaticamente un indirizzo pubblico. IPv4
  - BYOIP: IPv4 indirizzi pubblici che hai portato a AWS utilizzare Bring your own IP address (BYOIP).
  - Servizio gestito IPs: IPv4 indirizzi pubblici forniti e gestiti da un servizio. AWS
  - Servizio gestito da YOIP: IPv4 indirizzi pubblici trasferiti AWS e gestiti da un servizio. AWS
  - Contigui di proprietà di Amazon EIPs: indirizzi IP elastici allocati da un pool IPAM pubblico contiguo fornito da Amazon. IPv4
- Utilizzo EIP: numero di indirizzi IP elastici organizzati in base al loro utilizzo.
  - Di proprietà di Amazon associati EIPs: indirizzi IP elastici che hai fornito nel tuo AWS account e che hai associato a un' EC2 istanza, un'interfaccia di rete o una risorsa. AWS
  - BYOIP associato: IPv4 indirizzi pubblici che hai portato a AWS utilizzare BYOIP e che hai associato a un'interfaccia di rete.
  - Non di proprietà di Amazon EIPs: indirizzi IP elastici che hai fornito nel tuo AWS account ma che non hai associato a un'interfaccia di rete.
  - BYOIP non associato: IPv4 indirizzi pubblici che hai AWS utilizzato BYOIP ma che non hai associato a un'interfaccia di rete.
  - Contigui associati di proprietà di Amazon EIPs: indirizzi IP elastici allocati da un pool IPAM pubblico contiguo fornito da Amazon e associati a una risorsa. IPv4

    - Contigui non associati di proprietà di Amazon EIPs: indirizzi IP elastici allocati da un pool IPAM pubblico contiguo fornito da Amazon e non associati a una risorsa. IPv4
- Utilizzo IPv4 contiguo di proprietà di Amazon: una tabella che mostra IPs l'utilizzo contiguo degli IPv4 indirizzi pubblici nel tempo e i relativi pool IPAM di proprietà di Amazon. IPv4
- Indirizzi IP pubblici: tabella di indirizzi pubblici e relativi attributi. IPv4
    - Indirizzo IP: l' IPv4 indirizzo pubblico.
    - Associato: se l'indirizzo è associato o meno a un' EC2 istanza, un'interfaccia di rete o una AWS risorsa.
        - Associato: l' IPv4 indirizzo pubblico è associato a un' EC2 istanza, un'interfaccia di rete o AWS una risorsa.
        - Non associato: l' IPv4 indirizzo pubblico non è associato a nessuna risorsa ed è inattivo nel tuo AWS account.
    - Tipo di indirizzo: il tipo di indirizzo IP.
        - EIP di proprietà di Amazon: l' IPv4 indirizzo pubblico è un indirizzo IP elastico.
        - BYOIP: l'indirizzo pubblico è stato portato a utilizzare IPv4 BYOIP. AWS
        - EC2 IP pubblico: l' IPv4 indirizzo pubblico è stato assegnato automaticamente a un'istanza. EC2
        - Servizio gestito BYOIP: l' IPv4 indirizzo pubblico è stato impostato su Bring AWS your own IP (BYOIP).
        - IP gestito dal servizio: l' IPv4 indirizzo pubblico è stato fornito ed è gestito da un servizio. AWS
    - Servizio: il servizio a cui è associato l'indirizzo IP.
        - AGA: Un AWS Global Accelerator. Se viene utilizzato un acceleratore di routing personalizzato, i relativi dati pubblici non IPs sono elencati. Per visualizzarli pubblici IPs, vedi Visualizzazione degli acceleratori di routing personalizzati.
        - Database Migration Service: un' AWS Database Migration Service istanza di replica (DMS).
        - Redshift: un cluster Amazon Redshift.
        - RDS: un'istanza Amazon Relational Database Service (RDS).
        - Load balancer (EC2): Application Load Balancer o Network Load Balancer.
        - Gateway NAT (VPC): Un gateway NAT pubblico Amazon VPC.
        - Site-to-Site VPN: un gateway privato AWS Site-to-Site VPN virtuale.
        - Altro: altro servizio attualmente non identificabile.

- Nome (ID EIP): se questo IPv4 indirizzo pubblico è un'allocazione di indirizzi IP elastica, si tratta del nome e dell'ID dell'allocazione EIP.
- ID dell'interfaccia di rete: se questo IPv4 indirizzo pubblico è associato a un'interfaccia di rete, questo è l'ID dell'interfaccia di rete.
- ID istanza: se questo IPv4 indirizzo pubblico è associato a un' EC2 istanza, questo è l'ID dell'istanza.
- Gruppi di sicurezza: se questo IPv4 indirizzo pubblico è associato a un' EC2 istanza, si tratta del nome e dell'ID del gruppo di sicurezza assegnato all'istanza.
- IPv4 Pool pubblico: se si tratta di un indirizzo IP elastico proveniente da un pool di indirizzi IP di proprietà e gestito da Amazon, il valore è «-». Se si tratta di un indirizzo IP elastico appartenente a un intervallo di indirizzi IP di tua proprietà e che hai trasferito ad Amazon (utilizzando BYOIP), il valore è l'ID del IPv4 pool pubblico.
- Gruppo di confine di rete: se l'indirizzo IP è pubblicizzato, questa è la AWS regione da cui viene pubblicizzato l'indirizzo IP.
- ID del proprietario: il AWS numero di account del proprietario della risorsa.
- Sample time (Tempo campionamento): l'ultima volta in cui il rilevamento delle risorse è riuscito.
- ID di scoperta della risorsa: ID della scoperta della risorsa che ha scoperto questo indirizzo pubblico IPv4 .
- Service resource (Risorsa del servizio): ARN o ID della risorsa.

Se un indirizzo IP elastico è assegnato al tuo account ma non è associato a un'interfaccia di rete, viene visualizzato un banner che ti informa che non sei associato al EIPs tuo account e che dovresti rilasciarlo.

> **Important**
>
> L'aggiornamento di Informazioni sugli IP pubblici è avvenuto recentemente.
> Se visualizzi un errore relativo alla mancanza delle autorizzazioni di chiamata GetIpamDiscoveredPublicAddresses, è necessario aggiornare l'autorizzazione gestita associata a un rilevamento di risorse che è stata condivisa con te. Contatta la persona che ha creato il rilevamento delle risorse e chiedile di aggiornare l'autorizzazione gestita `AWSRAMPermissionIpamResourceDiscovery` alla versione predefinita. Per ulteriori informazioni, consulta Creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM .

AWS Management Console

Per visualizzare le informazioni dettagliate relative agli indirizzi IP pubblici

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, scegli Public IP insights.
3. Per visualizzare i dettagli di un indirizzo IP pubblico, selezionalo facendo clic su di esso.
4. Visualizza le seguenti informazioni relative all'indirizzo IP:

   - Dettagli: le stesse informazioni visibili nelle colonne del riquadro principale di Public IP Insights, ad esempio Tipo di indirizzo e Servizio.
   - Regole del gruppo di sicurezza in entrata: se questo indirizzo IP è associato a un' EC2 istanza, queste sono le regole del gruppo di sicurezza che controllano il traffico in entrata verso l'istanza.
   - Regole del gruppo di sicurezza in uscita: se questo indirizzo IP è associato a un' EC2 istanza, queste sono le regole del gruppo di sicurezza che controllano il traffico in uscita dall'istanza.
   - Tag: coppie di chiavi e valori che fungono da metadati per l'organizzazione delle risorse. AWS

Command line

Usa il seguente comando per ottenere gli indirizzi IP pubblici che sono stati scoperti da IPAM: - addresses get-ipam-discovered-public

Tutorial per Amazon VPC IP Address Manager

I seguenti tutorial mostrano come eseguire attività IPAM comuni utilizzando la CLI. AWS Per ottenere il, vedi. AWS CLIAccedi a IPAM Per ulteriori informazioni sui concetti IPAM menzionati in questi tutorial, consulta Funzionamento di IPAM.

Indice

- Guida introduttiva a IPAM utilizzando la CLI AWS
- Tutorial: Creazione di IPAM e pool utilizzando la console
- Tutorial: creare un IPAM e pool utilizzando il AWS CLI
- Tutorial: Visualizza la cronologia degli indirizzi IP utilizzando il AWS CLI
- Tutorial: Porta il tuo ASN in IPAM
- Tutorial: trasferisci i tuoi indirizzi IP su IPAM
- Tutorial: trasferimento di un IPv4 CIDR BYOIP a IPAM
- Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti
- Assegna indirizzi IP elastici sequenziali da un pool IPAM

Guida introduttiva a IPAM utilizzando la CLI AWS

Questo tutorial ti guida attraverso il processo di configurazione e utilizzo di Amazon VPC IP Address Manager (IPAM) con la AWS CLI utilizzando un unico account. AWS Alla fine di questo tutorial, avrai creato un IPAM, creato una gerarchia di pool di indirizzi IP e assegnato un CIDR a un VPC.

Prerequisiti

Prima di iniziare questo tutorial, assicurati di avere:

- Un AWS account con le autorizzazioni per creare e gestire risorse IPAM.
- La AWS CLI è stata installata e configurata con le credenziali appropriate. Per informazioni sull'installazione della AWS CLI, consulta Installazione o aggiornamento della versione più recente della AWS CLI. Per informazioni sulla configurazione della AWS CLI, consulta Nozioni di base sulla configurazione.
- Conoscenza di base dell'indirizzamento IP e della notazione CIDR.
- Conoscenza di base dei concetti di Amazon VPC.

- Circa 30 minuti per completare il tutorial.

Crea un IPAM

Il primo passo è creare un IPAM con regioni operative. Un IPAM ti aiuta a pianificare, tracciare e monitorare gli indirizzi IP per i tuoi AWS carichi di lavoro.

Crea un IPAM con regioni operative in us-east-1 e us-west-2:

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

Questo comando crea un IPAM e gli consente di gestire gli indirizzi IP nelle regioni specificate. Le regioni operative sono le AWS regioni in cui l'IPAM è autorizzato a gestire l'indirizzo IP. CIDRs

Verifica che il tuo IPAM sia stato creato:

```
aws ec2 describe-ipams
```

Prendi nota dell'ID IPAM dall'output, poiché ti servirà per i passaggi successivi.

Attendi che l'IPAM sia completamente creato e disponibile (circa 20 secondi):

```
sleep 20
```

Ottieni l'ID dell'ambito IPAM

Quando crei un IPAM, crea AWS automaticamente un ambito privato e uno pubblico. Per questo tutorial, useremo l'ambito privato.

Recupera i dettagli IPAM ed estrai l'ID dell'ambito privato:

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

`ipam-0abcd1234`Sostituiscilo con il tuo ID IPAM effettivo.

Dall'output, identifica e annota l'ID dell'ambito privato dal `PrivateDefaultScopeId` campo. L'aspetto sarà simile a `ipam-scope-0abcd1234`.

Crea un pool di primo livello IPv4

Ora, creiamo un pool di primo livello nell'ambito privato. Questo pool fungerà da genitore per tutti gli altri pool della nostra gerarchia.

Crea un pool di primo livello IPv4 :

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

`ipam-scope-0abcd1234`Sostituiscilo con il tuo ID effettivo dell'ambito privato.

Attendi che il pool sia completamente creato e disponibile:

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

`ipam-pool-0abcd1234`Sostituiscilo con l'effettivo ID del pool di primo livello. Lo stato dovrebbe essere `create-complete` prima di procedere.

Una volta che il pool è disponibile, esegui il provisioning di un blocco CIDR:

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

Attendi che il CIDR sia completamente fornito:

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

Lo stato dovrebbe essere `provisioned` prima di procedere.

Crea un pool regionale IPv4

Quindi, crea un pool regionale all'interno del pool di primo livello. Questo pool sarà specifico per una particolare AWS regione.

Crea un IPv4 pool regionale:

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

Sostituiscilo `ipam-scope-0abcd1234` con l'ID dell'ambito privato effettivo e `ipam-pool-0abcd1234` con l'ID del pool di primo livello.

Attendi che il pool regionale sia completamente creato e disponibile:

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

Sostituiscilo `ipam-pool-1abcd1234` con l'ID effettivo del pool regionale. Lo stato dovrebbe esserlo `create-complete` prima di procedere.

Una volta che il pool è disponibile, esegui il provisioning di un blocco CIDR:

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

Attendi che il CIDR sia completamente fornito:

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

Lo stato dovrebbe essere `provisioned` prima di procedere.

Crea un pool di sviluppo IPv4

Ora, crea un pool di sviluppo all'interno del pool regionale. Questo pool verrà utilizzato per ambienti di sviluppo.

Crea un IPv4 pool di sviluppo:

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

Sostituiscilo `ipam-scope-0abcd1234` con l'ID dell'ambito privato effettivo e `ipam-pool-1abcd1234` con l'ID del pool regionale.

Nota: è importante includere il `--locale` parametro in modo che corrisponda alle impostazioni locali del pool principale.

Attendi che il pool di sviluppo sia completamente creato e disponibile:

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

`ipam-pool-2abcd1234`Sostituiscilo con l'ID effettivo del pool di sviluppo. Lo stato dovrebbe essere `create-complete` prima di procedere.

Una volta che il pool è disponibile, esegui il provisioning di un blocco CIDR:

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

Attendi che il CIDR sia completamente fornito:

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

Lo stato dovrebbe essere `provisioned` prima di procedere.

Creare un VPC utilizzando un pool IPAM CIDR

Infine, crea un VPC che utilizzi un CIDR dal tuo pool IPAM. Questo dimostra come l'IPAM può essere utilizzato per allocare lo spazio degli indirizzi IP alle risorse. AWS

Crea un VPC utilizzando un pool IPAM CIDR:

```
aws ec2 create-vpc \
  --ipv4-ipam-pool-id ipam-pool-2abcd1234 \
  --ipv4-netmask-length 26 \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=IPAM-VPC}]'
```

`ipam-pool-2abcd1234`Sostituiscilo con l'ID effettivo del pool di sviluppo.

Il `--ipv4-netmask-length 26` parametro specifica che si desidera che un blocco CIDR /26 (64 indirizzi IP) venga allocato dal pool. Questa lunghezza della netmask viene scelta per garantire che sia inferiore al blocco CIDR del pool (/24).

Verifica che il tuo VPC sia stato creato:

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

Verifica l'allocazione del pool IPAM

Verifica che il CIDR sia stato allocato dal tuo pool IPAM:

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

`ipam-pool-2abcd1234`Sostituiscilo con l'ID effettivo del pool di sviluppo.

Questo comando mostra tutte le allocazioni dal pool IPAM specificato, incluso il VPC appena creato.

Risoluzione dei problemi

Ecco alcuni problemi comuni che potresti riscontrare quando lavori con IPAM:

- Errori di autorizzazione: assicurati che il tuo utente o ruolo IAM disponga delle autorizzazioni necessarie per creare e gestire le risorse IPAM. Potresti aver bisogno delle `ec2:CreateIpam` autorizzazioni e di altre autorizzazioni correlate. `ec2:CreateIpamPool`
- Limite di risorse superato: per impostazione predefinita, puoi creare un solo IPAM per account. Se hai già un IPAM, dovrai eliminarlo prima di crearne uno nuovo o utilizzare quello esistente.
- Errori di allocazione CIDR: durante il provisioning CIDRs ai pool, assicurati che il CIDR che stai cercando di fornire non si sovrapponga alle allocazioni esistenti in altri pool.

- Timeout delle richieste API: se riscontri errori "RequestExpired", ciò potrebbe essere dovuto a problemi di latenza di rete o di sincronizzazione dell'ora. Prova di nuovo il comando.
- Errori di stato errati: se ricevi errori IncorrectState "", è possibile che tu stia tentando di eseguire un'operazione su una risorsa che non si trova nello stato corretto. Attendi che la risorsa sia completamente creata o fornita prima di procedere.
- Errori relativi alle dimensioni dell'allocazione: se ricevi errori "InvalidParameterValue" sulla dimensione dell'allocazione, assicurati che la lunghezza della maschera di rete richiesta sia appropriata per la dimensione del pool. Ad esempio, non è possibile allocare un CIDR /25 da un pool /24.
- Violazioni delle dipendenze: durante la pulizia delle risorse, è possibile che si verifichino errori "». DependencyViolation Questo perché le risorse dipendono l'una dall'altra. Assicurati di eliminare le risorse nell'ordine inverso rispetto alla creazione e al deprovisioning CIDRs prima di eliminare i pool.

Pulizia delle risorse

Quando hai finito con questo tutorial, dovresti ripulire le risorse che hai creato per evitare di incorrere in costi inutili.

1. Eliminare il VPC

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

2. Estraete il CIDR dal pool di sviluppo:

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

3. Elimina il pool di sviluppo:

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

4. Estraete il CIDR dal pool regionale:

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

5. Eliminare il pool regionale:

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

6. Estraete il CIDR dal pool di primo livello:

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

7. Elimina il pool di primo livello:

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

8. Eliminare l'IPAM:

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

Sostituisci tutto IDs con la tua risorsa IDs effettiva.

> **Note**
>
> Potrebbe essere necessario attendere tra queste operazioni per consentire l'eliminazione completa delle risorse prima di procedere al passaggio successivo. Se riscontri violazioni delle dipendenze, attendi qualche secondo e riprova.

Passaggi successivi

Ora che hai imparato a creare e utilizzare IPAM con la AWS CLI, potresti voler esplorare funzionalità più avanzate:

- Pianificare il provisioning degli indirizzi IP— Scopri come pianificare efficacemente lo spazio degli indirizzi IP
- Monitoraggio dell'utilizzo del CIDR per risorsa— Scopri come monitorare l'utilizzo degli indirizzi IP
- Condivisione di un pool IPAM tramite AWS RAM— Scopri come condividere i pool IPAM tra più account AWS
- Integrare IPAM con gli account di un'organizzazione AWS— Scopri come utilizzare IPAM nella tua organizzazione

Tutorial: Creazione di IPAM e pool utilizzando la console

In questo tutorial, crei un IPAM, esegui l'integrazione AWS Organizations, crei pool di indirizzi IP e crei un VPC con un CIDR da un pool IPAM.

Questo tutorial mostra come utilizzare IPAM per organizzare lo spazio degli indirizzi IP in base alle diverse esigenze di sviluppo. Una volta completato questo tutorial, avrai a disposizione un pool di indirizzi IP per le risorse di pre-produzione. A questo punto, potrai creare altri pool in base alle tue esigenze di routing e sicurezza, ad esempio un pool per le risorse di produzione.

Sebbene sia possibile utilizzare IPAM come singolo utente, l'integrazione con AWS Organizations consente di gestire gli indirizzi IP tra gli account dell'organizzazione. In questo tutorial viene illustrata l'integrazione di IPAM con gli account in un'organizzazione. Non spiega come Come integrare IPAM con account esterni alla tua organizzazione.

> **Note**
>
> Ai fini di questo tutorial, le istruzioni ti diranno di denominare le risorse IPAM in un modo particolare, creare risorse IPAM in Regioni specifiche e utilizzare intervalli CIDR di indirizzi IP specifici per i tuoi pool. Lo scopo è quello di semplificare le scelte disponibili in IPAM e di iniziare rapidamente a utilizzare IPAM. Una volta completato questo tutorial, puoi anche decidere di creare un nuovo IPAM e di configurarlo diversamente.

Indice

- Prerequisiti
- Come si AWS Organizations integra con IPAM
- Fase 1: delega di un amministratore IPAM
- Passaggio 2: creazione di un IPAM
- Passaggio 3: creazione di un pool IPAM di livello superiore
- Fase 4: creazione di pool IPAM regionali
- Fase 5: creazione di un pool di sviluppo di pre-produzione
- Fase 6: condivisione del pool IPAM
- Fase 7: creazione di un VPC con un CIDR assegnato da un pool IPAM
- Fase 8: eliminazione

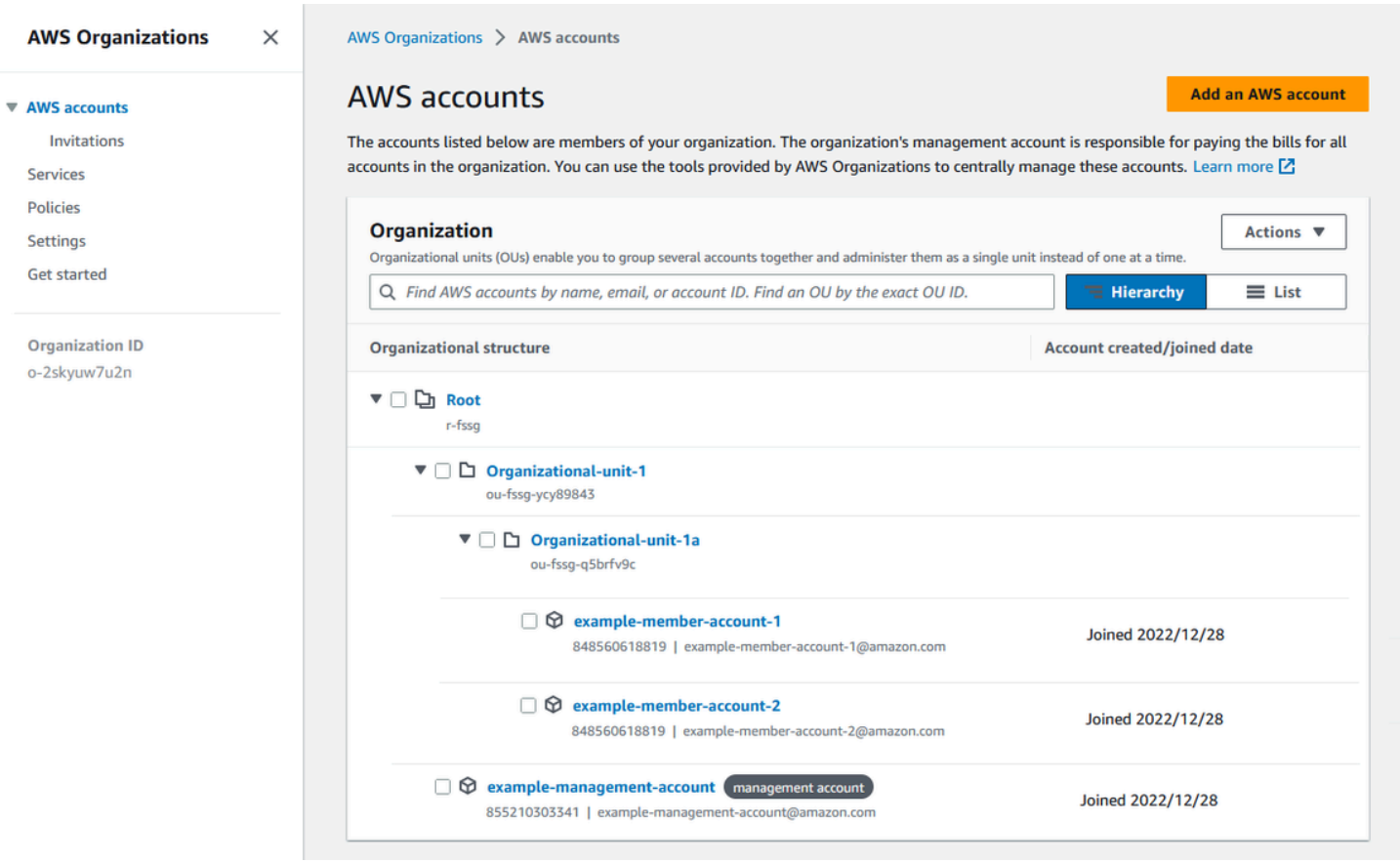
Prerequisiti

Prima di iniziare, devi aver creato un AWS Organizations account con almeno un account membro. Per istruzioni, consulta Creazione e configurazione di un'organizzazione nella Guida per l'utente di AWS Organizations .

Come si AWS Organizations integra con IPAM

Questa sezione mostra un esempio degli AWS Organizations account utilizzati in questo tutorial. Nella tua organizzazione esistono tre account che utilizzi quando effettui l'integrazione con IPAM in questo tutorial:

- L'account di gestione (chiamato example-management-accountnell'immagine seguente) per accedere alla console IPAM e delegare un amministratore IPAM. Non è possibile utilizzare l'account di gestione dell'organizzazione come amministratore di IPAM.
- Un account membro (chiamato example-member-account-1 nell'immagine seguente) come account amministratore IPAM. L'account amministratore di IPAM è responsabile della creazione e dell'utilizzo di un IPAM per gestire e monitorare l'uso dell'indirizzo IP nell'organizzazione. Qualsiasi account membro dell'organizzazione può essere delegato come amministratore di IPAM.
- Un account membro (chiamato example-member-account-2 nel seguito riportato sopra) come account sviluppatore. Questo account crea un VPC con un CIDR assegnato da un pool IPAM.



Oltre agli account, avrai bisogno dell'ID dell'unità organizzativa (ou-fssg-q5brfv9c nell'immagine precedente) che contiene l'account membro che utilizzerai come account sviluppatore. È necessario questo ID in modo che, in una fase successiva, quando si condivide il pool IPAM, sia possibile condividerlo con questa unità organizzativa.

> **Note**
>
> Per ulteriori informazioni sui tipi di account come gli AWS Organizations account di gestione e gli account dei membri, consulta la terminologia e i concetti.AWS Organizations

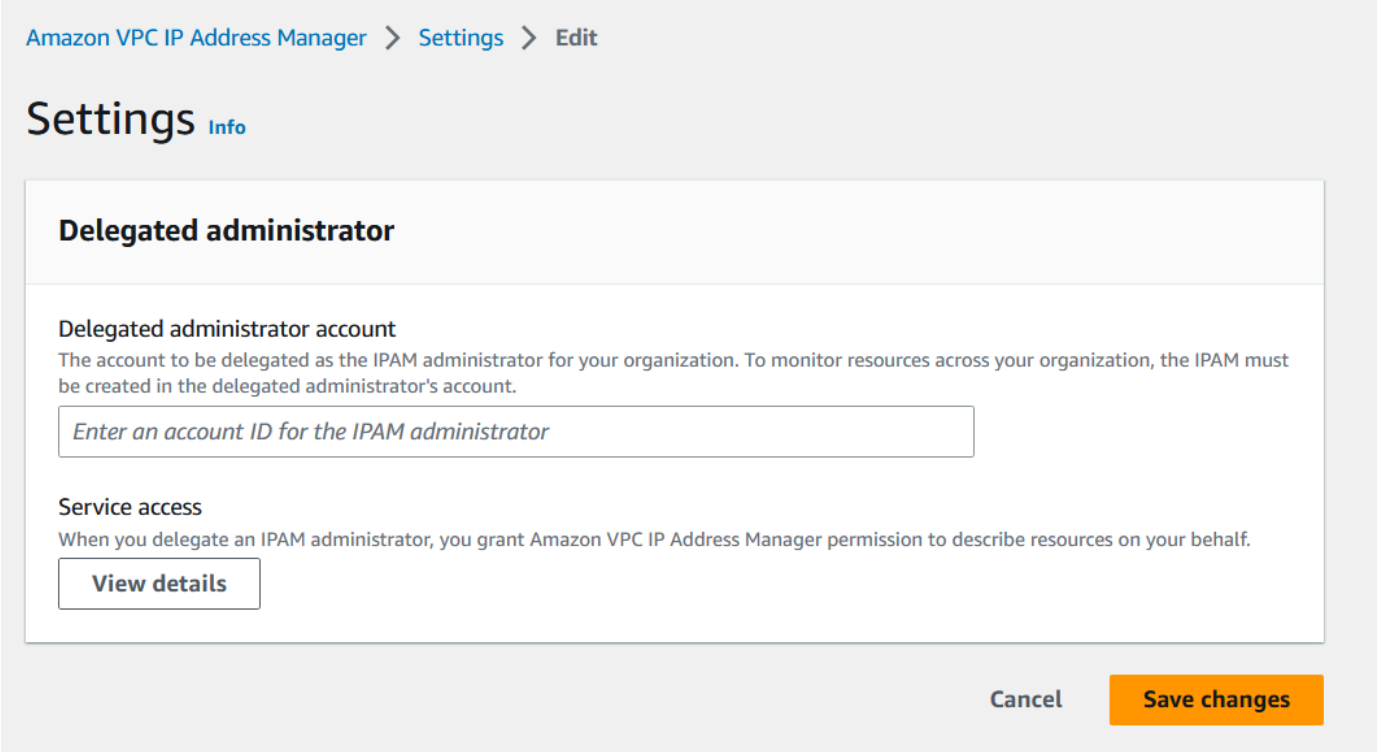
Fase 1: delega di un amministratore IPAM

In questo passaggio, delegherai un account AWS Organizations membro come amministratore IPAM. Quando deleghi un amministratore IPAM, viene creato automaticamente un ruolo collegato al servizio in ciascuno dei tuoi account membro. AWS Organizations IPAM monitora l'utilizzo dell'indirizzo IP in questi account assumendo il ruolo collegato al servizio in ciascun account membro. Può quindi scoprire le risorse e le relative CIDRs indipendentemente dalla relativa unità organizzativa.

Non è possibile completare questo passaggio se non si dispone delle autorizzazioni richieste AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Integrare IPAM con gli account di un'organizzazione AWS.

Per delegare un account amministratore IPAM

1. Utilizzando l'account AWS Organizations di gestione, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. In AWS Management Console, scegli la AWS regione in cui desideri lavorare con IPAM.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione).
4. Scegli Delega. L'opzione Delega è disponibile solo se hai effettuato l'accesso alla console come account di gestione. AWS Organizations
5. Inserisci l'ID dell' AWS account per un account membro dell'organizzazione. L'amministratore IPAM deve essere un account AWS Organizations membro, non l'account di gestione.



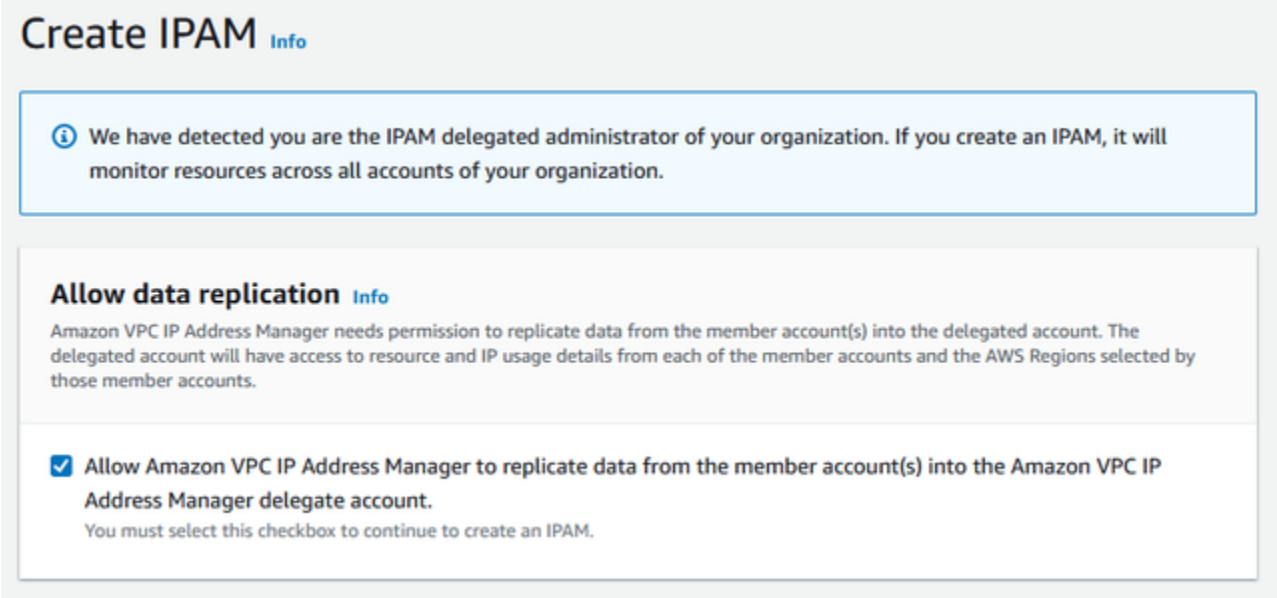
6. Scegli Save changes (Salva modifiche). Le informazioni sull'amministratore delegato sono compilate con i dettagli relativi all'account membro.

Passaggio 2: creazione di un IPAM

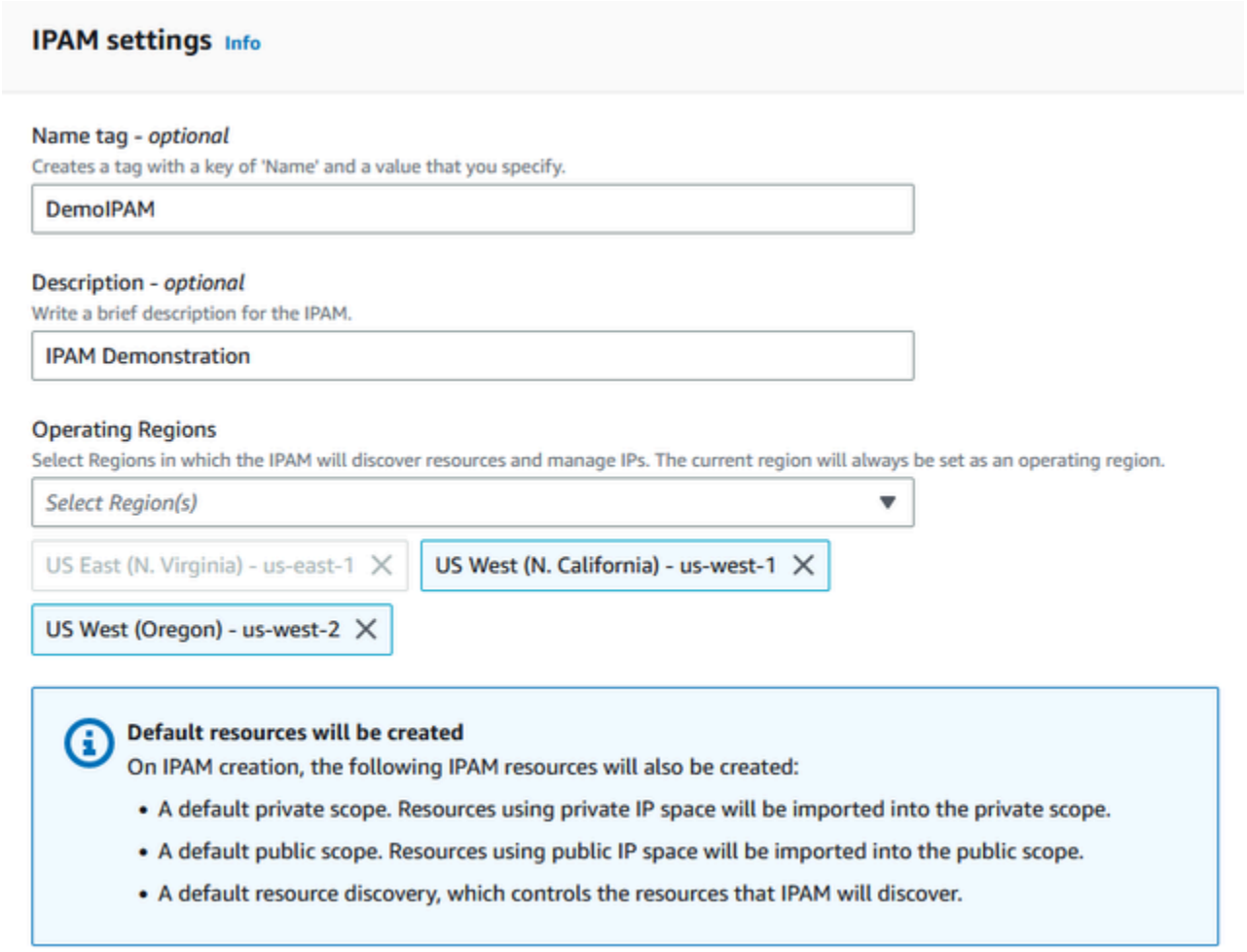
In questo passaggio creerai un IPAM. Quando crei un IPAM, questo crea automaticamente due ambiti per l'IPAM: l'ambito privato destinato a tutto lo spazio privato e l'ambito pubblico destinato a tutto lo spazio pubblico. Gli ambiti, insieme a pool e assegnazioni, sono componenti chiave del tuo IPAM. Per ulteriori informazioni, consulta Funzionamento di IPAM.

Per creare un IPAM

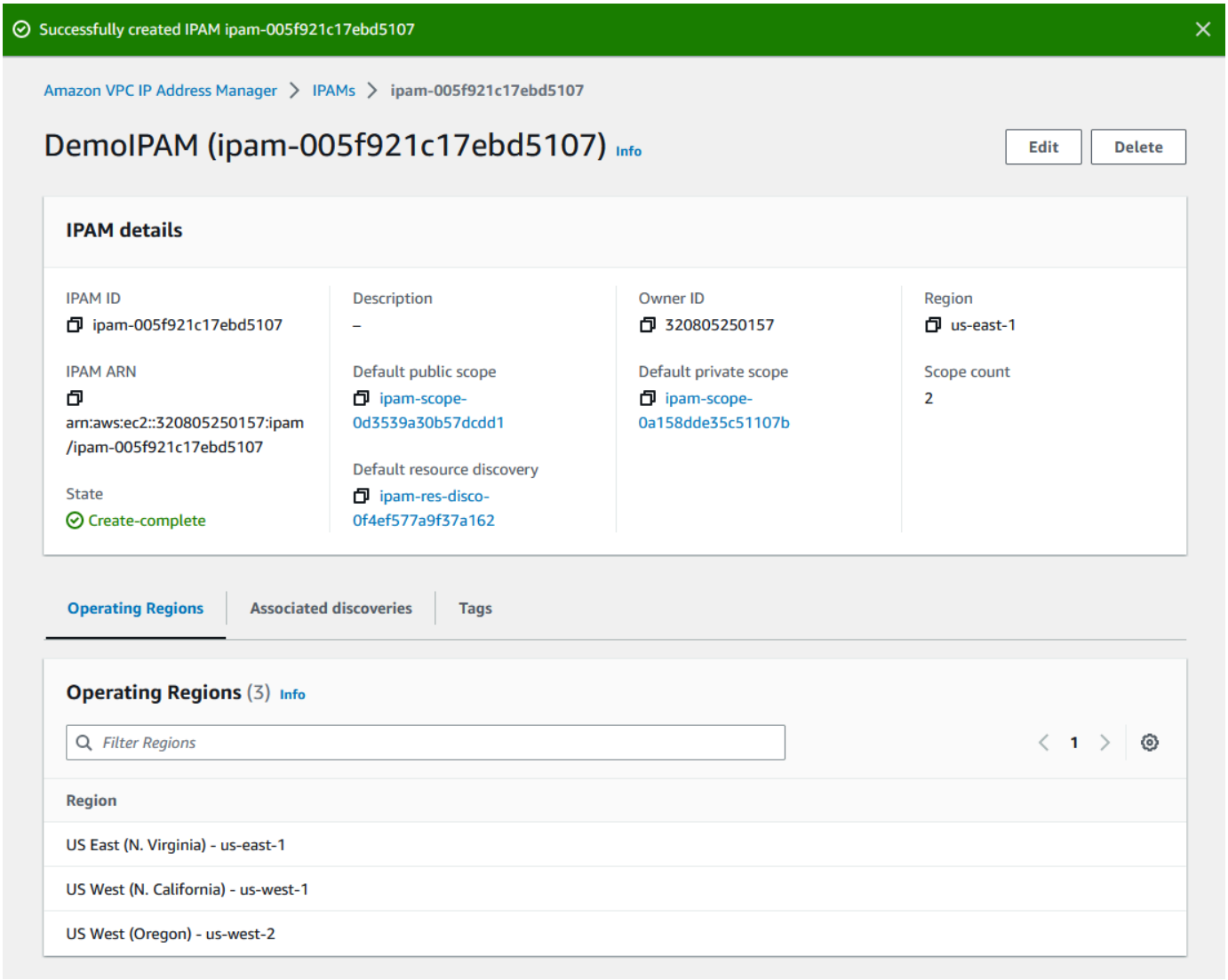
1. Utilizzando l'account AWS Organizations membro delegato come amministratore IPAM nel passaggio precedente, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nella Console AWS di gestione, scegli la AWS regione in cui desideri creare l'IPAM. Crea l'IPAM nella tua Regione operativa principale.
3. Nella home page del servizio, scegli Crea IPAM.
4. Seleziona Consenti a IP Address Manager di Amazon VPC di replicare i dati dagli account sorgente verso l'account IPAM delegato. Se non si seleziona questa opzione, non sarà possibile creare un IPAM.



5. In Regioni operative, scegli le AWS regioni in cui questo IPAM può gestire e scoprire le risorse. La AWS regione in cui si sta creando l'IPAM viene automaticamente selezionata come una delle regioni operative. In questo tutorial, la Regione principale del nostro IPAM è us-east-1, quindi sceglieremo us-west-1 e us-west-2 come regioni operative aggiuntive. Se dimentichi una regione operativa, puoi modificare le impostazioni IPAM in un secondo momento e aggiungere o rimuovere Regioni.



6. Scegli Create IPAM (Crea IPAM).



Passaggio 3: creazione di un pool IPAM di livello superiore

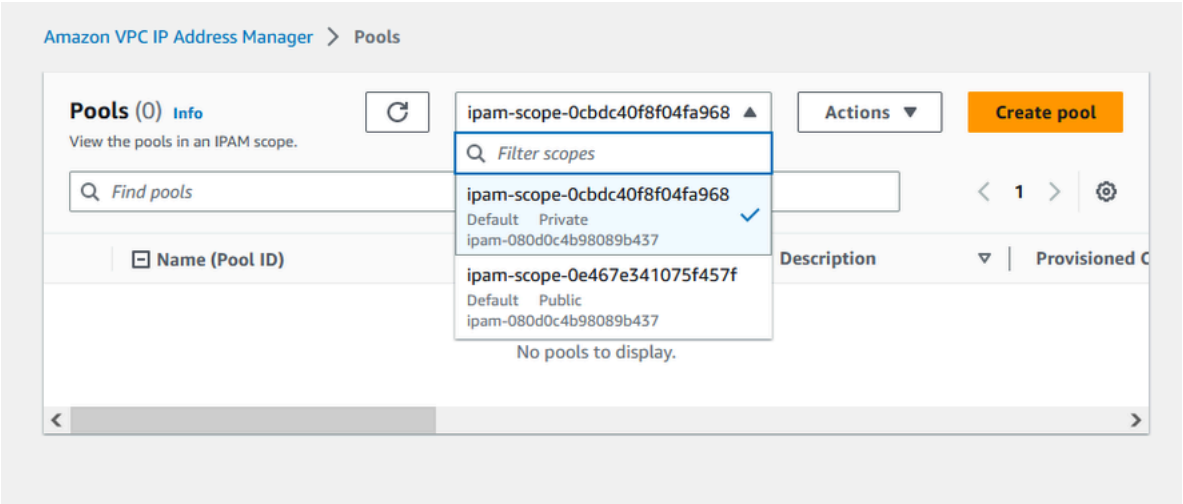
In questo tutorial, creerai una gerarchia di pool a partire dal pool IPAM di livello superiore. Nei passaggi successivi, creerai un paio di pool regionali e un pool di sviluppo di pre-produzione in uno dei pool regionali.

Per ulteriori informazioni sulle gerarchie di pool che è possibile creare con IPAM, consulta la sezione Esempio di piani di pool IPAM.

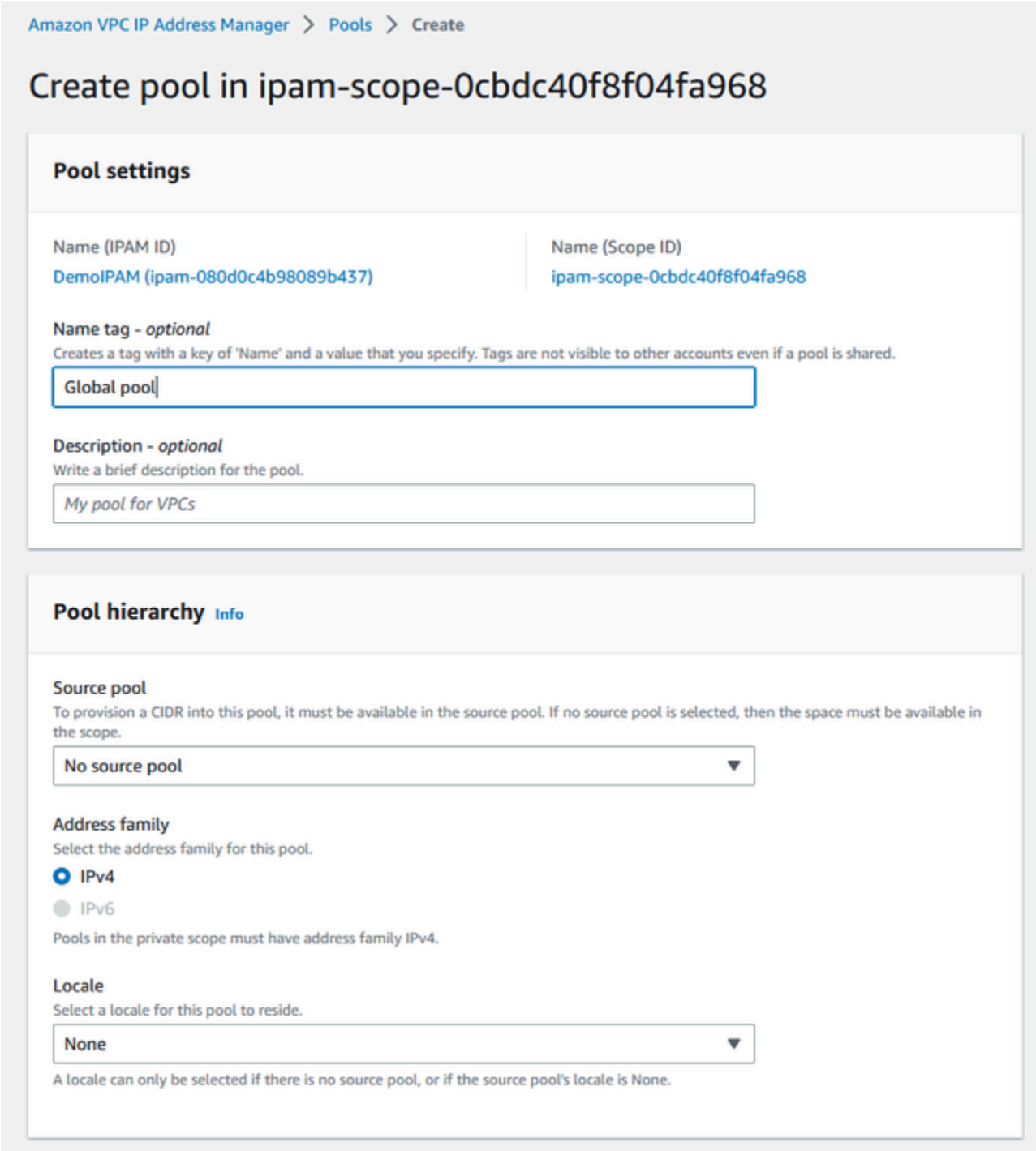
Per creare un pool di livello superiore

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/

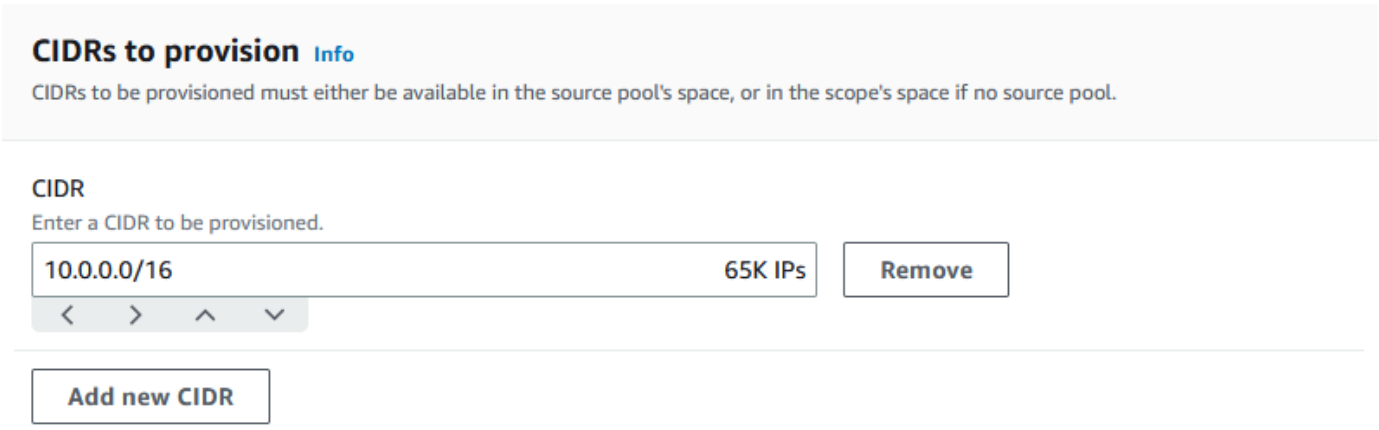
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato.



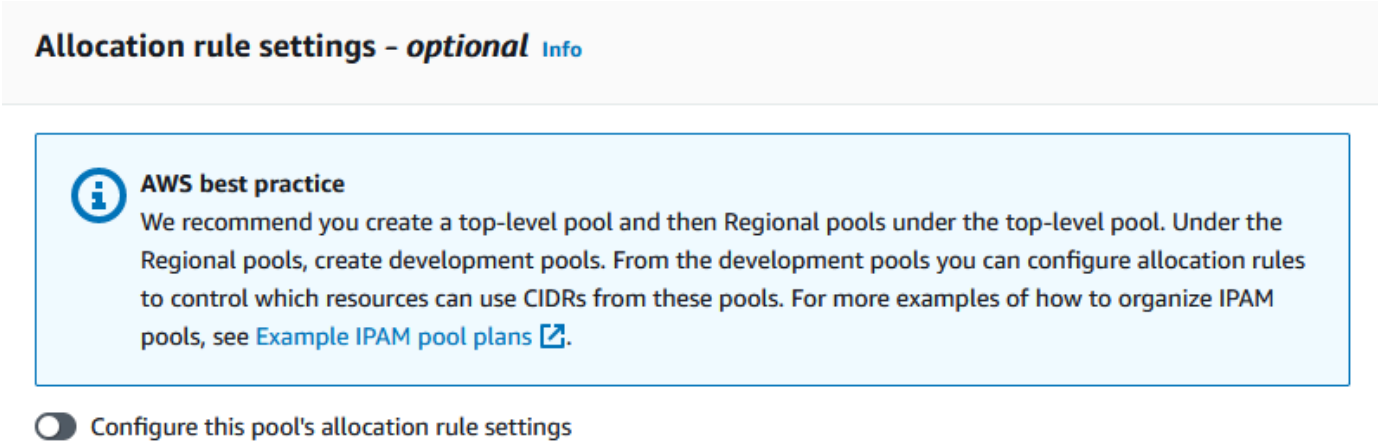
4. Scegli Crea pool.
5. Sotto la voce Ambito IPAM lascia selezionato l'ambito privato.
6. (Facoltativo) Aggiungi un Nome tag e una descrizione per il pool, ad esempio "Pool globale".
7. In Source (Origine), scegli IPAM scope (Ambito IPAM). Poiché questo è il nostro pool di primo livello, non avrà un pool di origine.
8. In Famiglia di indirizzi, scegli. IPv4
9. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
10. Per la Località, scegli Nessuna. Le impostazioni locali sono le AWS regioni in cui desideri che questo pool IPAM sia disponibile per le allocazioni. Nella prossima sezione di questo tutorial, stabilirai le impostazioni locali per i pool regionali che andrai a creare.



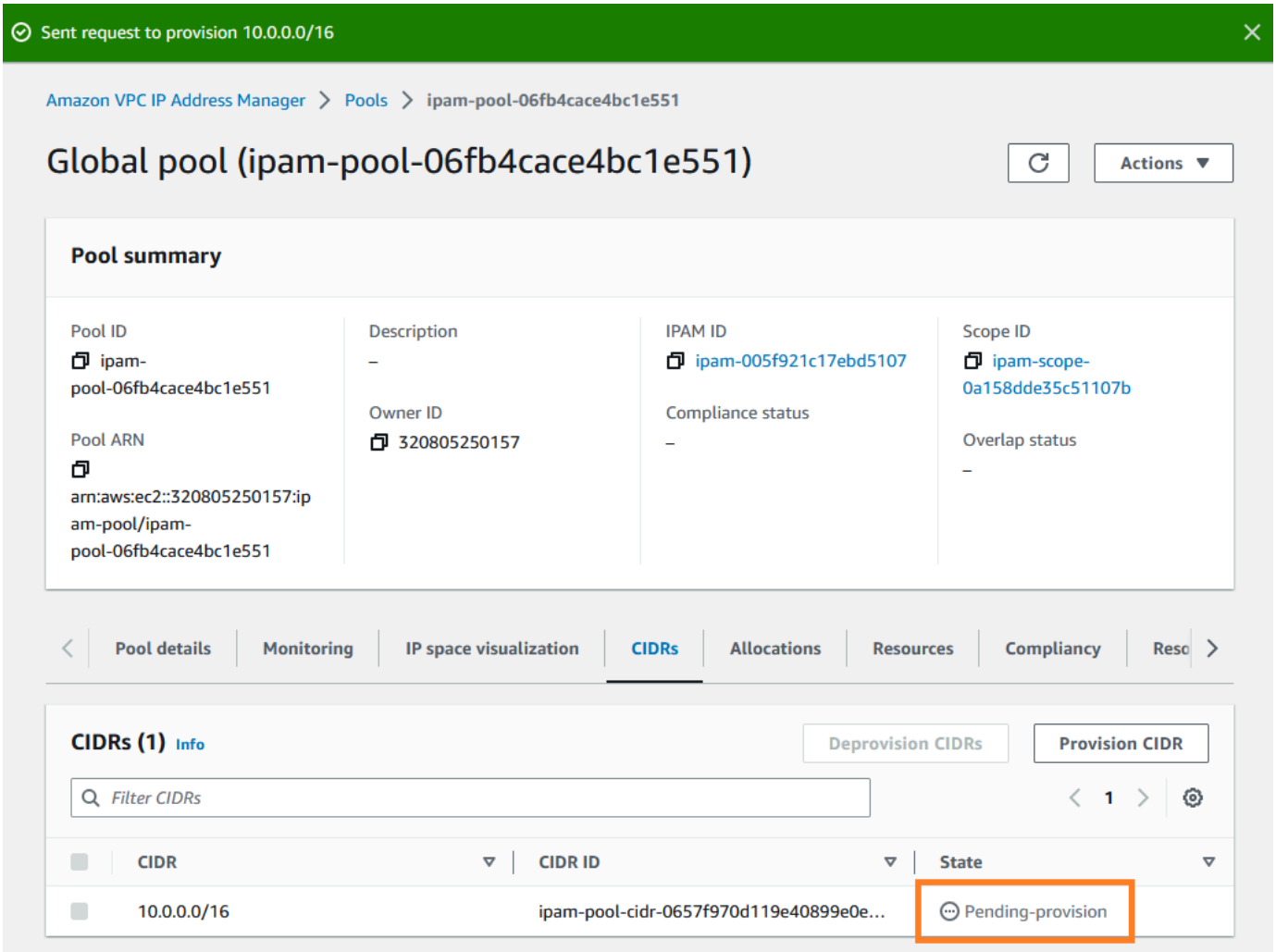
11. Scegli un CIDR su cui effettuare il provisioning per il pool. In questo esempio, forniamo in provisioning 10.0.0.0/16.



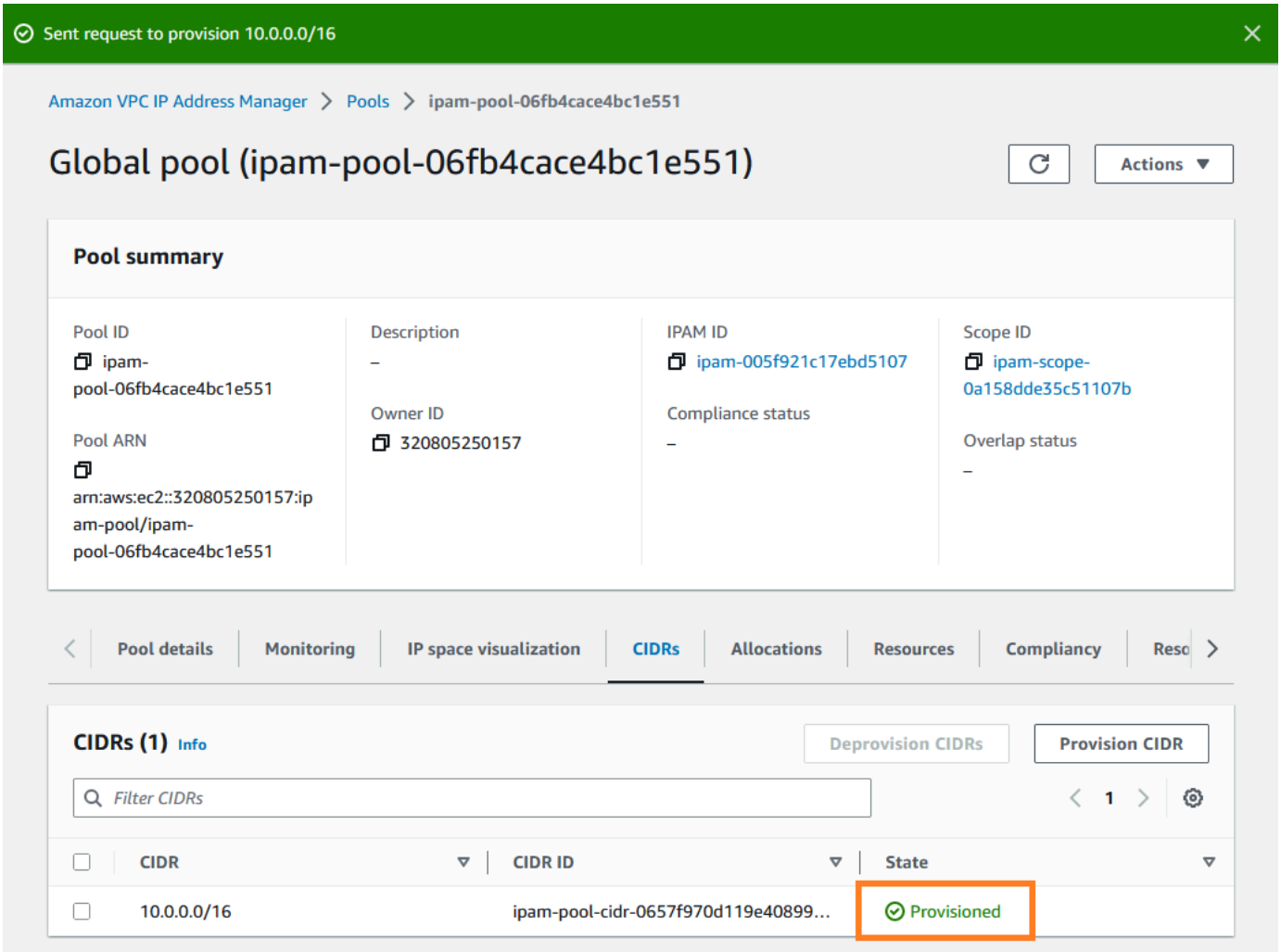
12. Lascia disattivate le impostazioni delle regole di allocazione di "Configura questo pool". Questo è il nostro pool di primo livello e non verrà allocato VPCs direttamente CIDRs da questo pool. Li allocherai, invece, da un sottogruppo creato da questo pool.



13. Scegli Crea pool. Il pool viene creato e il CIDR è in uno stato di fornitura in sospeso:



14. Attendi che lo stato sia Con provisioning prima di continuare con il passaggio successivo.



Ora che hai creato il tuo pool di livello superiore, creerai pool regionali nelle Regioni us-west-1 e us-west-2.

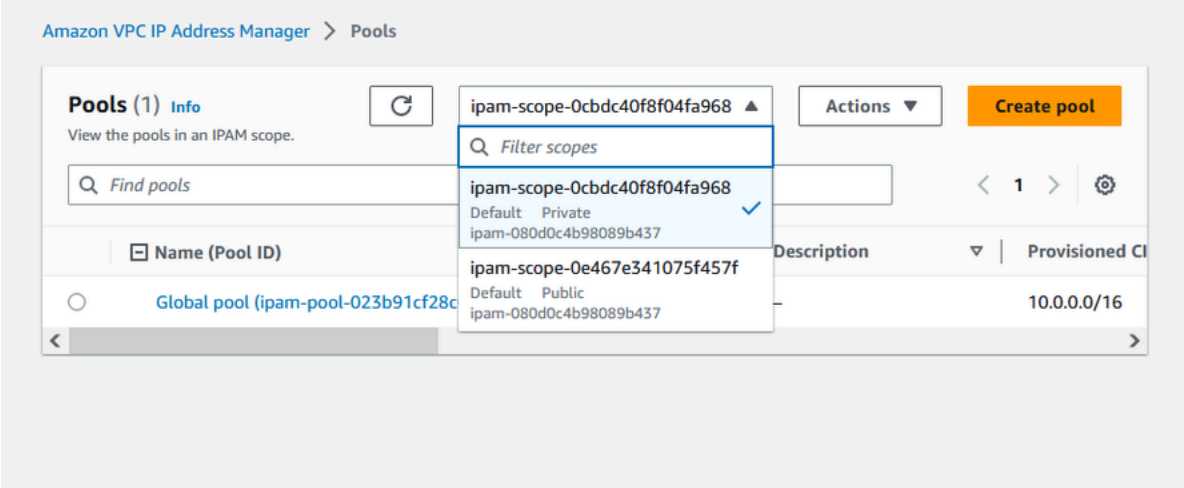
Fase 4: creazione di pool IPAM regionali

In questa sezione viene descritto come organizzare gli indirizzi IP utilizzando due pool Regionali. In questo tutorial, seguiremo uno degli esempi di piani di pool IPAM e creeremo due pool regionali che possono essere utilizzati dagli account membro dell'organizzazione per l'allocazione CIDRs ai rispettivi. VPCs

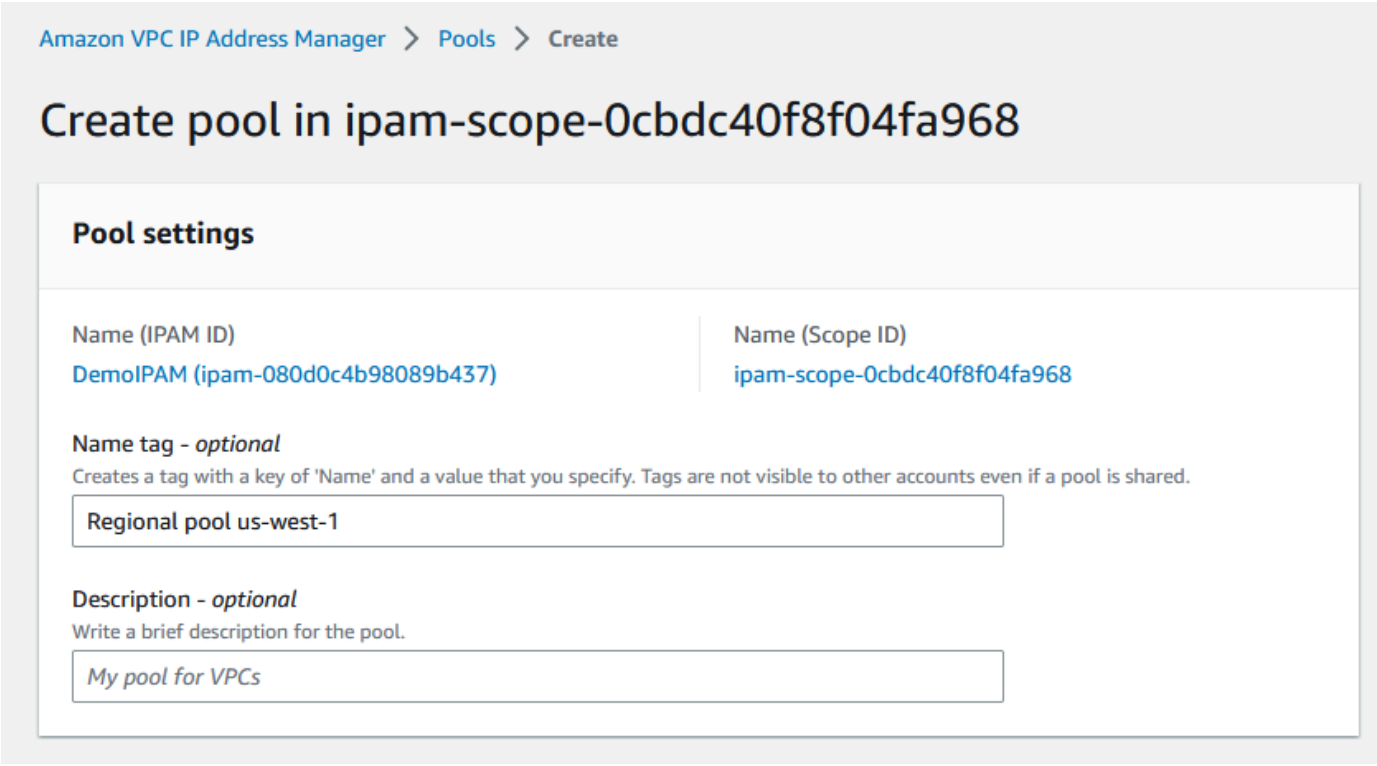
Per creare un pool regionale

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/

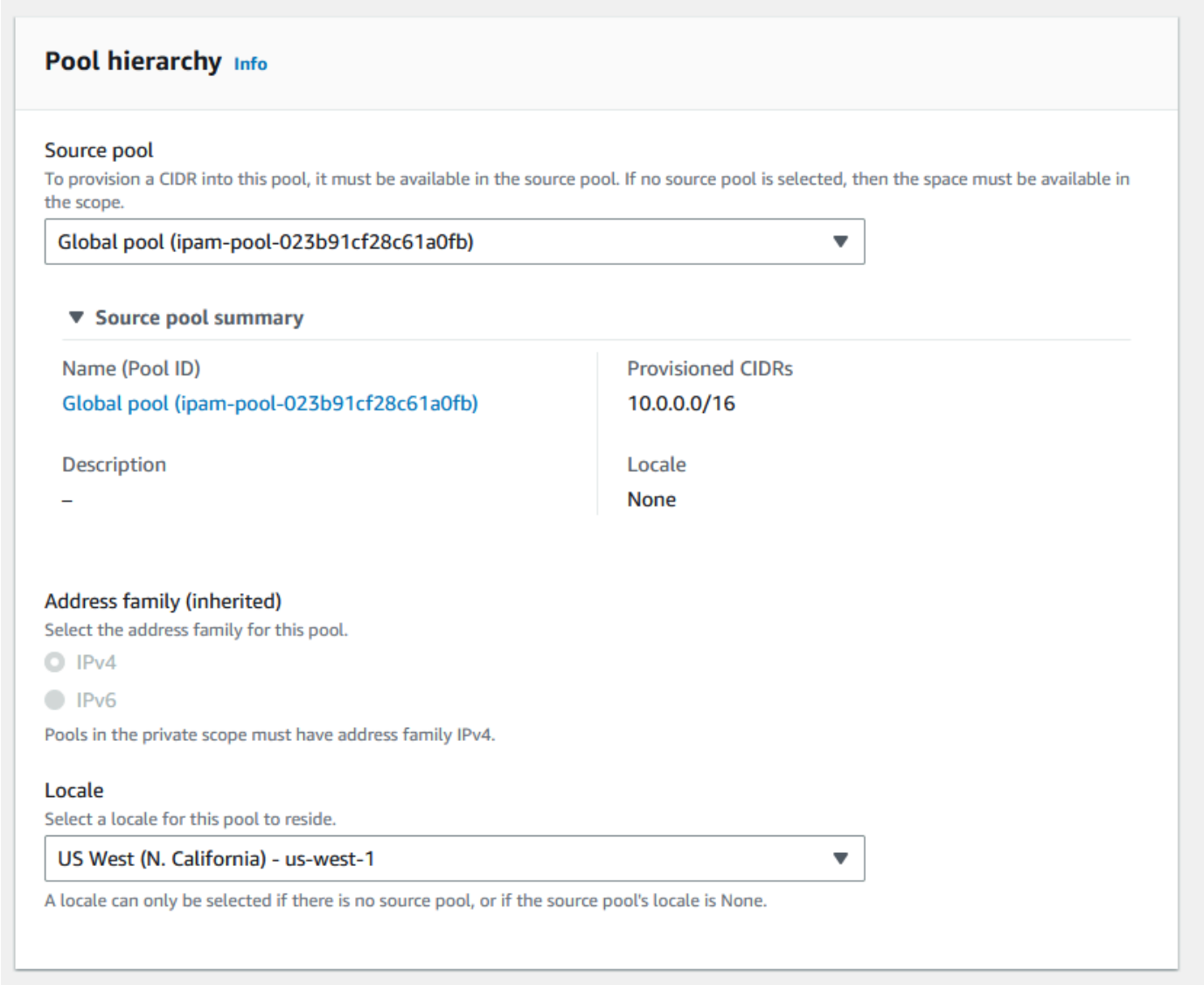
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato.



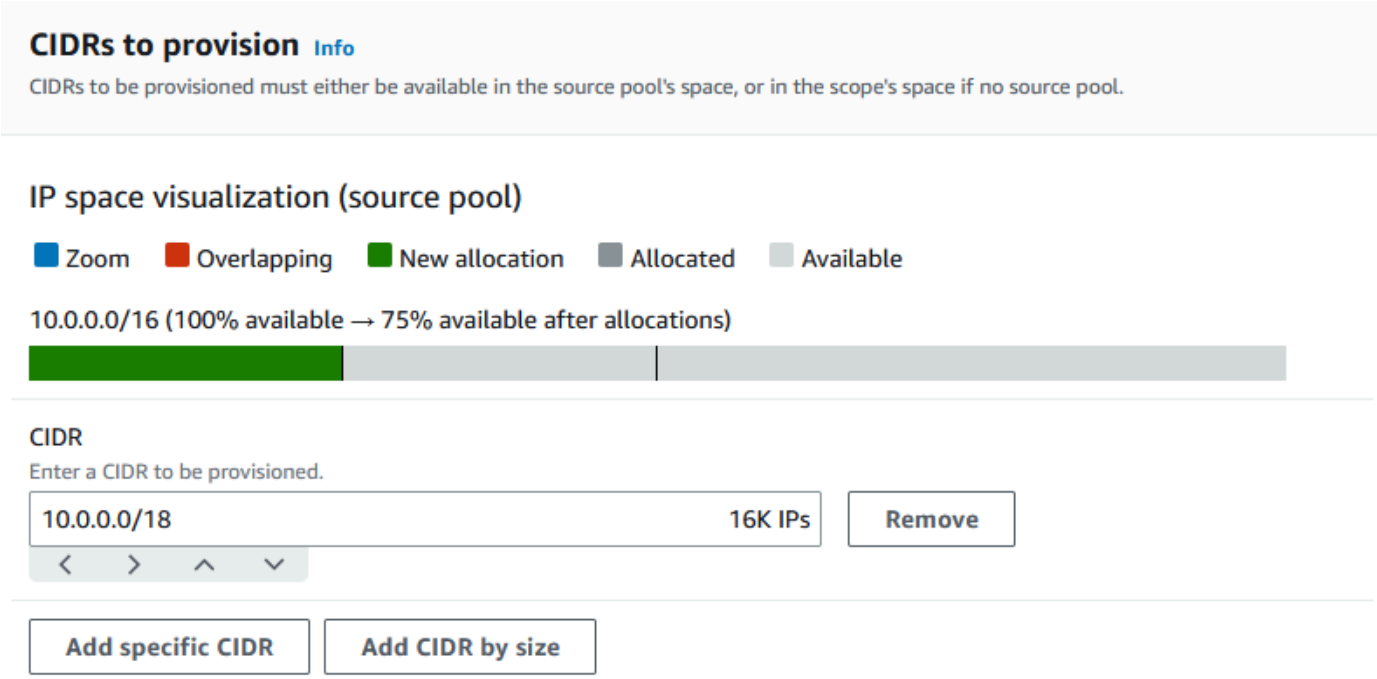
4. Scegli Crea pool.
5. Sotto la voce Ambito IPAM lascia selezionato l'ambito privato.
6. (Facoltativo) Aggiungi un Tag del nome e una descrizione per il pool, come pool regionale us-west-1.



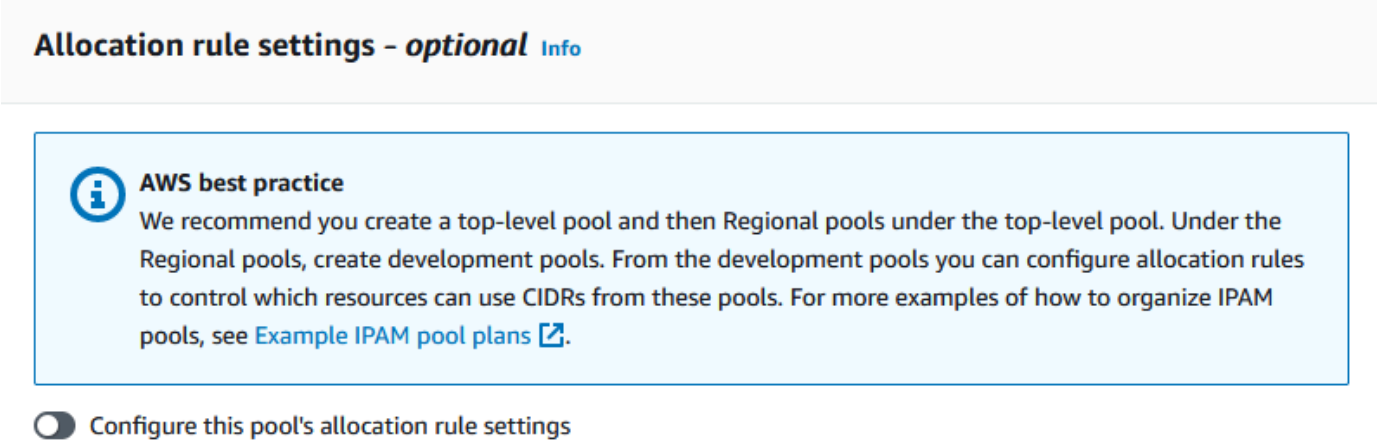
7. In Source (Origine), seleziona IPAM pool (Pool IPAM), quindi seleziona il pool di massimo livello (“Pool globale”) creato in Passaggio 3: creazione di un pool IPAM di livello superiore. Quindi, in Impostazione locale, scegli us-west-1.



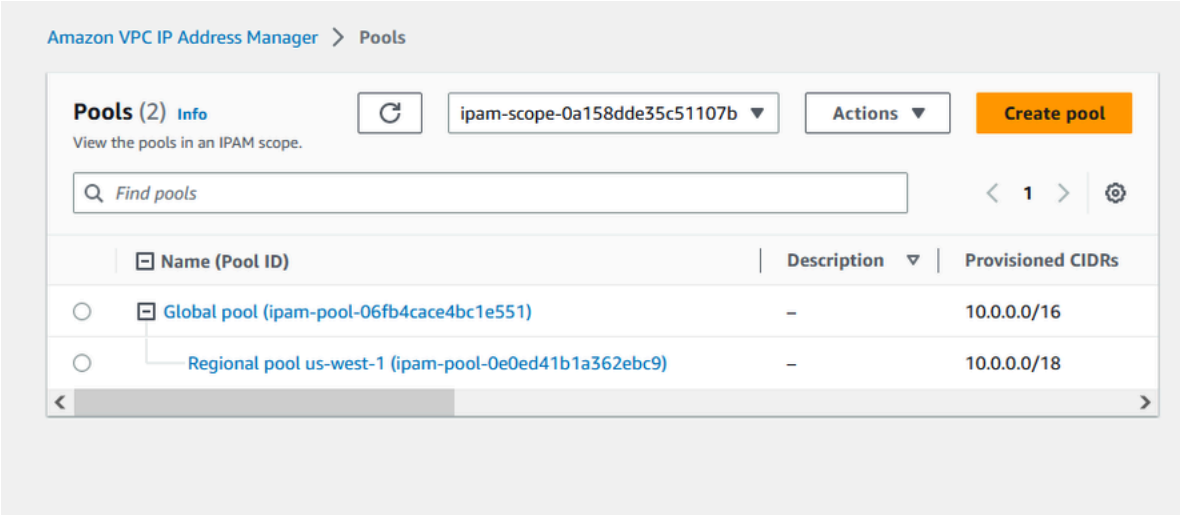
8. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell’ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
9. In CIDRs to provisioning, inserisci 10.0.0.0/18, che fornirà a questo pool circa 16.000 indirizzi IP disponibili.



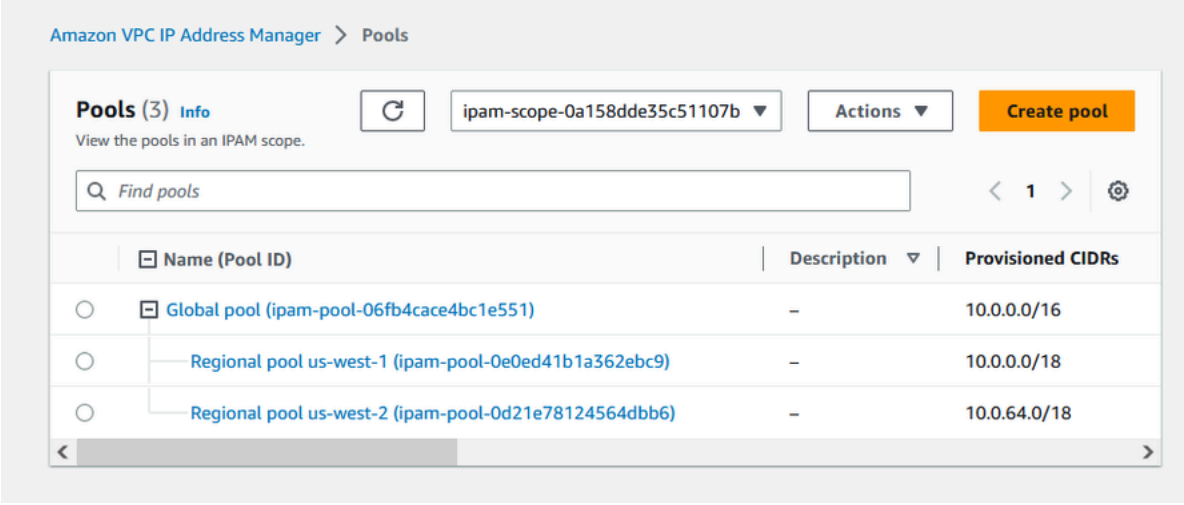
10. Lascia disattivate le impostazioni delle regole di allocazione di "Configura questo pool". Non effettuerai l'allocazione VPCs direttamente CIDRs da questo pool. Li allocherai, invece, da un sottogruppo creato da questo pool.



11. Scegli Crea pool.
12. Torna alla visualizzazione Pool per vedere la gerarchia dei pool IPAM che hai creato.



13. Ripeti i passaggi in questa sezione e crea un secondo pool regionale nella versione locale us-west-2 con il CIDR 10.0.64.0/18 a esso fornito in provisioning. Una volta completato il processo, disporrai di tre pool in una gerarchia simile a questa:

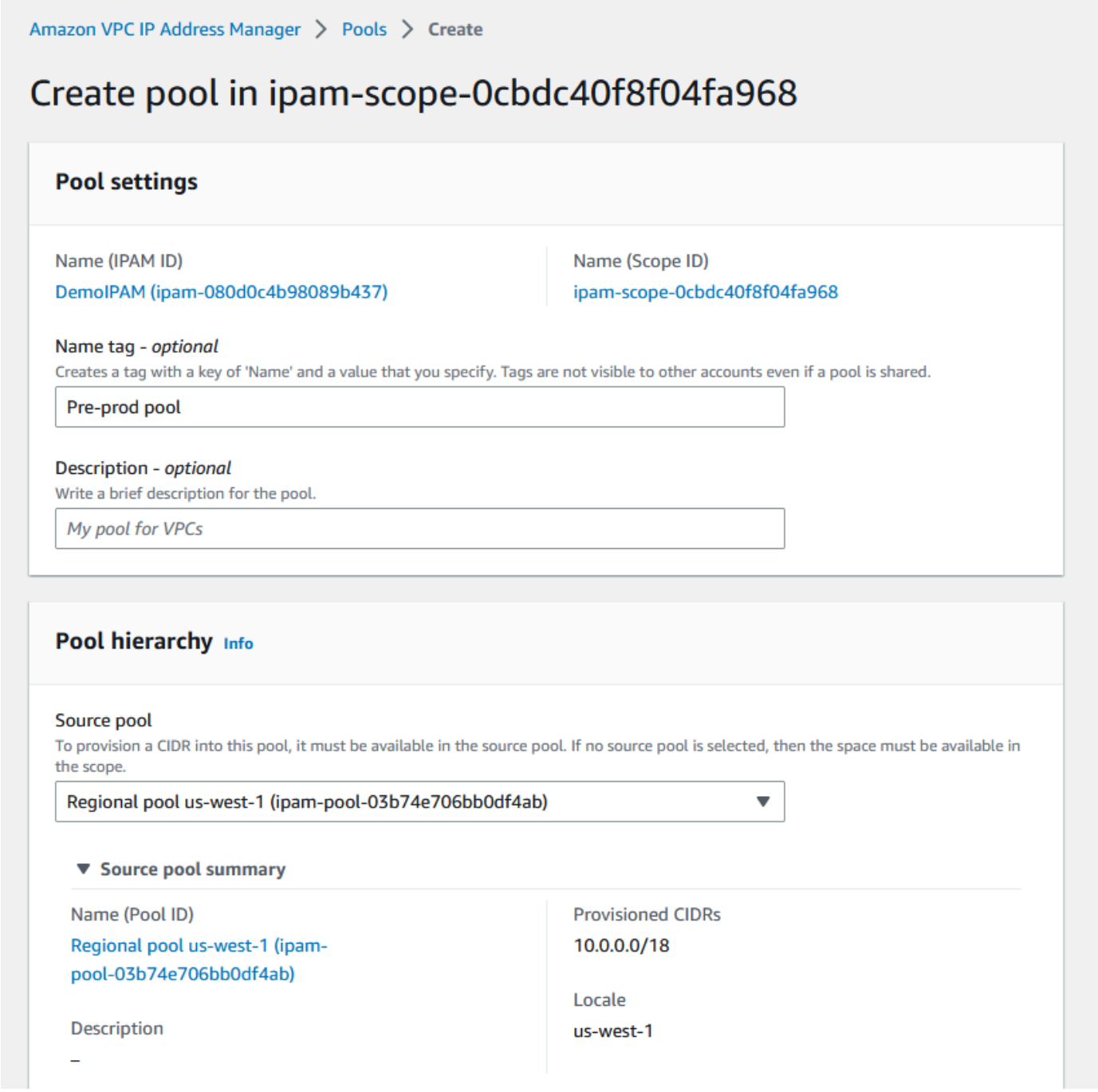


Fase 5: creazione di un pool di sviluppo di pre-produzione

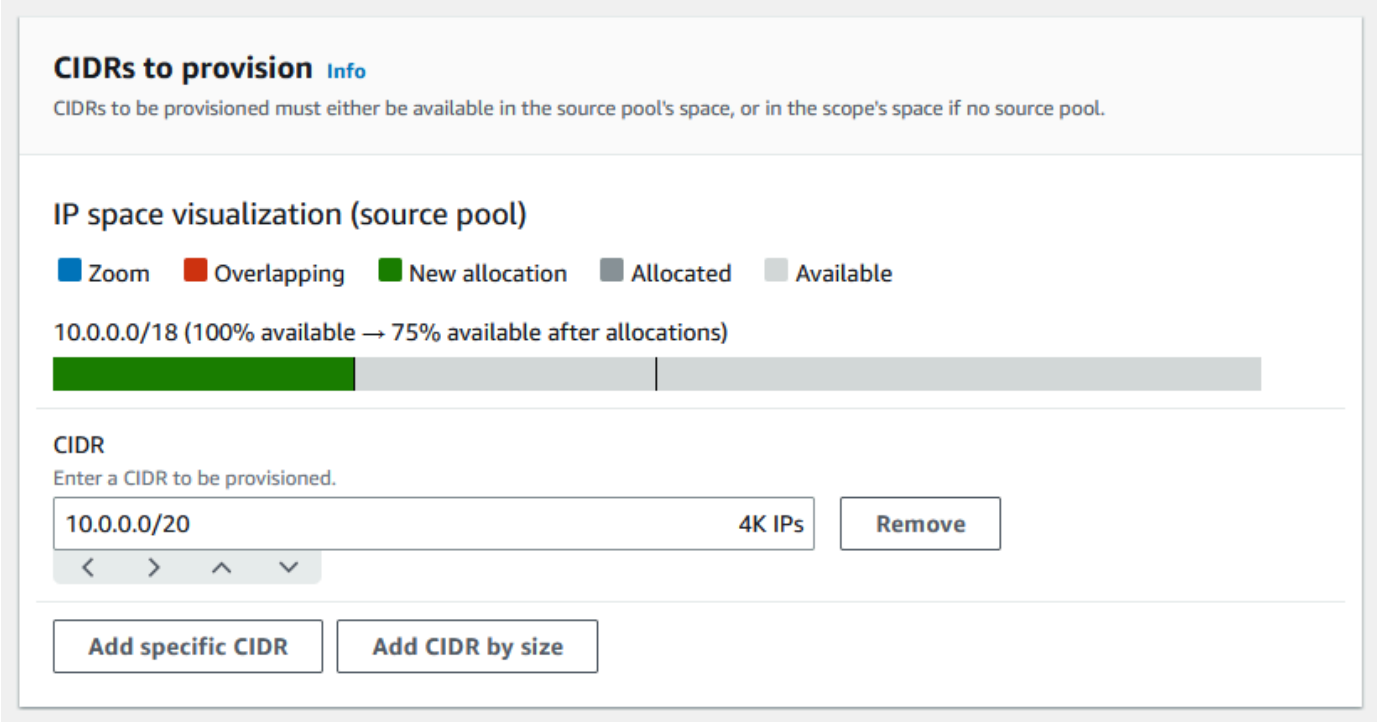
Segui i passaggi in questa sezione per creare un pool di sviluppo per le risorse di pre-produzione all'interno del tuo pool regionale.

Per creare un pool di sviluppo di pre-produzione

1. Analogamente a quanto hai fatto nel passaggio precedente, utilizzando l'account amministratore di IPAM crea un pool denominato Pre-prod pool, ma questa volta utilizza il pool regionale us-west-1 come pool di origine.

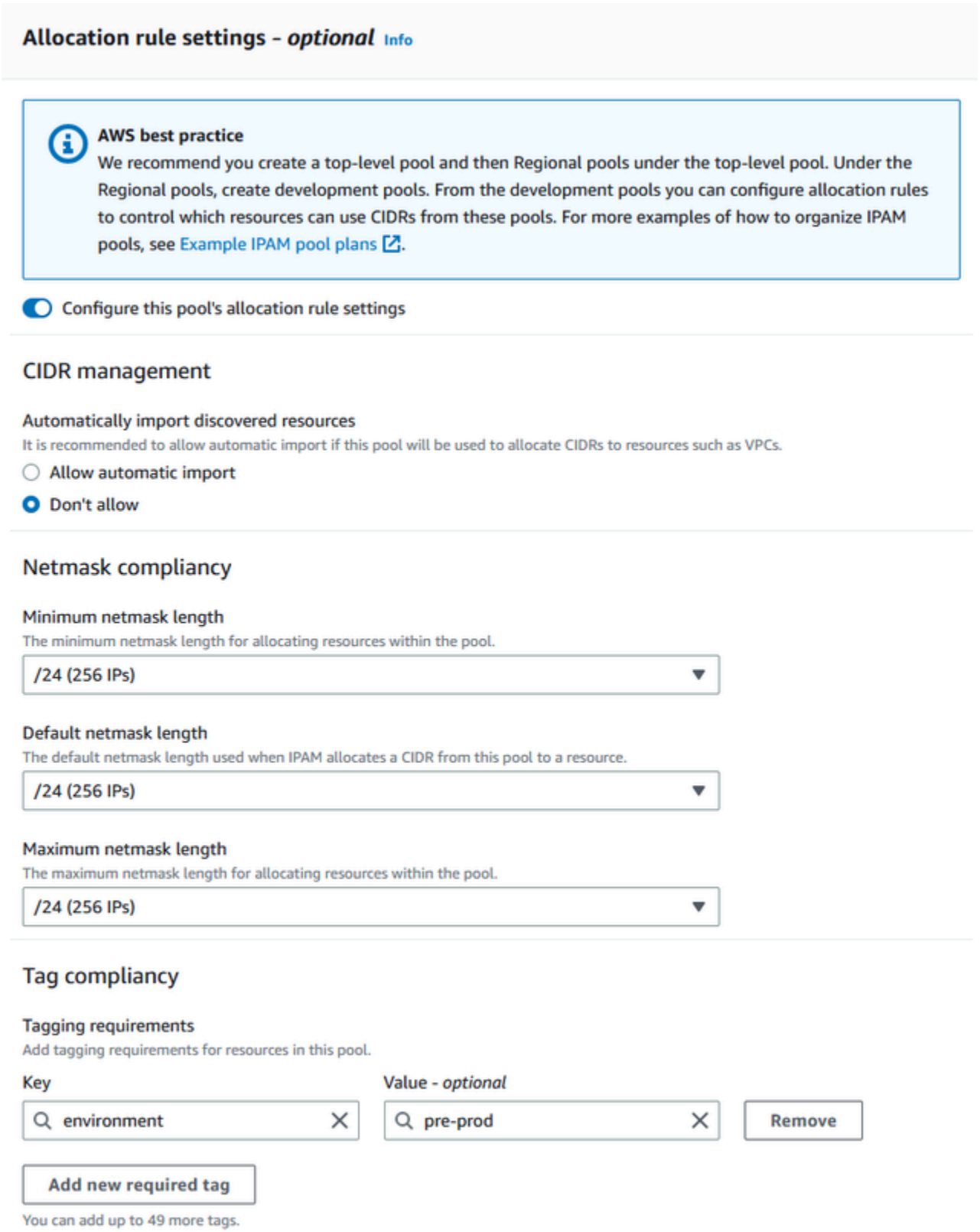


2. Specifica come CIDR per cui effettuare il provisioning 10.0.0.0/20, che fornirà a questo pool circa 4.000 indirizzi IP.



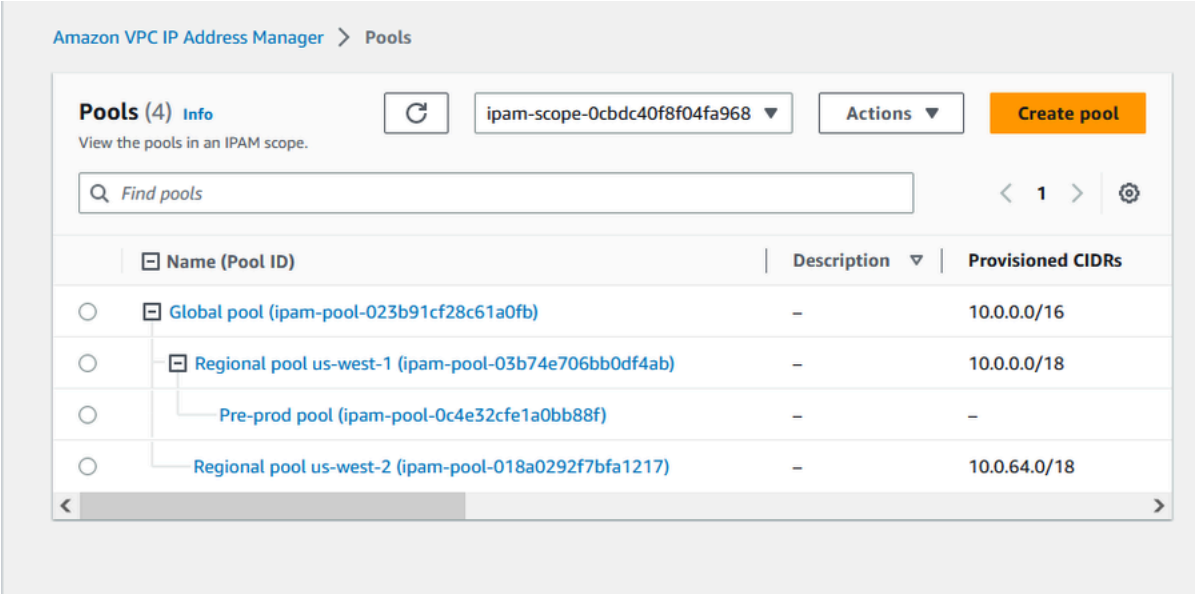
3. Attiva l'opzione Configura le impostazioni delle regole di allocazione di questo pool. Esegui questa operazione:

    1. In Gestione CIDR, per Importa automaticamente le risorse rilevate, lascia selezionata l'opzione predefinita Non consentire. Questa opzione consentirebbe a IPAM di importare automaticamente le risorse CIDRs che scopre nelle impostazioni locali del pool. Una descrizione dettagliata di questa opzione non rientra tra gli argomenti trattati in questo tutorial, ma puoi leggere maggiori informazioni su questa opzione in Creare un pool di primo livello IPv4 .
    2. In Conformità alla maschera di rete, scegli /24 per la lunghezza minima, predefinita e massima della maschera di rete. Una descrizione dettagliata di questa opzione non rientra tra gli argomenti trattati in questo tutorial, ma puoi leggere maggiori informazioni su questa opzione in Creare un pool di primo livello IPv4 . È importante notare che il VPC che creerai in seguito con un CIDR da questo pool sarà limitato a /24 in base a ciò che abbiamo impostato qui.
    3. In Conformità ai tag, inserisci ambiente/pre-prod. Questo tag sarà necessario per VPCs allocare lo spazio dal pool. Dimostreremo in seguito come funziona.



4. Scegli Crea pool.

5. La gerarchia dei pool ora include un sottopool aggiuntivo nel pool regionale us-west-1:



Ora sei pronto per condividere il pool IPAM con un altro account membro della tua organizzazione. In questo modo, potrai abilitare tale account ad allocare un CIDR dal pool per creare un VPC.

Fase 6: condivisione del pool IPAM

Segui i passaggi di questa sezione per condividere il pool IPAM di preproduzione utilizzando AWS Resource Access Manager (RAM).

Questa sezione è composta da due sottosezioni:

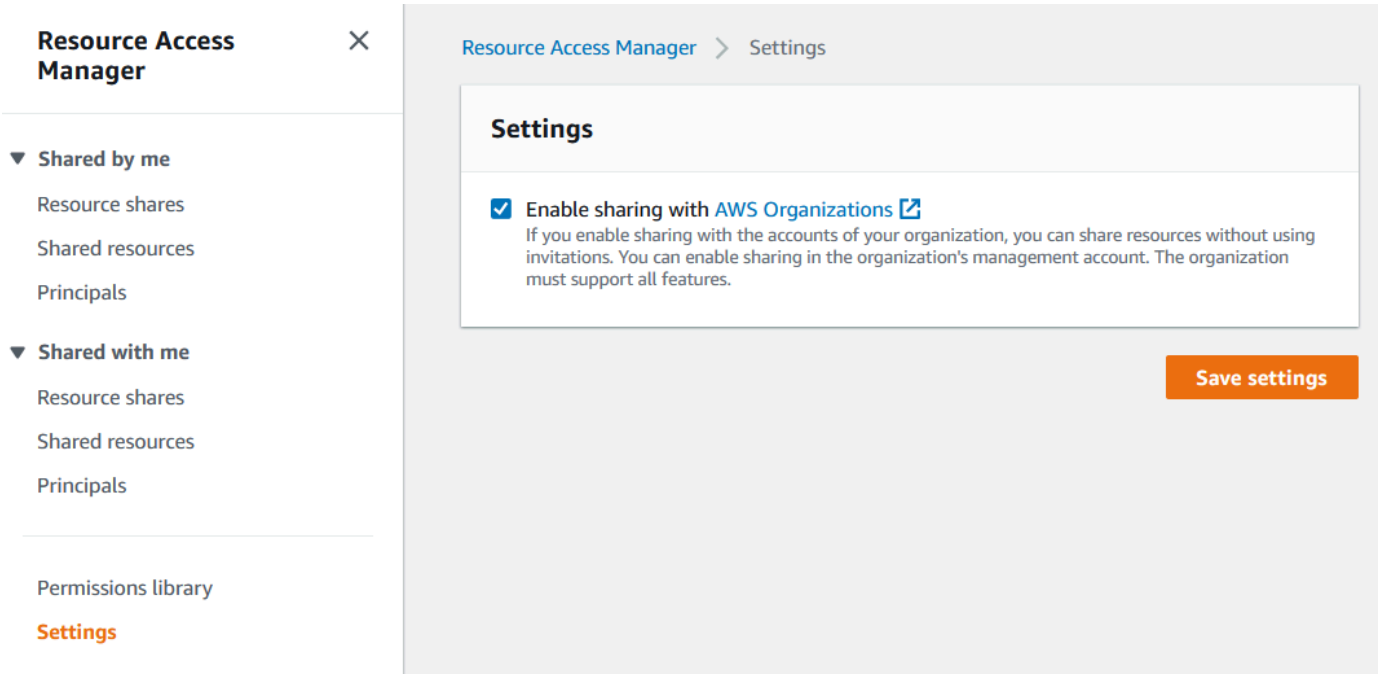
- Fase 6.1. Abilitazione della condivisione delle risorse in AWS RAM: questo passaggio deve essere eseguito dall'account di gestione di AWS Organizations .
- Fase 6.2. Condividi un pool IPAM utilizzando AWS RAM: questo passaggio deve essere eseguito dall'amministratore di IPAM.

Fase 6.1. Abilitazione della condivisione delle risorse in AWS RAM

Dopo aver creato il tuo IPAM, ti consigliamo di condividere i pool di indirizzi IP con altri account della tua organizzazione. Prima di condividere un pool IPAM, completa i passaggi di questa sezione per abilitare la condivisione delle risorse con. AWS RAM

Per abilitare la condivisione delle risorse

1. Utilizzando l'account AWS Organizations di gestione, apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, scegli Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.



Ora puoi condividere un pool IPAM con altri membri dell'organizzazione.

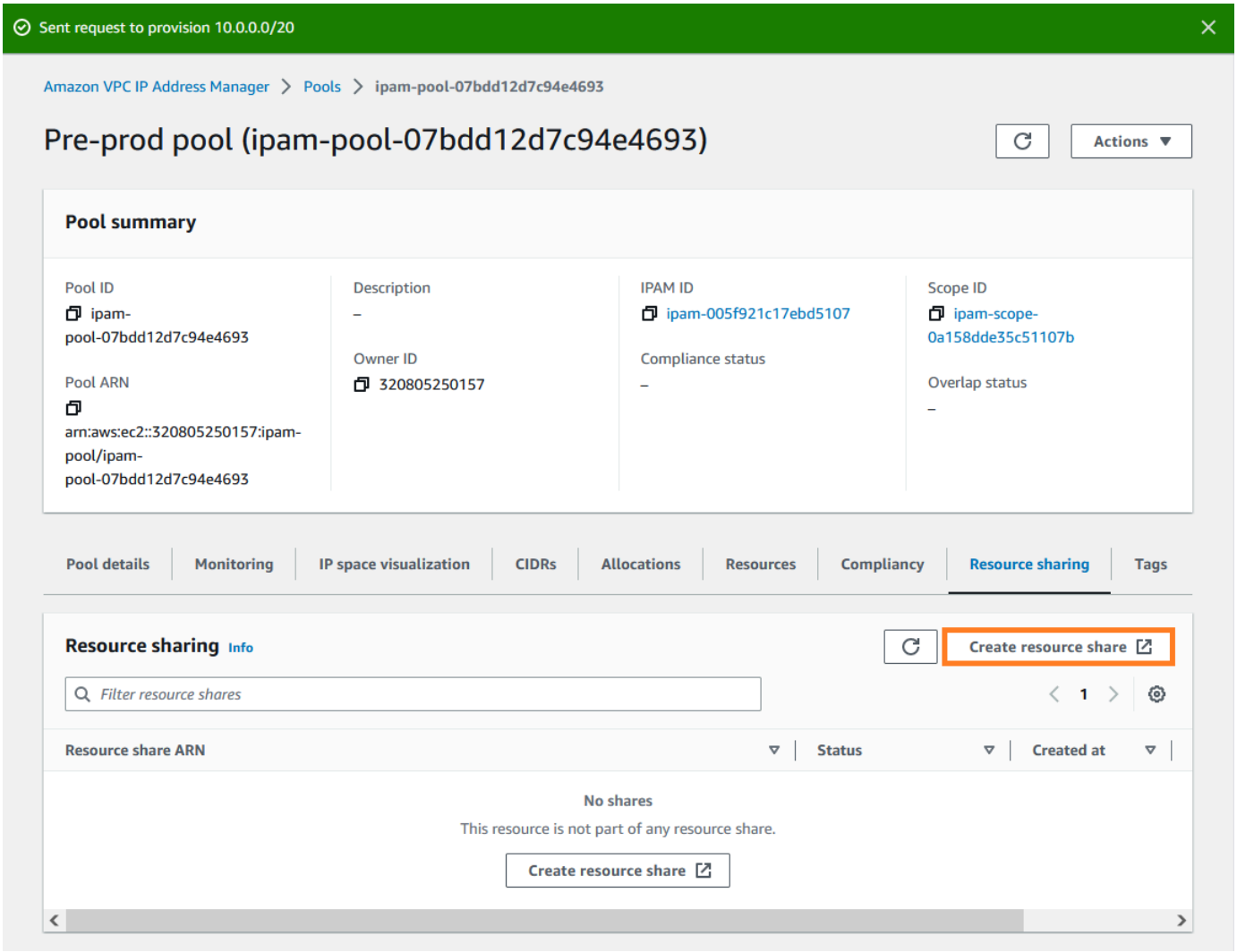
Fase 6.2. Condividi un pool IPAM utilizzando AWS RAM

In questa sezione condividerai il pool di sviluppo di pre-produzione con un altro account AWS Organizations membro. Per istruzioni complete sulla condivisione dei pool IPAM, comprese le informazioni sulle autorizzazioni IAM richieste, consulta Condivisione di un pool IPAM tramite AWS RAM.

Per condividere un pool IPAM utilizzando AWS RAM

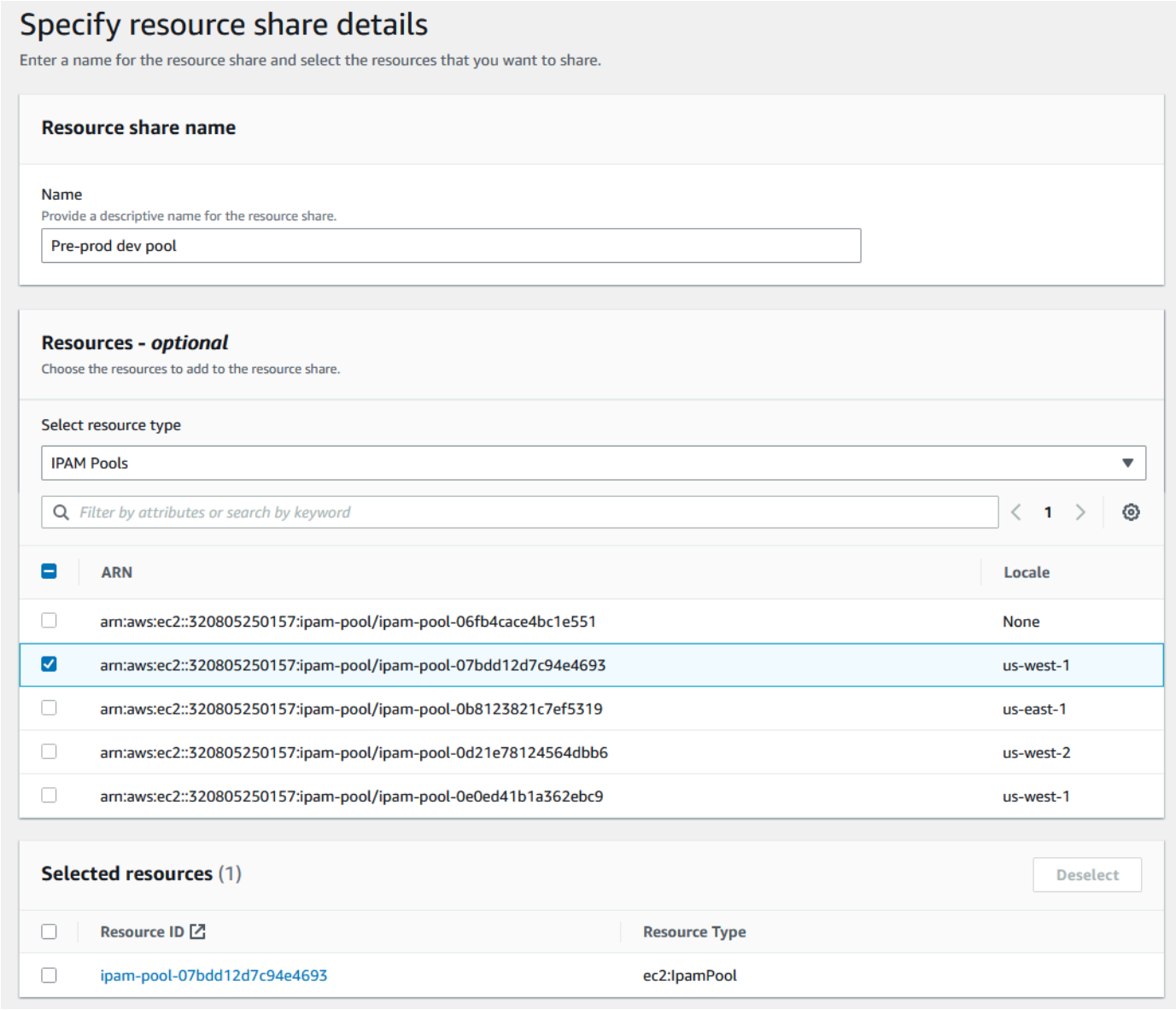
1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato, scegli il pool IPAM di pre-produzione e scegli Azioni > Visualizza dettagli.

4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. La AWS RAM console si apre. Condividerai il pool utilizzando AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).

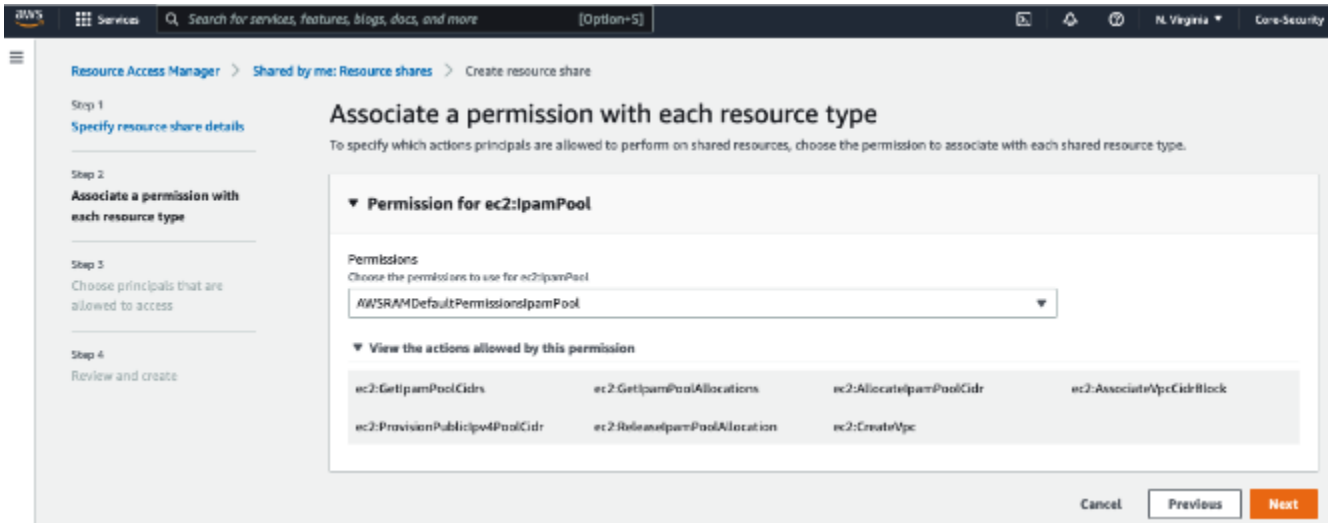


La AWS RAM console si apre.

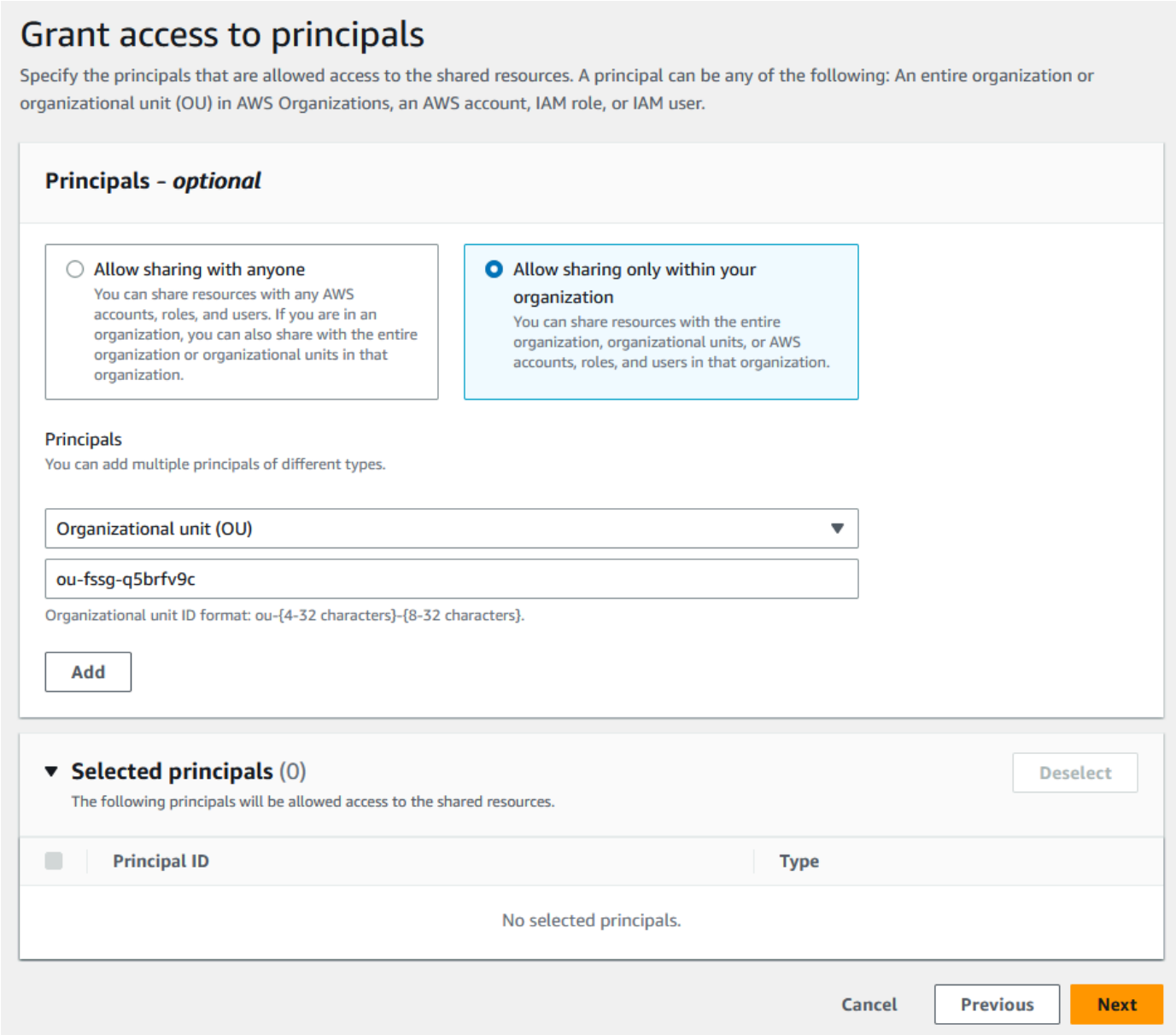
6. Nella AWS RAM console, scegli nuovamente Crea una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona il tipo di risorsa, scegli i pool IPAM, quindi scegli l'ARN del pool di sviluppo di pre-produzione.



9. Scegli Next (Successivo).
10. Lascia selezionata l'AWSRAMDefaultPermissionsIpamPoolautorizzazione predefinita. I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione Condivisione di un pool IPAM tramite AWS RAM.



11. Scegli Next (Successivo).
12. In Principali, scegli Consenti la condivisione solo all'interno dell'organizzazione. Inserisci AWS Organizations l'ID dell'unità organizzativa (come indicato in)Come si AWS Organizations integra con IPAM, quindi scegli Aggiungi.



13. Scegli Next (Successivo).
14. Controlla le opzioni di condivisione delle risorse e i principali con cui condividerai, quindi scegli Crea.

Ora che il pool è stato condiviso, vai al passaggio successivo per creare un VPC con un CIDR allocato da un pool IPAM.

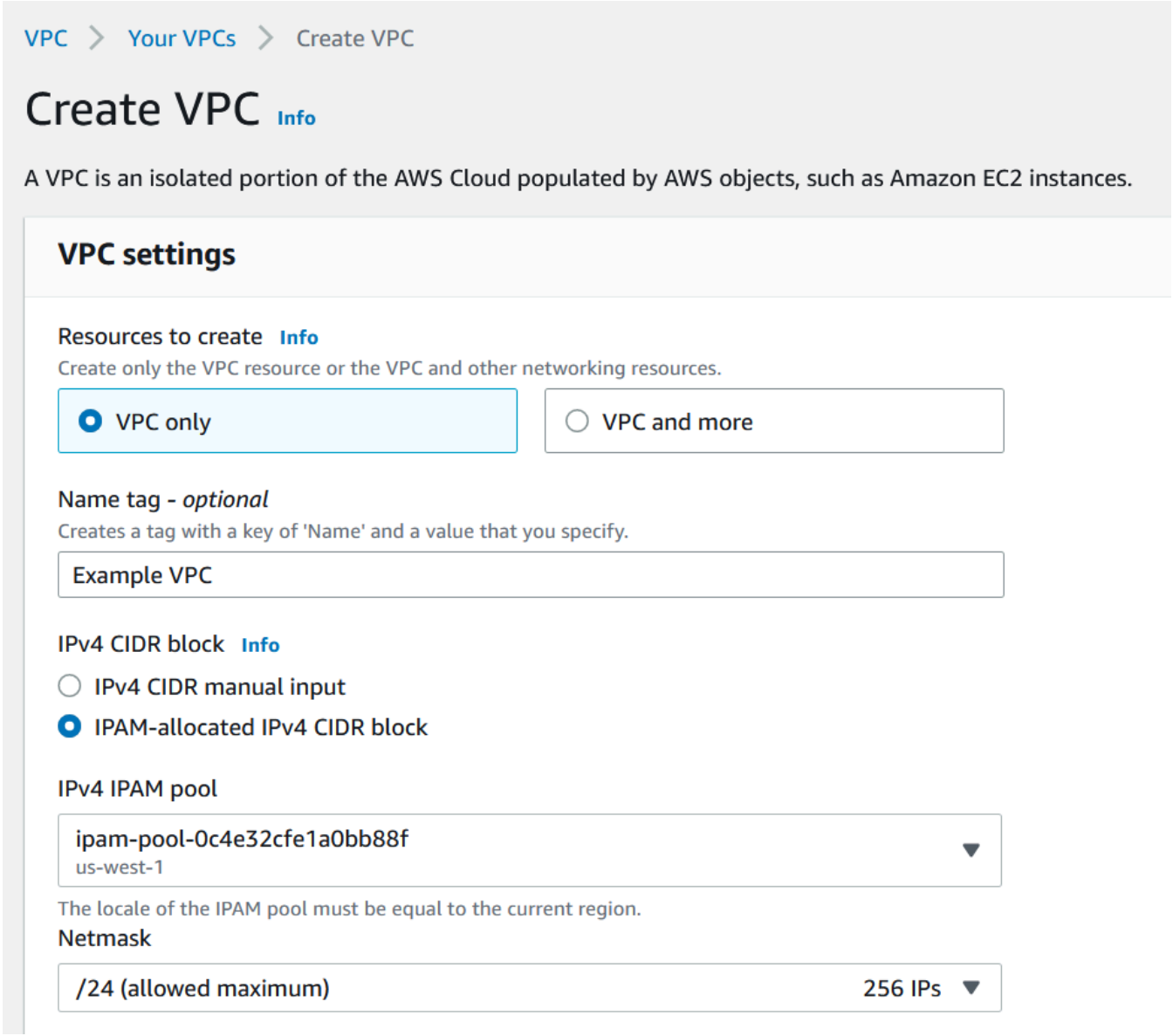
Fase 7: creazione di un VPC con un CIDR assegnato da un pool IPAM

Segui la procedura descritta in questa sezione per creare un VPC con un CIDR assegnato dal pool di pre-produzione. Questo passaggio deve essere completato dall'account membro dell'unità

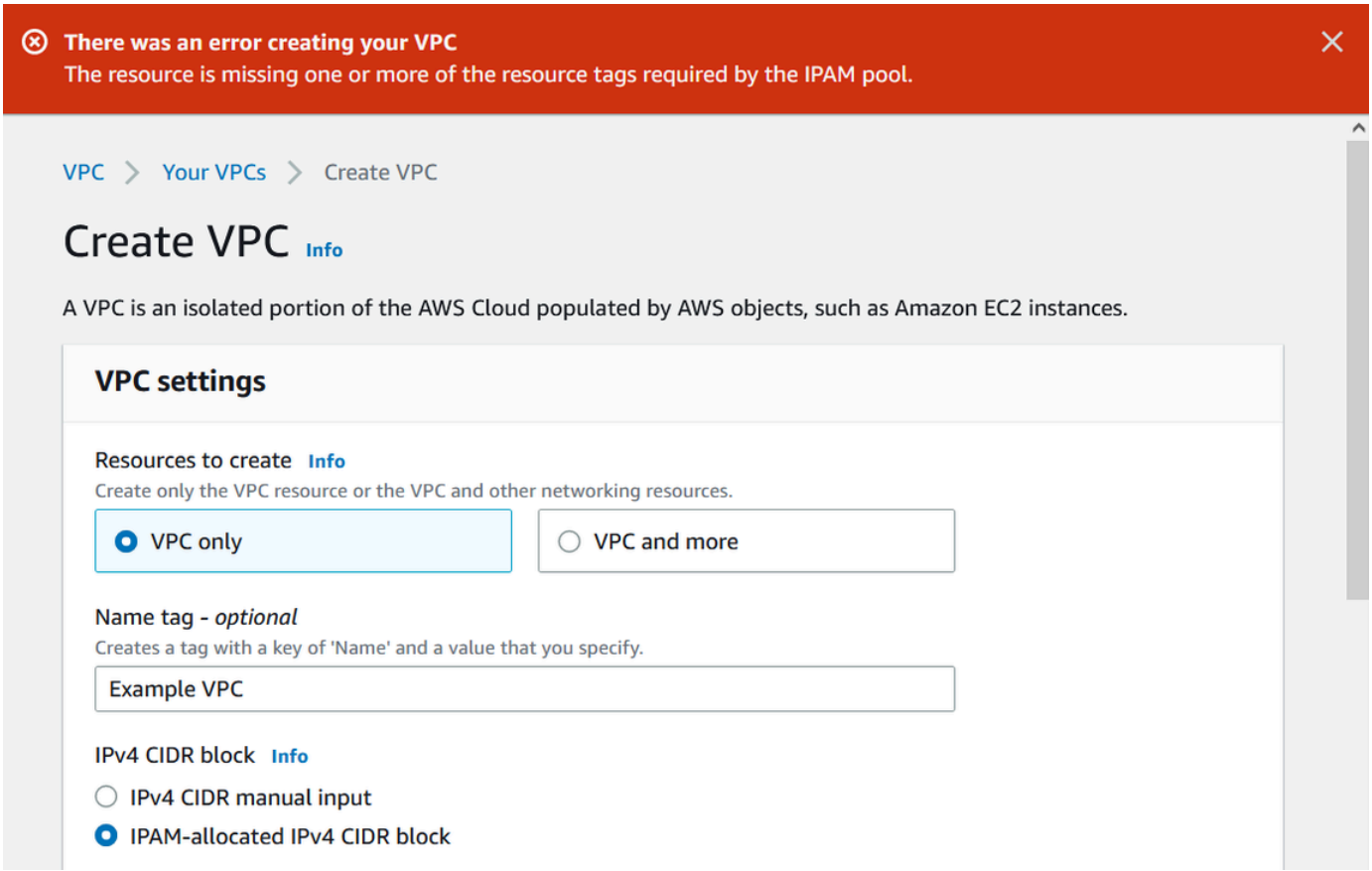
organizzativa con cui il pool IPAM è stato condiviso nella sezione precedente (denominata example-member-account-2 inCome si AWS Organizations integra con IPAM). Per ulteriori informazioni sulle autorizzazioni IAM necessarie per la creazione VPCs, consulta gli esempi di policy di Amazon VPC nella Amazon VPC User Guide.

Per creare un VPC con un CIDR assegnato da un pool IPAM

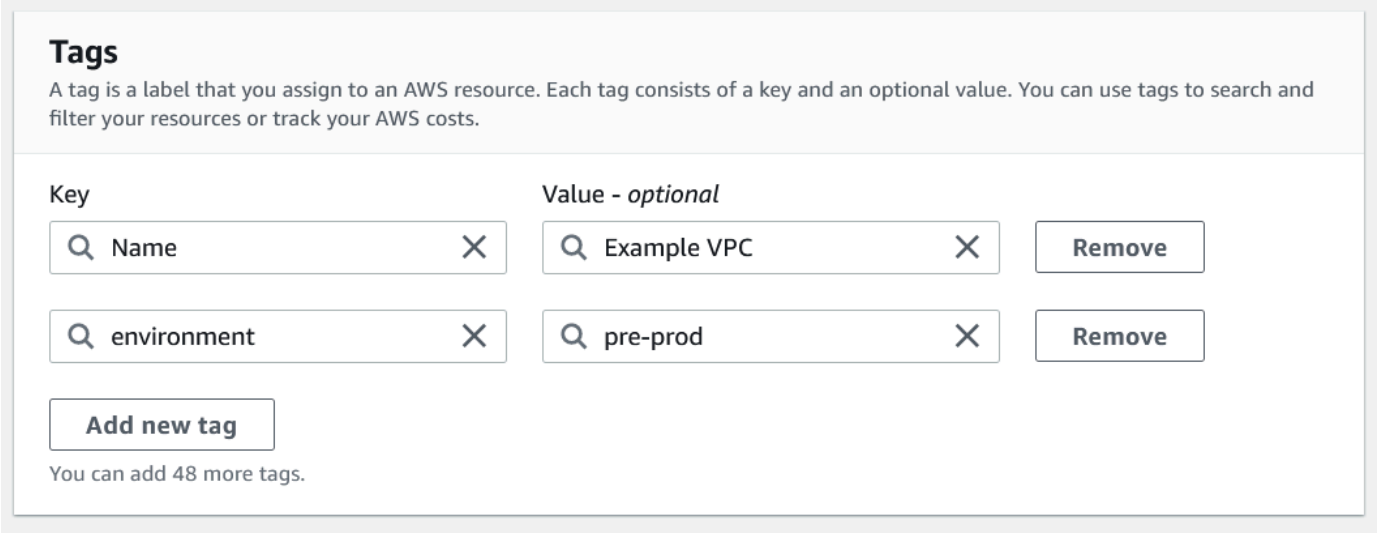
1. Utilizzando l'account membro, apri la console VPC https://console.aws.amazon.com/vpc/come account membro che utilizzerai come account sviluppatore.
2. Seleziona Crea VPC.
3. Esegui questa operazione:
    1. Inserisci un nome, come VPC di esempio.
    2. Scegli il blocco CIDR allocato su IPAM IPv4 .
    3. In pool IPv4 IPAM, scegli l'ID del pool di preproduzione.
    4. Scegli una lunghezza della Maschera di rete. Poiché hai limitato la lunghezza della maschera di rete disponibile per questo pool a /24 (in Fase 5: creazione di un pool di sviluppo di pre-produzione), l'unica opzione di maschera di rete disponibile è /24.



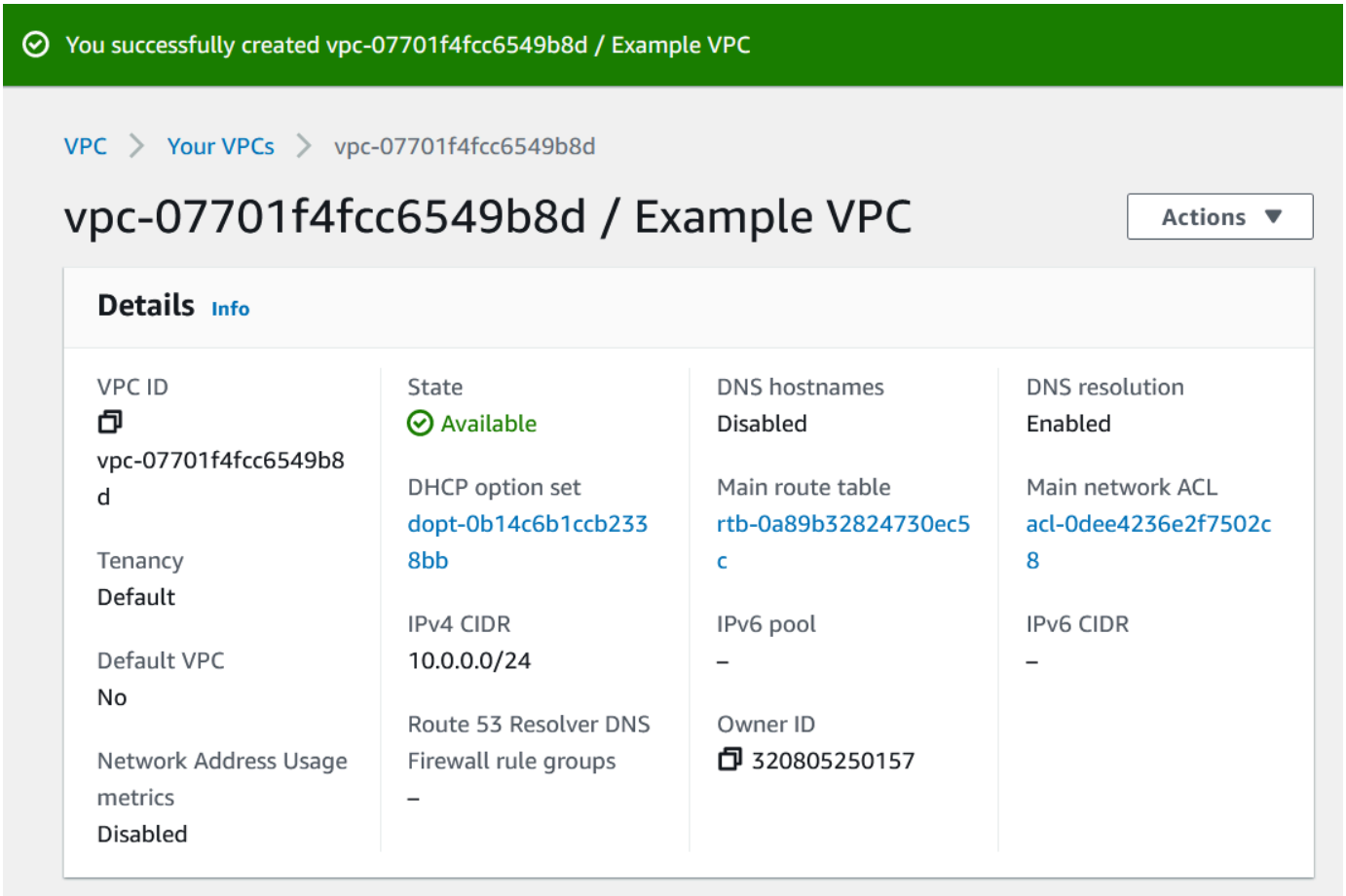
4. A scopo dimostrativo, in Tag, non aggiungere altri tag in questo momento. Quando avete creato il pool pre-prod (in[Fase 5: creazione di un pool di sviluppo di pre-produzione](#)), avete aggiunto una regola di allocazione che richiedeva VPCs che tutti quelli creati con questo pool abbiano per ora disattivato il tag environment/pre-prod tag. Leave the environment/pre -prod, in modo CIDRs da poter vedere che appare un errore che vi dice che non è stato aggiunto un tag richiesto.
5. Seleziona Crea VPC.
6. Viene visualizzato un errore che indica che non è stato aggiunto un tag obbligatorio. L'errore viene visualizzato perché hai impostato una regola di allocazione quando hai creato il pool di pre-produzione (in [Fase 5: creazione di un pool di sviluppo di pre-produzione](#)). La regola di allocazione richiedeva VPCs che tutte le regole create con questo pool avessero un tag CIDRs environment/pre-prod.



7. Ora, in Tag, aggiungi il tag ambiente/pre-prod e scegli nuovamente Crea VPC.



8. Il VPC è stato creato correttamente e il VPC è conforme alla regola dei tag sul pool di pre-produzione:



Nel pannello Risorse della console IPAM, l'amministratore IPAM sarà in grado di visualizzare e gestire il VPC e il relativo CIDR allocato. Tieni presente che occorre del tempo prima che il VPC venga visualizzato nel riquadro Risorse.

Fase 8: eliminazione

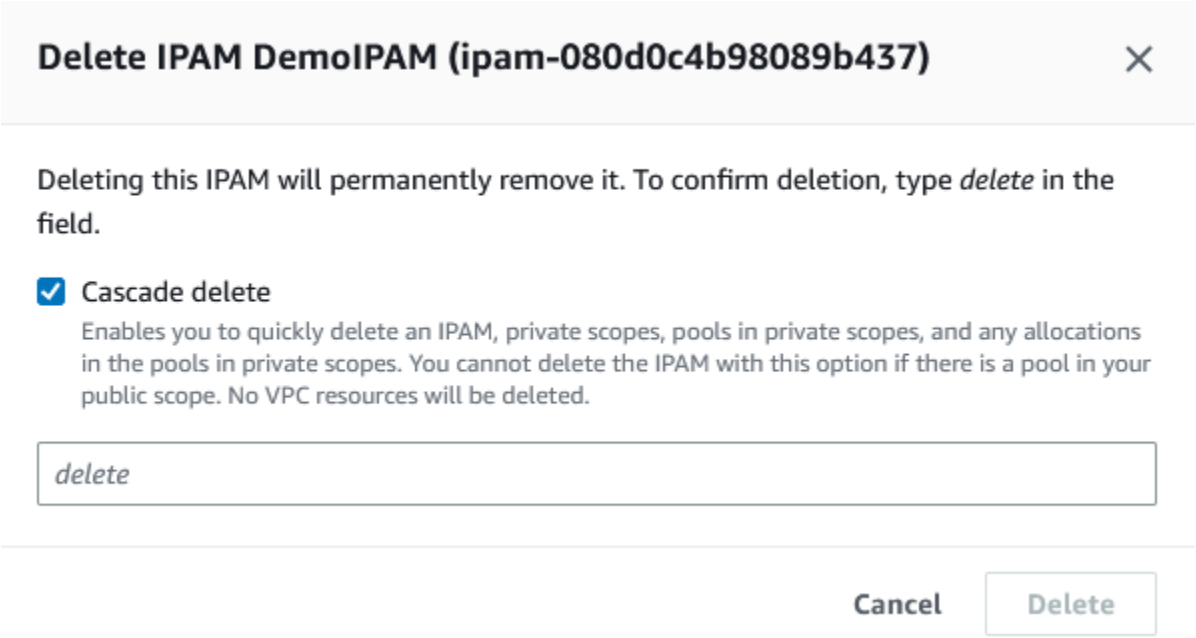
In questo tutorial, hai creato un IPAM con un amministratore delegato, creato più pool e abilitato un account membro della tua organizzazione ad allocare un CIDR VPC da un pool.

Segui i passaggi in questa sezione per eliminare le risorse che hai creato in questo tutorial.

Per eliminare le risorse create in questo tutorial

1. Utilizzando l'account membro che ha creato il VPC di esempio, elimina il VPC. Per istruzioni dettagliate, consulta Eliminazione del VPC nella Guida per l'utente di Amazon Virtual Private Cloud.

2. Utilizzando l'account amministratore IPAM, elimina l'esempio di condivisione di risorse nella console. AWS RAM Per istruzioni dettagliate, consulta Eliminazione di una condivisione di risorse in AWSAWS RAM nella Guida per l'utente di AWS Resource Access Manager .
3. Utilizzando l'account amministratore IPAM, accedi alla console RAM e disabilita la condivisione con AWS Organizations che abiliti in Fase 6.1. Abilitazione della condivisione delle risorse in AWS RAM.
4. Utilizzando l'account amministratore IPAM, elimina l'IPAM di esempio selezionando l'IPAM nella console IPAM e quindi scegliendo Azioni > Elimina. Per istruzioni dettagliate, vedi Elimina un IPAM.
5. Quando ti viene richiesto di eliminare l'IPAM, scegli Elimina a cascata. Questo eliminerà tutti gli ambiti e i pool all'interno dell'IPAM prima di eliminare l'IPAM.



6. Immetti elimina, quindi scegli Elimina.
7. Utilizzando l'account di AWS Organizations gestione, accedi alla console IPAM, scegli Impostazioni e rimuovi l'account amministratore delegato.
8. (Facoltativo) Quando integri IPAM con AWS Organizations, IPAM crea automaticamente un ruolo collegato al servizio in ogni account membro. Utilizzando ogni account AWS Organizations membro, accedi a IAM ed elimina il ruolo collegato al servizio AWSServiceRoleForIPAM in ogni account membro.
9. La pulizia è completa.

Tutorial: creare un IPAM e pool utilizzando il AWS CLI

Segui i passaggi di questo tutorial per utilizzare per AWS CLI creare un IPAM, creare pool di indirizzi IP e allocare un VPC con un CIDR da un pool IPAM.

Di seguito è riportata una gerarchia esemplificativa della struttura del pool che verrà creata seguendo i passaggi di questa sezione:

- IPAM che opera nella Regione 1, nella Regione 2 AWS AWS
  - Ambito privato
    - Pool di livello superiore
      - Pool regionale nella AWS Regione 2
        - Pool di sviluppo
          - Assegnazione per un VPC

> **Note**
>
> In questa sezione viene mostrato come creare un IPAM. Per impostazione predefinita, è possibile creare un solo IPAM. Per ulteriori informazioni, consulta Quote per l'IPAM. Se hai già delegato un account IPAM e creato un IPAM, puoi saltare i passaggi 1 e 2.

Indice

- Passaggio 1: abilitare IPAM nella tua organizzazione
- Passaggio 2: creare un IPAM
- Fase 3: Creare un pool di IPv4 indirizzi
- Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore
- Fase 5. Crea un pool Regionale con CIDR proveniente dal pool di livello superiore
- Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale
- Fase 7. Creare una condivisione RAM per abilitare le assegnazioni IP tra gli account
- Fase 8. Crea un VPC
- Fase 9. Rimozione

Passaggio 1: abilitare IPAM nella tua organizzazione

Questa fase è facoltativa. Completa questo passaggio per abilitare IPAM nella tua organizzazione e configurare l'IPAM delegato utilizzando la CLI. AWS Per ulteriori informazioni sul ruolo dell'account IPAM, consulta Integrare IPAM con gli account di un'organizzazione AWS.

Questa richiesta deve essere effettuata da un account di gestione di AWS Organizations. Quando si esegue il comando seguente, assicurarsi di utilizzare un ruolo con una policy IAM che consenta le seguenti azioni:

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

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

Si dovrebbe visualizzare il seguente output, che indica che l'abilitazione ha avuto successo.

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

Passaggio 2: creare un IPAM

Attenersi ai passaggi riportati in questa sezione per creare un IPAM e visualizzare ulteriori informazioni sugli ambiti creati. Utilizzerai questo IPAM quando crei pool ed effettui il provisioning degli intervalli di indirizzi IP per tali pool nei passaggi successivi.

> **Note**
>
> L'opzione Regioni operative determina per quali AWS regioni possono essere utilizzati i pool IPAM. Per ulteriori informazioni sulle Regioni operative, consulta Crea un IPAM.

Per creare un IPAM utilizzando il AWS CLI

1. Esegui il comando seguente per creare un'istanza IPAM.

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

Quando si crea un IPAM, AWS esegue automaticamente le seguenti operazioni:

- Restituisce un ID risorsa univoco globale (`IpamId`) per l'IPAM.
- Crea un ambito pubblico di default (`PublicDefaultScopeId`) e un ambito privato di default (`PrivateDefaultScopeId`).

```
{

    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-0de83dba6694560a9",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-0de83dba6694560a9",
        "PublicDefaultScopeId": "ipam-scope-02a24107598e982c5",
        "PrivateDefaultScopeId": "ipam-scope-065e7dfe880df679c",
        "ScopeCount": 2,
        "Description": "my-ipam",
        "OperatingRegions": [
            {
                "RegionName": "us-west-2"
            },
            {
                "RegionName": "us-east-1"
            }
        ],
        "Tags": []
    }
}
```

2. Esegui questo comando per visualizzare ulteriori informazioni relative agli ambiti. L'ambito pubblico è destinato agli indirizzi IP a cui si accede tramite Internet pubblico. L'ambito privato è destinato agli indirizzi IP a cui non si accede tramite Internet pubblico.

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

Nell'output vengono visualizzati gli ambiti disponibili. Verrà utilizzato l'ID dell'ambito privato nel passaggio successivo.


```
{
    "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
        }
    ]
}
```


Fase 3: Creare un pool di IPv4 indirizzi

Segui i passaggi di questa sezione per creare un pool di IPv4 indirizzi.

> **Important**
>
> Su questo pool di livello superiore non utilizzerai l'opzione `--locale`. In seguito, imposterai la località sul pool regionale. La località è la regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni CIDR. Come risultato della mancata configurazione della località sul pool di livello superiore, la località verrà impostata di default su `None`. Se un pool ha una lingua di`None`, il pool non sarà disponibile per le risorse VPC in nessuna AWS regione.

L'allocazione dello spazio degli indirizzi IP nel pool per riservare spazio può essere effettuata solo manualmente.

Per creare un pool di IPv4 indirizzi per tutte le AWS risorse, utilizza il AWS CLI

1. Esegui il comando seguente per creare un pool di IPv4 indirizzi. Utilizza l'ID dell'ambito privato dell'IPAM creato nel passaggio precedente.

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

   Nell'output, sarà visualizzabile uno stato `create-in-progress` per il pool.

```
{
    "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. Esegui il seguente comando fino a quando non viene visualizzato uno stato `create-complete` nell'output.

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

   Il seguente output esemplificativo mostra lo stato corretto.

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

Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore

Segui il passaggio descritto in questa sezione per effettuare il provisioning di un CIDR al pool di livello superiore, quindi verifica che sia stato effettuato il provisioning del CIDR. Per ulteriori informazioni, consulta Fornitura CIDRs a un pool.

Per fornire un blocco CIDR al pool utilizzando AWS CLI

1. Esegui il comando seguente per effettuare il provisioning del CIDR.

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

   Nell'output, è possibile verificare lo stato del provisioning.

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

```
    }
}
```

2. Esegui il seguente comando fino a quando non viene visualizzato uno stato `provisioned` nell'output.

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

Il seguente output esemplificativo mostra lo stato corretto.

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

Fase 5. Crea un pool Regionale con CIDR proveniente dal pool di livello superiore

Quando si crea un pool IPAM, per impostazione predefinita il pool appartiene alla AWS regione dell'IPAM. Quando si crea un VPC, il pool dal quale il VPC si estrae deve trovarsi nella stessa Regione del VPC. Puoi utilizzare l'opzione `--locale` quando crei un pool per rendere il pool disponibile ai servizi in una Regione diversa dalla Regione dell'IPAM. Attenersi ai passaggi riportati in questa sezione per creare un pool Regionale in un'altra località.

Per creare un pool con un CIDR proveniente dal pool precedente utilizzando la AWS CLI

1. Esegui il comando seguente per creare il pool e inserisci spazio con un CIDR noto disponibile dal pool precedente.

```
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
```

Nell'output, sarà visualizzabile l'ID del pool creato. Sarà necessario questo ID nel passaggio successivo.

```
{
    "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. Esegui il seguente comando fino a quando non viene visualizzato uno stato `create-complete` nell'output.

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

Nell'output, vedrai i pool contenuti nel tuo IPAM. In questo tutorial è stato creato un pool di livello superiore e un pool Regionale, in modo da vederli entrambi.

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

Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale

Segui il passaggio descritto in questa sezione per assegnare un blocco CIDR al pool e verificare che sia stato eseguito correttamente il provisioning.

Per assegnare un blocco CIDR al pool regionale utilizzando il AWS CLI

1. Esegui il comando seguente per effettuare il provisioning del CIDR.

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

Nell'output, sarà visualizzabile lo stato del pool.

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

2. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `provisioned` nell'output.

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

Il seguente output esemplificativo mostra lo stato corretto.

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

3. Esegui il seguente comando per effettuare una query sul pool di livello superiore per visualizzare le assegnazioni. Il pool Regionale è considerato un'assegnazione all'interno del pool di livello superiore.

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

Nell'output viene visualizzato il pool Regionale come assegnazione nel pool di livello superiore.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "10.0.0.0/16",
```

```
            "IpamPoolAllocationId": "ipam-pool-alloc-
fbd525f6c2bf4e77a75690fc2d93479a",
            "ResourceId": "ipam-pool-0da89c821626f1e4b",
            "ResourceType": "ipam-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Fase 7. Creare una condivisione RAM per abilitare le assegnazioni IP tra gli account

Questa fase è facoltativa. È possibile completare questo passaggio solo se Integrare IPAM con gli account di un'organizzazione AWS è stato completato.

Quando si crea una condivisione AWS RAM del pool IPAM, si abilitano le assegnazioni IP tra gli account. La condivisione della RAM è disponibile solo nella tua regione di residenza AWS . Si tenga presente che questa condivisione viene creata nella stessa Regione dell'IPAM, non nella Regione locale per il pool. Tutte le operazioni amministrative sulle risorse IPAM vengono effettuate attraverso la Regione di origine dell'IPAM. L'esempio in questo tutorial crea una singola condivisione per un singolo pool, ma è possibile aggiungere più pool a una singola condivisione. Per ulteriori informazioni, inclusa una spiegazione delle opzioni da inserire, consulta Condivisione di un pool IPAM tramite AWS RAM.

Esegui i seguenti comandi per creare una condivisione di risorse.

```
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
```

L'output indica che il pool è stato creato.

```
{
    "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
    }
}
```

Fase 8. Crea un VPC

Esegui il seguente comando per creare un VPC e assegnare un blocco CIDR al VPC dal pool nell'IPAM appena creato.

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

L'output indica che il VPC è stato creato.

```
{
    "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
    }
}
```

Fase 9. Rimozione

Segui i passaggi riportati in questa sezione per rimuovere le risorse IPAM che create in questo tutorial.

1. Elimina il VPC.

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

2. Elimina la condivisione RAM del pool IPAM.

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

3. Revoca il provisioning del CIDR del pool dal pool Regionale.

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

4. Revoca il provisioning del CIDR del pool dal pool di livello superiore.

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

5. Eliminare l'IPAM

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

Tutorial: Visualizza la cronologia degli indirizzi IP utilizzando il AWS CLI

Gli scenari descritti in questa sezione illustrano come analizzare e verificare l'utilizzo dell'indirizzo IP utilizzando la AWS CLI. Per informazioni generali sull'utilizzo di AWS CLI, vedere Utilizzo della Guida per l'utente dell'interfaccia AWS CLI a riga di AWS comando.

Indice

- Panoramica
- Scenari

Panoramica

IPAM conserva automaticamente i dati di monitoraggio dell'indirizzo IP per un massimo di tre anni. È possibile utilizzare i dati cronologici per analizzare e verificare le policy di sicurezza e routing della rete. È possibile cercare informazioni storiche dettagliate per i seguenti tipi di risorse:

- VPCs
- Sottoreti VPC
- Indirizzi IP elastici
- EC2 istanze in esecuzione
- EC2 interfacce di rete collegate alle istanze

Important

Sebbene IPAM non monitori EC2 le istanze Amazon o le interfacce di EC2 rete collegate alle istanze, puoi utilizzare la funzionalità di ricerca nella cronologia degli IP per cercare dati storici sull' EC2istanza e sull'interfaccia di rete. CIDRs

Note

- I comandi di questo tutorial devono essere eseguiti utilizzando l'account proprietario dell'IPAM e la AWS regione che ospita l'IPAM.
- I record delle modifiche CIDRs vengono raccolti in istantanee periodiche, il che significa che può essere necessario del tempo prima che i record appaiano o vengano aggiornati, e i valori relativi SampledStartTime e SampledEndTime possono differire dagli orari effettivi in cui si sono verificati.

Scenari

Gli scenari descritti in questa sezione illustrano come analizzare e verificare l'utilizzo dell'indirizzo IP utilizzando la AWS CLI. Per ulteriori informazioni sui valori menzionati in questo tutorial, come l'ora di fine e l'ora di inizio campionamento, consulta Visualizzazione della cronologia degli indirizzi IP.

Scenario 1: Quali risorse sono state associate con **`10.2.1.155/32`** tra l'1:00 e le 21:00 del 27 dicembre 2021 (UTC)?

1. Esegui il comando seguente:

```
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. Visualizza i risultati dell'analisi. Nell'esempio seguente, il CIDR è stato assegnato a un'interfaccia e a un' EC2 istanza di rete nel corso del periodo di tempo. Nota che nessun SampledEndTimevalore significa che il record è ancora attivo. Per ulteriori informazioni sui valori mostrati nell'output riportato di seguito, consulta Visualizzazione della cronologia degli indirizzi IP.

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "network-interface",
            "ResourceId": "eni-0b4e53eb1733aba16",
            "ResourceCidr": "10.2.1.155/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "instance",
            "ResourceId": "i-064da1f79baed14f3",
            "ResourceCidr": "10.2.1.155/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

Se l'ID proprietario dell'istanza a cui è collegata un'interfaccia di rete è diverso dall'ID proprietario dell'interfaccia di rete (come nel caso dei gateway NAT, delle interfacce di rete Lambda e di altri AWS servizi) VPCs, `ResourceOwnerId` è `amazon-aws` anziché l'ID account del proprietario

dell'interfaccia di rete. L'esempio seguente mostra il registro di un CIDR associato a un gateway NAT:

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "network-interface",
            "ResourceId": "eni-0b4e53eb1733aba16",
            "ResourceCidr": "10.0.0.176/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "amazon-aws",
            "ResourceRegion": "us-east-1",
            "ResourceType": "instance",
            "ResourceCidr": "10.0.0.176/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

Scenario 2: Quali risorse sono state associate con **`10.2.1.0/24`** tra il 1° dicembre 2021 e il 27 dicembre 2021 (UTC)?

1. Esegui il comando seguente:

```
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. Visualizza i risultati dell'analisi. Nell'esempio seguente, il CIDR è stato allocato a una sottorete e VPC nel periodo di tempo. Nota che nessun SampledEndTimevalore significa che il record è ancora attivo. Per ulteriori informazioni sui valori mostrati nell'output riportato di seguito, consulta Visualizzazione della cronologia degli indirizzi IP.

```
{
    "HistoryRecords": [
```

```
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0864c82a42f5bffed",
            "ResourceCidr": "10.2.1.0/24",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0f5ee7e1ba908a378",
            "ResourceCidr": "10.2.1.0/24",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

Scenario 3: Quali risorse sono state associate con **2605:9cc0:409::/56** tra il 1° dicembre 2021 e il 27 dicembre 2021 (UTC)?

1. Esegui il seguente comando, dove --region è la regione di origine dell'IPAM:

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

2. Visualizza i risultati dell'analisi. Nell'esempio seguente, il CIDR è stato assegnato a due diversi VPCs nel corso del periodo di tempo in una regione al di fuori della regione di origine dell'IPAM. Nota che nessun SampledEndTimevalore significa che il record è ancora attivo. Per ulteriori informazioni sui valori mostrati nell'output riportato di seguito, consulta Visualizzazione della cronologia degli indirizzi IP.

```
{
    "HistoryRecords": [
        {
```

```
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-01d967bf3b923f72c",
            "ResourceCidr": "2605:9cc0:409::/56",
            "ResourceName": "First example VPC",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-01d967bf3b923f72c",
            "SampledStartTime": "2021-12-23T20:02:00.701000+00:00",
            "SampledEndTime": "2021-12-23T20:12:59.848000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-03e62c7eca81cb652",
            "ResourceCidr": "2605:9cc0:409::/56",
            "ResourceName": "Second example VPC",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-03e62c7eca81cb652",
            "SampledStartTime": "2021-12-27T15:11:00.046000+00:00"
        }
    ]
}
```

Scenario 4: Quali risorse sono state associate con **`10.0.0.0/24`** nelle ultime 24 ore (supponendo che l'ora corrente sia mezzanotte del 27 dicembre 2021 (UTC))?

1. Esegui il comando seguente:

```
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. Visualizza i risultati dell'analisi. Nell'esempio seguente, il CIDR è stato assegnato a numerose sottoreti e VPCs nel periodo di tempo. Nota che nessun SampledEndTimevalore significa che il record è ancora attivo. Per ulteriori informazioni sui valori mostrati nell'output riportato di seguito, consulta Visualizzazione della cronologia degli indirizzi IP.

```
{
```

```
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0d1b8f899725aa72d",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "VpcId": "vpc-042b8a44f64267d67",
            "SampledStartTime": "2021-12-11T16:35:59.074000+00:00",
            "SampledEndTime": "2021-12-28T15:34:00.017000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-09754dfd85911abec",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-09754dfd85911abec",
            "SampledStartTime": "2021-12-27T20:07:59.947000+00:00",
            "SampledEndTime": "2021-12-28T15:34:00.017000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-west-2",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0a8347f594bea5901",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
            "ResourceComplianceStatus": "unmanaged",
            "ResourceOverlapStatus": "overlapping",
            "VpcId": "vpc-0a8347f594bea5901",
            "SampledStartTime": "2021-12-11T16:35:59.318000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0af7eadb0798e9148",
            "ResourceCidr": "10.0.0.0/24",
            "ResourceName": "Example name",
```

```
            "VpcId": "vpc-03298ba16756a8736",
            "SampledStartTime": "2021-12-14T21:07:22.357000+00:00"
        }
    ]
}
```

Scenario 5: Quali risorse sono attualmente associate con **`10.2.1.155/32`**?

1. Esegui il comando seguente:

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

2. Visualizza i risultati dell'analisi. Nell'esempio seguente, il CIDR è stato assegnato a un'interfaccia e a un' EC2 istanza di rete nel periodo di tempo. Nota che nessun SampledEndTimevalore significa che il record è ancora attivo. Per ulteriori informazioni sui valori mostrati nell'output riportato di seguito, consulta Visualizzazione della cronologia degli indirizzi IP.

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "network-interface",
            "ResourceId": "eni-0b4e53eb1733aba16",
            "ResourceCidr": "10.2.1.155/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "instance",
            "ResourceId": "i-064da1f79baed14f3",
            "ResourceCidr": "10.2.1.155/32",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

Scenario 6: Quali risorse sono attualmente associate con **`10.2.1.0/24`**?

1. Esegui il comando seguente:

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

2. Visualizza i risultati dell'analisi. Nell'esempio seguente, nel periodo di tempo il CIDR è stato allocato a un VPC e una sottorete. Solo i risultati che corrispondono esattamente a questo CIDR `/24` vengono restituiti, non tutti i codici `/32` all'interno del CIDR `/24`. Nota che nessun SampledEndTimevalore significa che il record è ancora attivo. Per ulteriori informazioni sui valori mostrati nell'output riportato di seguito, consulta Visualizzazione della cronologia degli indirizzi IP.

```
{
    "HistoryRecords": [
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "subnet",
            "ResourceId": "subnet-0864c82a42f5bffed",
            "ResourceCidr": "10.2.1.0/24",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        },
        {
            "ResourceOwnerId": "123456789012",
            "ResourceRegion": "us-east-1",
            "ResourceType": "vpc",
            "ResourceId": "vpc-0f5ee7e1ba908a378",
            "ResourceCidr": "10.2.1.0/24",
            "ResourceComplianceStatus": "compliant",
            "ResourceOverlapStatus": "nonoverlapping",
            "VpcId": "vpc-0f5ee7e1ba908a378",
            "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
        }
    ]
}
```

Scenario 7: Quali risorse sono attualmente associate con **`54.0.0.9/32`**?

In questo esempio, `54.0.0.9/32` viene assegnato a un indirizzo IP elastico che non fa parte dell' AWS organizzazione integrata con l'IPAM.

1. Esegui il comando seguente:

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

2. Poiché `54.0.0.9/32` è assegnato a un indirizzo IP elastico che non fa parte dell' AWS organizzazione integrata con l'IPAM in questo esempio, non viene restituito alcun record.

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

Tutorial: Porta il tuo ASN in IPAM

Se le tue applicazioni utilizzano indirizzi IP affidabili e numeri di sistema autonomi (ASNs) consentiti dai tuoi partner o clienti elencati nella loro rete, puoi eseguire queste applicazioni AWS senza richiedere ai tuoi partner o clienti di modificare i loro elenchi di autorizzazioni.

Un Numero di sistema autonomo (ASN) è un numero unico a livello globale che consente l'identificazione di un gruppo di reti su Internet e lo scambio di dati di routing con altre reti in maniera dinamica tramite Border Gateway Protocol. I provider di servizi Internet (ISPs), ad esempio, lo utilizzano ASNs per identificare la fonte del traffico di rete. Non tutte le organizzazioni ne acquistano uno proprio ASNs, ma le organizzazioni che lo fanno possono portare il proprio ASN a AWS.

Bring your own autonomous system number (BYOASN) ti consente di pubblicizzare IPv6 gli indirizzi IPv4 o gli indirizzi a AWS cui porti utilizzando il tuo ASN pubblico anziché l'ASN. AWS Quando utilizzi BYOASN, il traffico in origine dal tuo indirizzo IP trasporta il tuo ASN anziché l'ASN AWS e i tuoi carichi di lavoro sono raggiungibili da clienti o partner che hanno inserito nella lista di accettazione il traffico basato sul tuo indirizzo IP e ASN.

⚠ Important

- Completa questo tutorial utilizzando l'account di amministratore IPAM nella regione di origine del tuo IPAM.

- Questo tutorial presuppone che tu sia il proprietario dell'ASN pubblico che desideri trasferire su IPAM e che tu abbia già portato un CIDR BYOIP e lo abbia fornito a un pool di ambito pubblico. AWS Puoi inserire un ASN in IPAM in qualsiasi momento, ma per utilizzarlo devi associarlo a un CIDR che hai inserito nel tuo account. AWS Questo tutorial presuppone che tu abbia già effettuato questa operazione. Per ulteriori informazioni, consulta Tutorial: trasferisci i tuoi indirizzi IP su IPAM.
- Puoi passare dalla pubblicità al tuo ASN o a un AWS ASN senza indugio, ma sei limitato a passare da un AWS ASN al tuo ASN una volta all'ora.
- Se il tuo CIDR BYOIP attualmente è pubblicizzato, non devi ritirarlo dalla pubblicità per associarlo al tuo ASN.

Prerequisiti di onboarding per l'ASN

Per completare questo tutorial, occorre quanto indicato di seguito:

- Il tuo ASN pubblico a 2 o 4 byte.
- Se hai già inserito un intervallo di indirizzi IPTutorial: trasferisci i tuoi indirizzi IP su IPAM, ti serve AWS l'intervallo CIDR di indirizzi IP. Sarà inoltre necessaria una chiave privata. Puoi utilizzare la chiave privata che hai creato quando hai portato l'intervallo CIDR degli indirizzi IP AWS oppure puoi creare una nuova chiave privata come descritto in Creare una chiave privata e generare un certificato X.509 nella Amazon EC2 User Guide.
- Quando aggiungi un intervallo di IPv6 indirizzi IPv4 o a AWS withTutorial: trasferisci i tuoi indirizzi IP su IPAM, crei un certificato X.509 e carichi il certificato X.509 nel record RDAP del tuo RIR. È necessario caricare lo stesso certificato creato nel record RDAP del RIR per l'ASN. Assicurati di includere le stringhe `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` prima e dopo la porzione codificata. Tutto questo contenuto deve trovarsi su un'unica linea lunga. La procedura per l'aggiornamento di RDAP dipende dal RIR:
  - Per ARIN, utilizza il portale Account Manager per aggiungere il certificato nella sezione "Commenti pubblici" per l'oggetto "Informazioni di rete" che rappresenta l'ASN utilizzando l'opzione "Modifica ASN". Non aggiungerlo alla sezione commenti dell'organizzazione.
  - Per RIPE, aggiungi il certificato come nuovo campo "descr" all'oggetto "aut-num" che rappresenta il tuo ASN. Di solito si trovano nella sezione "Le mie risorse" del

    portale del database RIPE. Non aggiungerlo alla sezione commenti della tua organizzazione o al campo "osservazioni" dell'oggetto "aut-num".

  - Per APNIC, invia via email il certificato a helpdesk@apnic.net per aggiungerlo manualmente al campo "osservazioni" per il tuo ASN. Invia l'e-mail utilizzando il contatto autorizzato APNIC per l'ASN.
- Quando trasferisci un intervallo di indirizzi IP in IPAM, crei un ROA per verificare di controllare lo spazio di indirizzi IP che stai trasferendo a IPAM. Oltre a quel ROA, devi averne un secondo nel RIR con l'ASN che stai trasferendo a IPAM. Se non hai questo secondo ROA per l'ASN nel tuo RIR, completa 3. Creazione di un oggetto ROA nel RIR. Ignora gli altri passaggi.

Passaggi del tutorial

Completa i passaggi seguenti utilizzando la console o il. AWS AWS CLI

AWS Management Console

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel riquadro di navigazione a sinistra, scegliere IPAMs.
3. Scegli il tuo IPAM.
4. Scegli la BYOASNsscheda e scegli Fornitura BYOASNs.
5. Inserisci l'ASN. In tal modo, il campo Message (Messaggio) viene compilato automaticamente con il messaggio necessario per l'accesso al passaggio successivo.

   - Il formato del messaggio è il seguente, dove ACCOUNT è il numero del tuo AWS account, ASN è l'ASN che stai trasferendo a IPAM e YYYYMMDD è la data di scadenza del messaggio (che per impostazione predefinita è l'ultimo giorno del mese successivo). Esempio:

     ```
     text_message="1|aws|ACCOUNT|ASN|YYYYMMDD|SHA256|RSAPSS"
     ```
6. Copia il messaggio e sostituisci la data di scadenza con un valore tuo, se necessario.
7. Firma il messaggio utilizzando la chiave privata. Esempio:

   ```
   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. In Firma, inserisci la firma.

9. (Facoltativo) Per eseguire il provisioning di un altro ASN, scegli Esegui il provisioning di un ASN. Puoi fornire fino a 5. ASNs Per aumentare questa quota, consulta Quote per l'IPAM.
10. Scegli Provision (Esegui il provisioning).
11. Visualizza il processo di provisioning nella BYOASNsscheda. Attendi che lo Stato passi da Pending-Provisioning a Provisioned. BYOASNs in uno stato di Failed-provisioning vengono rimossi automaticamente dopo 7 giorni. Una volta eseguito correttamente il provisioning dell'ASN, puoi associarlo a un CIDR BYOIP.
12. Nel riquadro di navigazione a sinistra, seleziona Pools (Pool).
13. Scegli il tuo ambito pubblico. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
14. Scegli un pool regionale di cui sia stato eseguito il provisioning di un CIDR BYOIP. Il pool deve avere Service impostato su EC2e deve avere una locale scelta.
15. Scegli la CIDRsscheda e seleziona un CIDR BYOIP.
16. Scegli Actions (Azioni) > Manage BYOASN associations (Gestisci associazioni BYOASN).
17. In Associato BYOASNs, scegli l'ASN a cui ti sei trasferito. AWS Se ne hai più ASNs, puoi associarne più ASNs al CIDR BYOIP. Puoi associarne quanti ne puoi portare ASNs a IPAM. Tieni presente che per impostazione predefinita puoi portarne fino a 5 ASNs a IPAM. Per ulteriori informazioni, consulta Quote per l'IPAM.
18. Selezionare Associate (Associa).
19. Attendi il completamento dell'associazione ASN. Una volta che l'ASN è stato associato correttamente al CIDR BYOIP, puoi pubblicizzare nuovamente il CIDR BYOIP.
20. Scegli la CIDRsscheda piscina.
21. Seleziona il CIDR BYOIP e scegli Actions (Operazioni) > Advertise (Pubblicizzazione). Di conseguenza, vengono visualizzate le tue opzioni ASN: Amazon ASN e tutte le opzioni che ASNs hai portato a IPAM.
22. Seleziona l'ASN che hai portato in IPAM e scegli Advertise CIDR (Pubblicizza CIDR). In tal modo, il CIDR BYOIP viene pubblicizzato e il valore nella colonna Advertising (Pubblicità) passa da Withdrawn (Ritirato) a Advertised (Pubblicizzato). La colonna Autonomous System Number (Numero di sistema autonomo) visualizza l'ASN associato al CIDR.
23. (Facoltativo) Se decidi di cambiare nuovamente l'associazione ASN nell'ASN Amazon, seleziona il CIDR BYOIP e scegli nuovamente Actions (Azioni) > Advertise (Pubblicizza). Questa volta, scegli l'ASN Amazon. Puoi tornare all'ASN Amazon in qualunque momento, ma puoi passare a un ASN personalizzato solo una volta all'ora.

Il tutorial è terminato.

Rimozione

1. Dissocia l'ASN dal CIDR BYOIP

   - Per ritirare il CIDR BYOIP dalla pubblicità, nel pool nell'ambito pubblico, scegli il CIDR BYOIP, quindi scegli Actions (Azioni) > Withdraw from advertising (Ritiro dalla pubblicità).
   - Per dissociare l'ASN dal CIDR, scegli Actions (Azioni) > Manage BYOASN associations (Gestisci associazioni BYOASN).

2. Annullamento del provisioning dell'ASN

   - Per effettuare il deprovisioning dell'ASN, nella BYOASNs scheda, scegli l'ASN e scegli Deprovisioning ASN. Di conseguenza, l'ASN viene disattivato. BYOASNs in uno stato di disattivazione vengono rimossi automaticamente dopo 7 giorni.

La pulizia è completa.

Command line

1. Fornisci il tuo ASN includendo l'ASN e il messaggio di autorizzazione. La firma è il messaggio firmato con la chiave privata.

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

2. Descrivi il tuo ASN per monitorare il processo di provisioning. Se la richiesta ha esito positivo, dopo alcuni minuti dovresti vedere il ProvisionStatusset impostato su Provisioned.

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

3. Associa il tuo ASN al tuo CIDR BYOIP. Qualunque ASN personalizzato da cui desideri pubblicizzare deve prima essere associato al tuo CIDR.

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

4. Descrivi il tuo CIDR per tracciare il processo di associazione.

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

5. Pubblicizza il tuo CIDR con il tuo ASN. Se il CIDR è già pubblicizzato, l'ASN di origine da Amazon diventerà tuo.

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

6. Descrivi il tuo CIDR per vedere lo stato ASN passare da associated (associato) a advertised (pubblicizzato).

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

Il tutorial è terminato.

Rimozione

1. Esegui una di queste operazioni:

   - Per ritirare solo la tua pubblicità ASN e tornare a utilizzare Amazon ASNs mantenendo pubblicizzato il CIDR, devi chiamare advertise-byoip-cidr con il AWS valore speciale per il parametro asn. Puoi tornare all'ASN Amazon in qualunque momento, ma puoi passare a un ASN personalizzato solo una volta all'ora.

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

   - Per ritirare contemporaneamente la tua pubblicità CIDR e ASN, puoi chiamare. withdraw-byoip-cidr

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

2. Per ripulire il tuo ASN, devi prima annullarne l’associazione dal CIDR BYOIP.

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

3. Una volta dissociato il tuo ASN da tutti i BYOIP a cui lo hai CIDRs associato, puoi rimuoverlo.

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

4. Il provisioning del CIDR BYOIP può essere annullato anche dopo la rimozione di tutte le associazioni ASN.

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

5. Conferma l'annullamento del provisioning.

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

La pulizia è completa.

Tutorial: trasferisci i tuoi indirizzi IP su IPAM

I tutorial di questa sezione illustrano il processo di trasferimento dello spazio di indirizzi IP pubblici AWS e della gestione dello spazio con IPAM.

La gestione dello spazio di indirizzo IP pubblico con IPAM ha i seguenti vantaggi:

- Migliora l'utilizzo degli indirizzi IP pubblici in tutta l'organizzazione: È possibile utilizzare IPAM per condividere lo spazio degli indirizzi IP tra gli account AWS . Senza utilizzare IPAM, non è possibile condividere lo spazio IP pubblico tra gli account di AWS Organizations.
- Semplifica il processo di trasferimento dello spazio IP pubblico a AWS: è possibile utilizzare IPAM per integrare lo spazio di indirizzi IP pubblico una sola volta, quindi utilizzare IPAM per distribuire il pubblico tra le IPs regioni su risorse come istanze e sistemi di bilanciamento del carico delle applicazioni. EC2 Senza IPAM, è necessario effettuare l'onboarding del pubblico per ogni regione. IPs AWS

Indice

- Verifica il controllo del dominio
- Porta il tuo IP su IPAM utilizzando sia la console di AWS gestione che la CLI AWS
- Porta il tuo IP CIDR su IPAM usando solo la CLI AWS

Verifica il controllo del dominio

Prima di aggiungere un intervallo di indirizzi IP a AWS, è necessario utilizzare una delle opzioni descritte in questa sezione per verificare di controllare lo spazio degli indirizzi IP. Successivamente, quando si porta l'intervallo di indirizzi IP a AWS, AWS verifica che sia l'utente a controllare

l'intervallo di indirizzi IP. Questa convalida garantisce che i clienti non possano utilizzare intervalli IP appartenenti ad altri, prevenendo problemi di routing e sicurezza.

Esistono due metodi che è possibile utilizzare per verificare il controllo dell'intervallo:

- Certificato X.509: se l'intervallo di indirizzi IP è registrato in un registro Internet che supporta RDAP (come ARIN, RIPE e APNIC), è possibile utilizzare un certificato X.509 per verificare la proprietà del dominio.
- Record TXT DNS: indipendentemente dal fatto che il registro Internet supporti RDAP, è possibile utilizzare un token di verifica e un record TXT DNS per verificare la proprietà del dominio.

Indice

- Verifica il dominio con un certificato X.509
- Verifica il dominio con un record TXT DNS

Verifica il dominio con un certificato X.509

Questa sezione descrive come verificare il dominio con un certificato X.509 prima di trasferire l'intervallo di indirizzi IP su IPAM.

Per verificare il dominio con un certificato X.509

1. Completa i tre passaggi indicati nella sezione Prerequisiti per BYOIP in Amazon EC2 nella Amazon EC2 User Guide.

   > **Note**
   >
   > Quando crei il ROAs, for IPv4 CIDRs devi impostare la lunghezza massima del prefisso di un indirizzo IP su. `/24` Infatti IPv6 CIDRs, se li stai aggiungendo a un pool pubblicizzabile, la lunghezza massima del prefisso di un indirizzo IP deve essere. `/48` Ciò garantisce la massima flessibilità per dividere l'indirizzo IP pubblico tra AWS le regioni. IPAM applica la lunghezza massima impostata. La lunghezza massima è il più piccolo avviso di lunghezza del prefisso che puoi consentire per questo percorso. Ad esempio, se porti un blocco CIDR `/20` su AWS impostando la lunghezza massima su `/24`, puoi dividere il blocco più grande come preferisci (come ad esempio con `/21`, `/22` oppure `/24`) e distribuire i blocchi CIDR più piccoli in qualsiasi regione. Se hai impostato la lunghezza massima su `/23`, non puoi dividere e pubblicizzare un `/24` dal blocco più

grande. Inoltre, tieni presente che `/24` è il IPv4 blocco più piccolo ed `/48` è il IPv6 blocco più piccolo che puoi pubblicizzare da una regione a Internet.

2. Completa i passaggi 1 e 2 solo nella sezione Fornisci un intervallo di indirizzi pubblicizzabile pubblicamente AWS nella Amazon EC2 User Guide e non fornire ancora l'intervallo di indirizzi (passaggio 3). Salva `text_message` e `signed_message`. Saranno necessari più avanti in questa processo.

Dopo aver completato questi passaggi, continua con Porta il tuo IP su IPAM utilizzando sia la console di AWS gestione che la CLI AWS o Porta il tuo IP CIDR su IPAM usando solo la CLI AWS.

Verifica il dominio con un record TXT DNS

Completa i passaggi in questa sezione per verificare il dominio con un record TXT DNS prima di trasferire l'intervallo di indirizzi IP su IPAM.

Puoi utilizzare i record TXT DNS per verificare di avere il controllo di un intervallo di indirizzi IP pubblico. Un record TXT DNS è un tipo di record DNS che contiene informazioni sul nome di dominio. Questa funzionalità consente di importare gli indirizzi IP registrati con qualsiasi registro Internet (come JPNIC, LACNIC e AFRINIC), non solo quelli che supportano le convalide basate su record RDAP (Registration Data Access Protocol), come ARIN, RIPE e APNIC.

Important

Prima di continuare, è necessario aver già creato un IPAM nel piano gratuito o avanzato. Se non disponi di un IPAM, completa prima Crea un IPAM.

Indice

- Passaggio 1: creare un ROA, se non ne hai già uno
- Fase 2: Crea un token di verifica
- Fase 3. Configura la zona DNS e il record TXT

Passaggio 1: creare un ROA, se non ne hai già uno

Devi disporre di un ROA (Route Origin Authorization) nel tuo RIR (Regional Internet Registry) per gli intervalli di indirizzi IP che desideri pubblicizzare. Se non hai un ROA nel RIR, completa 3. Crea un oggetto ROA nel tuo RIR nella Amazon EC2 User Guide. Ignora gli altri passaggi.

L'intervallo di IPv4 indirizzi più specifico che puoi inserire è /24. L'intervallo di IPv6 indirizzi più specifico che puoi inserire è /48 per gli indirizzi pubblicizzabili pubblicamente e /60 per CIDRs quelli CIDRs che non sono pubblicizzabili pubblicamente.

Fase 2: Crea un token di verifica

Un token di verifica è un valore casuale AWS generato in modo casuale che puoi utilizzare per dimostrare il controllo di una risorsa esterna. Ad esempio, puoi utilizzare un token di verifica per confermare che controlli un intervallo di indirizzi IP pubblico quando porti un intervallo di indirizzi IP a AWS (BYOIP).

Completa i passaggi di questa sezione per creare un token di verifica, necessario in un passaggio successivo di questo tutorial per portare l'intervallo di indirizzi IP su IPAM. Utilizza le istruzioni riportate di seguito per la AWS console o per. AWS CLI

AWS Management Console

Per creare un token di verifica

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nella console di AWS gestione, scegli la AWS regione in cui hai creato il tuo IPAM.
3. Nel riquadro di navigazione a sinistra, scegliere IPAMs.
4. Scegli l'IPAM e poi seleziona la scheda Token di verifica.
5. Seleziona Crea token di verifica.
6. Dopo aver creato il token, lascia aperta questa scheda del browser. Avrai bisogno del Valore del token e del Nome del token nel passaggio successivo e poi successivamente dell'ID token.

Tieni presente quanto segue:

- Dopo aver creato un token di verifica, puoi riutilizzarlo per più BYOIP CIDRs forniti dal tuo IPAM entro 72 ore. Se desideri fornire altri token CIDRs dopo 72 ore, hai bisogno di un nuovo token.
- Puoi creare fino a 100 token. Se raggiungi il limite, elimina i token scaduti.

Command line

- Richiedi che IPAM crei un token di verifica da utilizzare per la configurazione DNS con create-ipam-external-resource -verification-token:

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

Ciò restituirà un token IpamExternalResourceVerificationTokenId and con e e `TokenName` e `TokenValue` l'ora di scadenza () del token. `NotAfter`

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

Tieni presente quanto segue:

- Dopo aver creato un token di verifica, puoi riutilizzarlo per più BYOIP forniti CIDRs dal tuo IPAM entro 72 ore. Se desideri fornire altri token CIDRs dopo 72 ore, hai bisogno di un nuovo token.
- Puoi visualizzare i tuoi token utilizzando describe-ipam-external-resource-verification-tokens.
- Puoi creare fino a 100 token. Se raggiungi il limite, puoi eliminare i token scaduti utilizzando - verification-token. delete-ipam-external-resource

Fase 3. Configura la zona DNS e il record TXT

Completa la procedura descritta in questa sezione per configurare la zona DNS e il record TXT. Se non utilizzi Route 53 come DNS, segui la documentazione fornita dal provider DNS per configurare una zona DNS e aggiungere un record TXT.

Se utilizzi Route 53, tieni presente quanto segue:

- Per creare una zona di ricerca inversa nella AWS console, consulta Creazione di una zona ospitata pubblica nella Amazon Route 53 Developer Guide o usa il AWS CLI comando create-hosted-zone.

- Per creare un record nella zona di ricerca inversa della AWS console, consulta Creazione di record utilizzando la console Amazon Route 53 nella Amazon Route 53 Developer Guide o usa il AWS CLI comando change-resource-record-sets.
- Dopo aver creato la zona ospitata, delegala dal RIR ai server dei nomi forniti da Route 53 (ad esempio LACNIC o APNIC).

Sia che utilizzi un altro provider DNS o Route 53, tieni presente quanto segue durante la configurazione del record TXT:

- Il nome del record deve essere il nome del token.
- Il tipo di record deve essere TXT.
- ResourceRecord Il valore deve essere il valore del token.

Esempio:

- Nome: `86950620.113.0.203.in-addr.arpa`
- Tipo: TXT
- ResourceRecords Value (Valore): `a34597c3-5317-4238-9ce7-50da5b6e6dc8`

Dove:

- `86950620` è il nome del token di verifica.
- `113.0.203.in-addr.arpa` è il nome della zona di ricerca inversa.
- TXT è il tipo di record.
- `a34597c3-5317-4238-9ce7-50da5b6e6dc8` è il valore del token di verifica.

> **Note**
>
> A seconda della dimensione del prefisso da trasferire a IPAM con BYOIP, è necessario creare uno o più record di autenticazione nel DNS. Questi record di autenticazione sono del tipo di record TXT e devono essere collocati nella zona inversa del prefisso stesso o del prefisso principale.
>
> - Infatti IPv4, i record di autenticazione devono allinearsi agli intervalli in corrispondenza del limite di ottetti che costituiscono il prefisso.

- Examples (Esempi)
- Per 198.18.123.0/24, che è già allineato al limite di un ottetto, è necessario creare un singolo record di autenticazione su:
  - *token-name*.123.18.198.in-addr.arpa. IN TXT "*token-value*"
- Per 198.18.12.0/22, che non è allineato al limite dell'ottetto, è necessario creare quattro record di autenticazione. Questi record devono coprire le sottoreti 198.18.12.0/24, 198.18.13.0/24, 198.18.14.0/24 e 198.18.15.0/24 che sono allineate al limite di un ottetto. Le voci DNS corrispondenti devono essere:
  - *token-name*.12.18.198.in-addr.arpa. IN TXT "*token-value*"
  - *token-name*.13.18.198.in-addr.arpa. IN TXT "*token-value*"
  - *token-name*.14.18.198.in-addr.arpa. IN TXT "*token-value*"
  - *token-name*.15.18.198.in-addr.arpa. IN TXT "*token-value*"
- Per 198.18.0.0/16, che è già allineato al limite di un ottetto, è necessario creare un singolo record di autenticazione:
  - *token-name*.18.198.in-addr.arpa. IN TXT "*token-value*"

- Infatti IPv6, i record di autenticazione devono allinearsi agli intervalli al limite del nibble che compongono il prefisso. I valori nibble validi sono ad esempio 32, 36, 40, 44, 48, 52, 56 e 60.
  - Examples (Esempi)
    - Per 2001:0db8::/40, che è già allineato al limite di nibble, è necessario creare un singolo record di autenticazione:
      - *token-name*.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
    - Per 2001:0db8:80::/42, che non è allineato al limite di nibble, è necessario creare quattro record di autenticazione. Questi record devono coprire le sottoreti 2001:db8:80::/44, 2001:db8:90::/44, 2001:db8:a0::/44 e 2001:db8:b0::/44 che sono allineate al limite di un nibble. Le voci DNS corrispondenti devono essere:
      - *token-name*.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
      - *token-name*.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
      - *token-name*.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
      - *token-name*.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
    - Per l'intervallo non pubblicizzato 2001:db8:0:1000::/54, che non è allineato al limite di un nibble, è necessario creare quattro record di autenticazione. Questi record devono

coprire le sottoreti 2001:db8:0:1000::/56, 2001:db8:0:1100::/56, 2001:db8:0:1200::/56 e 2001:db8:0:1300::/56 che sono allineate sul limite di un nibble. Le voci DNS corrispondenti devono essere:

- *token-name*.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
- *token-name*.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
- *token-name*.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
- *token-name*.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"

- Per convalidare il numero corretto di numeri esadecimali tra token-name e la stringa "ip6.arpa", moltiplica il numero per quattro. Il risultato deve corrispondere alla lunghezza del prefisso. Ad esempio, per un prefisso /56 dovresti avere 14 cifre esadecimali.

Dopo aver completato questi passaggi, continua con Porta il tuo IP su IPAM utilizzando sia la console di AWS gestione che la CLI AWS o Porta il tuo IP CIDR su IPAM usando solo la CLI AWS.

Porta il tuo IP su IPAM utilizzando sia la console di AWS gestione che la CLI AWS

Bringing Your Own IP (BYOIP) su IPAM ti consente di utilizzare gli intervalli di indirizzi esistenti e quelli IPv4 della tua organizzazione. IPv6 AWS Ciò consente di mantenere un marchio coerente, migliorare le prestazioni di rete, aumentare la sicurezza e semplificare la gestione unificando gli ambienti on-premises e cloud nello spazio di indirizzi IP.

Segui questi passaggi per portare un IPv4 o IPv6 CIDR a IPAM utilizzando sia la console di AWS gestione che la AWS CLI.

> **Note**
>
> Prima di iniziare, devi disporre di un controllo di dominio verificato.

Una volta impostato un intervallo di IPv4 indirizzi AWS, è possibile utilizzare tutti gli indirizzi IP dell'intervallo, incluso il primo indirizzo (l'indirizzo di rete) e l'ultimo indirizzo (l'indirizzo di trasmissione).

Indice

- Porta il tuo IPv4 CIDR in IPAM utilizzando sia la console di AWS gestione che la CLI AWS
- Porta il tuo IPv6 CIDR in IPAM utilizzando la AWS console di gestione

Porta il tuo IPv4 CIDR in IPAM utilizzando sia la console di AWS gestione che la CLI AWS

Segui questi passaggi per portare un IPv4 CIDR a IPAM e allocare un indirizzo IP elastico (EIP) utilizzando sia la console di AWS gestione che la CLI. AWS

Important

- Questo tutorial presuppone che tu abbia già completato i passaggi nelle sezioni seguenti:
  - Integrare IPAM con gli account di un'organizzazione AWS.
  - Crea un IPAM.
- Ogni passaggio di questo tutorial deve essere eseguito da uno dei tre account AWS Organizations:
  - L'account di gestione.
  - L'account membro configurato come amministratore IPAM in Integrare IPAM con gli account di un'organizzazione AWS. In questo tutorial, tale account verrà chiamato account IPAM.
  - L'account membro dell'organizzazione che verrà allocato CIDRs da un pool IPAM. In questo tutorial, tale account verrà chiamato account membro.

Indice

- Fase 1: Creare profili AWS CLI denominati e ruoli IAM
- Passaggio 2: creazione di un pool IPAM di livello superiore
- Fase 3. Crea un pool Regionale all'interno del pool di livello superiore
- Passaggio 4: pubblicizzazione del CIDR

- Fase 5. Condividi il pool regionale
- Passaggio 6: assegnazione di un indirizzo IP elastico dal pool
- Passaggio 7: associare l'indirizzo IP elastico a un' EC2 istanza
- Fase 8: eliminazione
- Alternativa al passaggio 6

Fase 1: Creare profili AWS CLI denominati e ruoli IAM

Per completare questo tutorial come singolo AWS utente, puoi utilizzare i profili AWS CLI denominati per passare da un ruolo IAM a un altro. I profili denominati sono raccolte di impostazioni e credenziali a cui si fa riferimento quando si utilizza l'opzione `--profile` con la AWS CLI. Per ulteriori informazioni su come creare ruoli IAM e profili denominati per AWS gli account, consulta Using an IAM role in AWS CLI.

Crea un ruolo e un profilo con nome per ciascuno dei tre AWS account che utilizzerai in questo tutorial:

- Un profilo chiamato `management-account` per l'account di gestione AWS Organizations.
- Un profilo chiamato `ipam-account` per l'account membro AWS Organizations configurato per essere l'amministratore IPAM.
- Un profilo chiamato `member-account` per l'account membro AWS Organizations dell'organizzazione che verrà allocato CIDRs da un pool IPAM.

Dopo avere creato i ruoli IAM e i profili denominati, torna su questa pagina e vai al passaggio successivo. Nel resto di questo tutorial noterete che AWS CLI i comandi di esempio utilizzano l'`--profile`opzione con uno dei profili denominati per indicare quale account deve eseguire il comando.

Passaggio 2: creazione di un pool IPAM di livello superiore

Completa i passaggi descritti in questa sezione per creare un pool IPAM di livello superiore.

Questo passaggio deve essere eseguito dall'account IPAM.

Per creare un pool

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, seleziona Pool.

3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Scegli l'ambito Public (Pubblico). Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Scegli Crea pool.
5. (Facoltativo) Aggiungi un Name tag (Tag nome) e una Description (Descrizione) per il pool.
6. In Source (Origine), scegli IPAM scope (Ambito IPAM).
7. In Famiglia di indirizzi, scegli IPv4.
8. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
9. In Locale (Località), scegli None (Nessuna).

   L'integrazione IPAM con BYOIP richiede che la località sia impostata su qualsiasi pool verrà utilizzato per il CIDR BYOIP. Poiché creeremo un pool IPAM di livello superiore con un pool regionale al suo interno e allocheremo spazio a un indirizzo IP elastico dal pool regionale, la località andrà impostata sul pool regionale e non sul pool di livello superiore. La località sarà aggiunta al pool regionale una volta creato il pool Regionale in un passaggio successivo.

   > **Note**
   >
   > Se stai creando solo un pool singolo e non un pool di livello superiore con pool Regionali al suo interno, è consigliabile selezionare una Località per questo pool in modo che il pool sia disponibile per le assegnazioni.

10. In Origine IP pubblica, scegli BYOIP.
11. In CIDRs Nessuna disposizione, esegui una delle seguenti operazioni:

    - Se hai verificato il controllo del dominio con un certificato X.509, devi includere il CIDR e il messaggio BYOIP e la firma del certificato che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.
    - Se hai verificato il controllo del dominio con un record TXT DNS, devi includere il CIDR e il token di verifica IPAM che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.

Tieni presente che quando esegui il provisioning di un IPv4 CIDR in un pool all'interno del pool di primo livello, il IPv4 CIDR minimo che puoi fornire è`/24`; non sono consentiti dati più specifici CIDRs (ad esempio`/25`).

> **Important**
>
> Sebbene la maggior parte del provisioning venga completata entro due ore, il completamento del processo di provisioning per gli intervalli pubblicizzabili pubblicamente può richiedere fino a una settimana.

12. Lascia le impostazioni delle regole di allocazione di "Configura questo pool" deselezionate.
13. (Facoltativo) Scegli Tag per il pool.
14. Scegli Crea pool.

Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare. È possibile visualizzare lo stato del provisioning nella CIDRsscheda della pagina dei dettagli del pool.

Fase 3. Crea un pool Regionale all'interno del pool di livello superiore

Crea un pool regionale all'interno del pool di livello superiore. L'integrazione IPAM con BYOIP richiede che la località sia impostata su qualsiasi pool verrà utilizzato per il CIDR BYOIP. Aggiungerai la località al pool regionale una volta creato il pool regionale in questa sezione. La `Locale` deve far parte di una delle regioni operative configurate al momento della creazione dell'IPAM. Ad esempio, se l'impostazione locale è us-east-1, us-east-1 deve essere una regione operativa per l'IPAM. Un'impostazione locale di us-east-1-scl-1 (un gruppo di confine di rete utilizzato per le zone locali) significa che l'IPAM deve avere una regione operativa di us-east-1.

Questo passaggio deve essere eseguito dall'account IPAM.

Per creare un pool Regionale all'interno di un pool di livello superiore

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Se non si desidera utilizzare l'ambito privato di default, scegliere l'ambito che si desidera utilizzare dal menu a tendina nella parte superiore del riquadro dei contenuti. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.

4. Scegli Crea pool.
5. (Facoltativo) Aggiungi un Name tag (Tag nome) e una Description (Descrizione) per il pool.
6. In Source (Origine), scegli il pool di livello superiore che hai creato nella sezione precedente.
7. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
8. In Locale (Località), scegli la località per il pool. In questo tutorial, useremo `us-east-2` come località del pool regionale. Le opzioni qui disponibili provengono dalle Regioni operative scelte al momento della creazione dell'IPAM.

   L'impostazione locale per il pool deve essere una delle seguenti:

   - Una AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni.
   - Il gruppo di confine di rete per una zona AWS locale in cui si desidera che questo pool IPAM sia disponibile per le allocazioni (Local Zones supportate). Questa opzione è disponibile solo per i IPv4 pool IPAM di ambito pubblico.
   - Una zona locale AWS dedicata. Per creare un pool all'interno di una zona locale AWS dedicata, inserisci la zona locale AWS dedicata nell'input del selettore.

   Ad esempio, è possibile assegnare un CIDR per un VPC solo da un pool IPAM che condivide una lingua con la Regione del VPC. Tieni presente che dopo aver scelto una lingua per un pool, questa non può essere modificata. Se la regione di origine dell'IPAM non è disponibile a causa di un'interruzione e il pool è in una località differente dalla regione di origine dell'IPAM, il pool può essere ancora utilizzato per assegnare gli indirizzi IP.

   La scelta di una località garantisce che non vi siano dipendenze interregionali tra il pool e le risorse da esso assegnate.
9. In Servizio, scegli EC2 (EIP/VPC). Il servizio selezionato determina il servizio in cui il AWS CIDR sarà pubblicizzabile. Attualmente, l'unica opzione è EC2 (EIP/VPC), il che significa che quanto CIDRs allocato da questo pool sarà pubblicizzabile per il EC2 servizio Amazon (per indirizzi IP elastici) e il servizio Amazon VPC (per associato a). CIDRs VPCs
10. CIDRs Per quanto riguarda la fornitura, scegli un CIDR da fornire per il pool.

> **Note**
>
> Quando si esegue il provisioning di un CIDR a un pool regionale all'interno del pool di primo livello, è possibile fornire i IPv4 CIDR più specifici/24; non sono consentiti dati più specifici CIDRs (ad /25 esempio). Dopo aver creato il pool regionale, è possibile creare pool più piccoli (ad esempio /25) all'interno dello stesso. Tieni presente che, se condividi il pool regionale o i pool al suo interno, questi pool possono essere utilizzati solo nelle impostazioni locali di quello regionale.

11. Attiva le impostazioni delle regole di allocazione di "Configura questo pool". Qui hai a disposizione le stesse opzioni delle regole di assegnazione rispetto a quando hai creato il pool Regionale di alto livello. Consulta Creare un pool di primo livello IPv4 per una spiegazione delle opzioni disponibili durante la creazione di pool. Le regole di allocazione per il pool Regionale non vengono ereditate dal pool di primo livello. Se non si applica alcuna regola, non verranno impostate regole di assegnazione per il pool.
12. (Facoltativo) Scegli Tag per il pool.
13. Quando hai finito di configurare il pool, scegli Crea pool.

Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare. È possibile visualizzare lo stato del provisioning nella CIDRsscheda della pagina dei dettagli del pool.

Passaggio 4: pubblicizzazione del CIDR

I passaggi in questa sezione devono essere eseguiti dall'account IPAM. Dopo aver associato l'indirizzo IP elastico (EIP) a un'istanza o Elastic Load Balancer, puoi iniziare a pubblicizzare il CIDR che hai portato AWS e che si trova nel pool in cui è configurato il EC2 servizio (EIP/VPC). In questo tutorial, questo è il tuo pool Regionale. Per impostazione predefinita, il CIDR non è pubblicizzato, il che significa che non è accessibile pubblicamente su Internet.

Questo passaggio deve essere eseguito dall'account IPAM.

> **Note**
>
> Lo stato dell'annuncio non limita la capacità di assegnare indirizzi IP elastici. Anche se il tuo BYOIPv4 CIDR non è pubblicizzato, puoi comunque creare dal pool IPAM. EIPs

Pubblicizzazione del CIDR

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Scegli l'ambito Public (Pubblico). Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Scegli il pool regionale creato in questo tutorial.
5. Scegliere la scheda CIDRs.
6. Seleziona il CIDR BYOIP e scegli Actions (Operazioni) > Advertise (Pubblicizzazione).
7. Scegli Advertise CIDR (Pubblicizza CIDR).

Di conseguenza, il CIDR BYOIP viene pubblicizzato e il valore nella colonna Advertising (Pubblicizzazione) passa da Withdrawn (Ritirato) a Advertised (Pubblicizzato).

Fase 5. Condividi il pool regionale

Segui i passaggi di questa sezione per condividere il pool IPAM utilizzando AWS Resource Access Manager (RAM).

Abilitazione della condivisione delle risorse in AWS RAM

Dopo aver creato il tuo IPAM, ti consigliamo di condividere il pool regionale con altri account della tua organizzazione. Prima di condividere un pool IPAM, completa i passaggi di questa sezione per abilitare la condivisione delle risorse con. AWS RAM Se si utilizza AWS CLI per abilitare la condivisione delle risorse, utilizzare l'`--profile` **`management-account`**opzione.

Per abilitare la condivisione delle risorse

1. Utilizzando l'account AWS Organizations di gestione, apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, scegli Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Ora puoi condividere un pool IPAM con altri membri dell'organizzazione.

Condividi un pool IPAM utilizzando AWS RAM

In questa sezione condividerai il pool regionale con un altro account AWS Organizations membro. Per istruzioni complete sulla condivisione dei pool IPAM, comprese le informazioni sulle autorizzazioni IAM richieste, consulta Condivisione di un pool IPAM tramite AWS RAM. Se stai utilizzando AWS CLI per abilitare la condivisione delle risorse, usa l'`--profile` **`ipam-account`**opzione.

Per condividere un pool IPAM utilizzando AWS RAM

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato e il pool IPAM e seleziona Operazioni > Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. La AWS RAM console si apre. Si condivide il pool utilizzando AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).
6. Nella AWS RAM console, scegli nuovamente Crea una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona il tipo di risorsa, scegli Pool IPAM e poi l'ARN del pool che vuoi condividere.
9. Scegli Next (Successivo).
10. Scegli l'AWSRAMPermissionIpamPoolByoipCidrImportautorizzazione. I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione Condivisione di un pool IPAM tramite AWS RAM.
11. Scegli Next (Successivo).
12. Sotto le voci Principali > Seleziona il tipo principale, scegli Account AWS e inserisci l'ID dell'account che porterà un intervallo di indirizzi IP su IPAM, quindi scegli Aggiungi.
13. Scegli Next (Successivo).
14. Controlla le opzioni di condivisione delle risorse e i principali con cui condividerai, quindi scegli Crea.
15. Per consentire all'account **`member-account`** di assegnare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool`. Il valore per `--resource-arns` è l'ARN del pool IPAM creato nella sezione precedente. Il valore per `--principals` è l'ID account di **`member-account`**. Il valore per `--permission-arns` è l'ARN dell'autorizzazione `AWSRAMDefaultPermissionsIpamPool`.

Passaggio 6: assegnazione di un indirizzo IP elastico dal pool

Completa i passaggi in questa sezione per assegnare un indirizzo IP elastico dal pool. Tieni presente che se utilizzi IPv4 pool pubblici per allocare indirizzi IP elastici, puoi utilizzare i passaggi alternativi descritti in questa sezione Alternativa al passaggio 6 anziché i passaggi descritti in questa sezione.

> **Important**
>
> Se visualizzi un errore relativo alla mancanza delle autorizzazioni per chiamare ec2:AllocateAddress, l'autorizzazione gestita attualmente assegnata al pool IPAM che è stato condiviso con te deve essere aggiornata. Contatta la persona che ha creato la condivisione delle risorse e chiedile di aggiornare l'autorizzazione gestita di `AWSRAMPermissionIpamResourceDiscovery` alla versione predefinita. Per ulteriori informazioni, consulta Creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM .

AWS Management Console

Segui la procedura descritta in Allocare un indirizzo IP elastico nella Amazon EC2 User Guide per allocare l'indirizzo, ma tieni presente quanto segue:

- Questo passaggio deve essere eseguito dall'account membro.
- Assicurati che la AWS regione in cui ti trovi nella EC2 console corrisponda all'opzione Locale che hai scelto quando hai creato il pool regionale.
- Quando scegli il pool di indirizzi, scegli l'opzione Allocazione utilizzando un pool IPv4 IPAM e scegli il pool regionale che hai creato.

Command line

Assegna un indirizzo dal pool con il comando allocate-address. L'opzione `--region` che utilizzi deve corrispondere all'opzione `-locale` scelta al momento della creazione del pool nel passaggio 2. Includi l'ID del pool IPAM creato nel passaggio 2 in `--ipam-pool-id`. Facoltativamente, puoi anche scegliere un `/32` specifico nel tuo pool IPAM utilizzando l'opzione `--address`.

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

Risposta di esempio:

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

Per ulteriori informazioni, consulta Allocate an Elastic IP address nella Amazon EC2 User Guide.

Passaggio 7: associare l'indirizzo IP elastico a un' EC2 istanza

Completa i passaggi di questa sezione per associare l'indirizzo IP elastico a un' EC2istanza.

AWS Management Console

Segui i passaggi in Associare un indirizzo IP elastico nella Amazon EC2 User Guide per allocare un indirizzo IP elastico dal pool IPAM, ma tieni presente quanto segue: Quando utilizzi l'opzione Console di AWS gestione, la AWS regione in cui associ l'indirizzo IP elastico deve corrispondere all'opzione Locale che hai scelto quando hai creato il pool regionale.

Questo passaggio deve essere eseguito dall'account membro.

Command line

Questo passaggio deve essere eseguito dall'account membro. Utilizza l'opzione `--profile` **`member-account`**.

Associa l'indirizzo IP elastico a un'istanza con il comando associate-address. Il `--region` a cui associ l'indirizzo IP elastico deve corrispondere all'opzione `--locale` scelta al momento della creazione del pool regionale.

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

Risposta di esempio:

```
{
```

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

Per ulteriori informazioni, consulta Associare un indirizzo IP elastico a un'istanza o a un'interfaccia di rete nella Amazon EC2 User Guide.

Fase 8: eliminazione

Segui i passaggi in questa sezione per ripulire le risorse che hai creato e di cui hai effettuato il provisioning in questo tutorial.

Passaggio 1: ritiro del CIDR dalla pubblicizzazione

Questo passaggio deve essere eseguito dall'account IPAM.

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, seleziona Pool.
3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Scegli l'ambito Public (Pubblico).
4. Scegli il pool regionale creato in questo tutorial.
5. Scegliere la scheda CIDRs.
6. Seleziona il CIDR BYOIP e scegli Actions (Operazioni) >Withdraw from advertising (Ritira dalla pubblicizzazione).
7. Scegli Withdraw CIDR (Ritira CIDR).

Di conseguenza, il CIDR BYOIP non è più pubblicizzato e il valore nella colonna Advertising (Pubblicizzazione) passa da Advertised (Pubblicizzato) a Withdrawn (Ritirato).

Passaggio 2: annullamento dell'associazione di un indirizzo IP elastico

Questo passaggio deve essere eseguito dall'account membro. Se si utilizza il AWS CLI, utilizzare l'`--profile` **`member-account`**opzione.

- Completa la procedura descritta in Dissociazione di un indirizzo IP elastico nella Amazon EC2 User Guide per dissociare l'EIP. Quando si apre EC2 nella console di AWS gestione, la AWS regione in cui si dissocia l'EIP deve corrispondere all'`Locale`opzione scelta al momento della

creazione del pool che verrà utilizzato per il CIDR BYOIP. In questo tutorial, il pool è il pool regionale.

Passaggio 3: rilascio dell'indirizzo IP elastico

Questo passaggio deve essere eseguito dall'account membro. Se si utilizza il, utilizzare l'opzione. AWS CLI`--profile` **`member-account`**

- Completa i passaggi in Release an Elastic IP address nella Amazon EC2 User Guide per rilasciare un indirizzo IP elastico (EIP) dal IPv4 pool pubblico. Quando si apre EC2 nella console di AWS gestione, la AWS regione in cui si alloca l'EIP deve corrispondere all'`Locale`opzione scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP.

Passaggio 4: eliminazione delle condivisioni RAM e disabilitazione dell'integrazione di RAM con AWS Organizations

Questo passaggio deve essere eseguito rispettivamente dall'account IPAM e dall'account di gestione. Se si utilizza il AWS CLI per eliminare le condivisioni RAM e disabilitare l'integrazione della RAM, utilizzare le opzioni and. `--profile` **`ipam-account`** `--profile` **`management-account`**

- Completa i passaggi descritti in Eliminazione di una condivisione di risorse nella AWS RAM e Disabilitazione della condivisione delle risorse con AWS Organizzazioni nella AWS RAM User Guide, in quest'ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione della RAM con Organizations AWS .

Fase 5: Eliminare il rifornimento dal pool regionale e CIDRs dal pool di primo livello

Questo passaggio deve essere eseguito dall'account IPAM. Se si utilizza il AWS CLI per condividere il pool, utilizzare l'`--profile` **`ipam-account`**opzione.

- Completa i passaggi Deapprovvigionamento CIDRs da un pool per rimuovere il provisioning CIDRs dal pool regionale e quindi dal pool di livello superiore, in quest'ordine.

Passaggio 6: eliminazione del pool regionale e del pool di livello superiore

Questo passaggio deve essere eseguito dall'account IPAM. Se si utilizza il AWS CLI per condividere il pool, utilizzare l'`--profile` **`ipam-account`**opzione.

- Completa i passaggi descritti in Elimina un pool per eliminare il pool regionale e quindi il pool di livello superiore, in questo ordine.

Alternativa al passaggio 6

Se utilizzi IPv4 pool pubblici per allocare indirizzi IP elastici, puoi utilizzare i passaggi in questa sezione anziché i passaggi seguenti. Passaggio 6: assegnazione di un indirizzo IP elastico dal pool

Indice

- Fase 1: Creare un pool pubblico IPv4
- Fase 2: Fornisci il IPv4 CIDR pubblico al tuo pool pubblico IPv4
- Fase 3: Allocazione di un indirizzo IP elastico dal pool pubblico IPv4
- Alternativa alla pulizia del passaggio 6

Fase 1: Creare un pool pubblico IPv4

Questo passaggio dovrebbe essere eseguito dall'account membro che effettuerà il provisioning di un indirizzo IP elastico.

> **Note**
>
> - Questo passaggio deve essere eseguito dall'account membro utilizzando la AWS CLI.
> - I IPv4 pool pubblici e i pool IPAM sono gestiti da risorse distinte in AWS. I IPv4 pool pubblici sono risorse con account singolo che consentono di convertire gli indirizzi IP di proprietà pubblica in indirizzi IP CIDRs elastici. I pool IPAM possono essere utilizzati per allocare lo spazio pubblico ai pool pubblici. IPv4

Per creare un IPv4 pool pubblico utilizzando il AWS CLI

- Esegui il comando seguente per effettuare il provisioning del CIDR. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `Locale` scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP.

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

Nell'output, vedrai l'ID del IPv4 pool pubblico. Sarà necessario questo ID nel passaggio successivo.

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

Fase 2: Fornisci il IPv4 CIDR pubblico al tuo pool pubblico IPv4

Fornisci il IPv4 CIDR pubblico al tuo pool pubblico IPv4 . Il valore per `--region` deve corrispondere al valore `Locale` scelto al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP. `--netmask-length` è la quantità di spazio fuori dal pool IPAM che si desidera portare nel pool pubblico. Il valore non può essere maggiore della lunghezza della maschera di rete del pool IPAM. La `--netmask-length` meno specifica che puoi definire è `24`.

> **Note**
>
> - Se stai trasferendo un intervallo di CIDR `/24` su IPAM per condividerlo in un'organizzazione AWS , puoi fornire prefissi più piccoli a più pool IPAM, ad esempio`/27` (utilizzando `-- netmask-length 27`) anziché fornire l'intero CIDR `/24` (utilizzando `--netmask-length 24`) come mostrato in questo tutorial.
> - Questo passaggio deve essere eseguito dall'account membro utilizzando la AWS CLI.

Per creare un IPv4 pool pubblico utilizzando il AWS CLI

1. Esegui il comando seguente per effettuare il provisioning del CIDR.

```
aws ec2 provision-public-ipv4-pool-cidr --region us-east-2 --ipam-pool-id ipam-
pool-04d8e2d9670eeab21 --pool-id ipv4pool-ec2-09037ce61cf068f9a --netmask-length 24
 --profile member-account
```

   Nell'output, sarà visualizzato il CIDR su cui è stato effettuato il provisioning.

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

```
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. Esegui il comando seguente per visualizzare il CIDR distribuito nel pool pubblico IPv4 .

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

Nell'output, sarà visualizzato il CIDR su cui è stato effettuato il provisioning. Per impostazione predefinita, il CIDR non è pubblicizzato, il che significa che non è accessibile pubblicamente su Internet. Avrai la possibilità di impostare questo CIDR su pubblicizzato nell'ultimo passaggio di questo tutorial.

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 255
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 255,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

Dopo aver creato il IPv4 pool pubblico, per visualizzare il pool pubblico allocato nel IPv4 pool regionale IPAM, apri la console IPAM e visualizza l'allocazione nel pool regionale in Allocazioni o Risorse.

Fase 3: Allocazione di un indirizzo IP elastico dal pool pubblico IPv4

Completa i passaggi in Allocare un indirizzo IP elastico nella Amazon EC2 User Guide per allocare un EIP dal pool pubblico. IPv4 Quando si apre EC2 nella console di AWS gestione, la AWS regione in cui si alloca l'EIP deve corrispondere all'`Locale`opzione scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account membro. Se si utilizza il, utilizzare l'opzione. AWS CLI`--profile` **`member-account`**

Una volta completati questi tre passaggi, torna al tutorial Passaggio 7: associare l'indirizzo IP elastico a un' EC2 istanza e continua fino al completamento.

Alternativa alla pulizia del passaggio 6

Completa questi passaggi per pulire i IPv4 pool pubblici creati con l'alternativa al passaggio 9. È necessario completare questi passaggi dopo aver rilasciato l'indirizzo IP elastico durante il processo di pulizia standard in Fase 8: eliminazione.

Passaggio 1: rimuovere il IPv4 CIDR pubblico dal pool pubblico IPv4

> **Important**
>
> Questo passaggio deve essere eseguito dall'account membro utilizzando la AWS CLI.

1. Visualizza il tuo BYOIP. CIDRs

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

Nell'output, vedrai gli indirizzi IP nel tuo CIDR BYOIP.

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-09037ce61cf068f9a",
            "Description": "",
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
```

```
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 256
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 256,
            "NetworkBorderGroup": "us-east-2",
            "Tags": []
        }
    ]
}
```

2. Esegui il comando seguente per rilasciare il CIDR dal pool pubblico. IPv4

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

3. Visualizza CIDRs nuovamente il tuo BYOIP e assicurati che non ci siano altri indirizzi forniti. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

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

Nell'output, vedrai il numero di indirizzi IP nel tuo pool pubblico. IPv4

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

> **Note**
>
> L'IPAM potrebbe impiegare del tempo per scoprire che le allocazioni dei IPv4 pool pubblici sono state rimosse. Non è possibile continuare a ripulire e revocare il provisioning del CIDR del pool IPAM fino a quando non si vede che l'assegnazione è stata rimossa da IPAM.

Fase 2: Eliminare il pool pubblico IPv4

Questo passaggio deve essere eseguito dall'account membro.

- Esegui il seguente comando per eliminare il IPv4 pool pubblico (il CIDR). Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `Locale` scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP. In questo tutorial, il pool è il pool regionale. Questo passaggio deve essere eseguito utilizzando la AWS CLI.

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

  Nell'output restituito vedrai il valore true (vero).

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

  Una volta eliminato il pool, per visualizzare l'allocazione non gestita da IPAM, apri la console IPAM e visualizza i dettagli del pool regionale sotto Allocations (Allocazioni).

Porta il tuo IPv6 CIDR in IPAM utilizzando la AWS console di gestione

Segui i passaggi di questo tutorial per portare un IPv6 CIDR a IPAM e allocare un VPC con il CIDR utilizzando sia la Console di gestione che il. AWS AWS CLI

Se non hai bisogno di pubblicizzare i tuoi IPv6 indirizzi su Internet, puoi fornire un indirizzo GUA privato a un IPAM. IPv6 Per ulteriori informazioni, consulta Abilita il provisioning GUA privato IPv6 CIDRs.

Important

- Questo tutorial presuppone che tu abbia già completato i passaggi nelle sezioni seguenti:
  - Integrare IPAM con gli account di un'organizzazione AWS.
  - Crea un IPAM.
- Ogni passaggio di questo tutorial deve essere eseguito da uno dei tre account AWS Organizations:
  - L'account di gestione.
  - L'account membro configurato come amministratore IPAM in Integrare IPAM con gli account di un'organizzazione AWS. In questo tutorial, tale account verrà chiamato account IPAM.
  - L'account membro dell'organizzazione che verrà allocato CIDRs da un pool IPAM. In questo tutorial, tale account verrà chiamato account membro.

Indice

- Passaggio 1: creazione di un pool IPAM di livello superiore
- Fase 2: Crea un pool Regionale all'interno del pool di livello superiore
- Fase 3. Condividi il pool regionale
- Passaggio 4: creazione di un VPC
- Passaggio 5: pubblicizzazione del CIDR
- Passaggio 6: pulizia

Passaggio 1: creazione di un pool IPAM di livello superiore

Poiché si intende creare un pool IPAM di livello superiore con un pool Regionale al suo interno e si andrà ad assegnare spazio a una risorsa dal pool Regionale, la località andrà impostata sul pool Regionale e non sul pool di livello superiore. La località sarà aggiunta al pool regionale una volta creato il pool Regionale in un passaggio successivo. L'integrazione IPAM con BYOIP richiede che la località sia impostata su qualsiasi pool verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account IPAM.

Per creare un pool

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Scegli l'ambito Public (Pubblico). Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Scegli Crea pool.
5. (Facoltativo) Aggiungi un Name tag (Tag nome) e una Description (Descrizione) per il pool.
6. In Source (Origine), scegli IPAM scope (Ambito IPAM).
7. In Famiglia di indirizzi, scegli IPv6.
8. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
9. In Locale (Località), scegli None (Nessuna). Imposterai la località sul pool Regionale.

   La lingua è la AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni. Ad esempio, è possibile assegnare un CIDR per un VPC solo da un pool IPAM che condivide una lingua con la Regione del VPC. Tieni presente che dopo aver scelto una lingua per un pool, questa non può essere modificata. Se la regione di origine dell'IPAM non è disponibile a causa di un'interruzione e il pool è in una località differente dalla regione di origine dell'IPAM, il pool può essere ancora utilizzato per assegnare gli indirizzi IP.

   > **Note**
   >
   > Se stai creando solo un pool singolo e non un pool di livello superiore con pool Regionali al suo interno, è consigliabile selezionare una Località per questo pool in modo che il pool sia disponibile per le assegnazioni.

10. In Origine IP pubblico, BYOIP è selezionato per impostazione predefinita.
11. In base CIDRs alla disposizione, esegui una delle seguenti operazioni:

    - Se hai verificato il controllo del dominio con un certificato X.509, devi includere il CIDR e il messaggio BYOIP e la firma del certificato che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.

- Se hai verificato il controllo del dominio con un record TXT DNS, devi includere il CIDR e il token di verifica IPAM che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.

Tieni presente che quando esegui il provisioning di un IPv6 CIDR a un pool all'interno del pool di primo livello, l'intervallo di IPv6 indirizzi più specifico che puoi inserire è /48 per quelli pubblicizzabili pubblicamente e /60 per CIDRs CIDRs quelli non pubblicizzabili pubblicamente.

> **Important**
>
> Sebbene la maggior parte del provisioning venga completata entro due ore, il completamento del processo di provisioning per gli intervalli pubblicizzabili pubblicamente può richiedere fino a una settimana.

12. Lascia le impostazioni delle regole di allocazione di "Configura questo pool" deselezionate.
13. (Facoltativo) Scegli Tag per il pool.
14. Scegli Crea pool.

Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare. Puoi vedere lo stato del provisioning nella scheda della pagina dei dettagli del pool. CIDRs

Fase 2: Crea un pool Regionale all'interno del pool di livello superiore

Crea un pool regionale all'interno del pool di livello superiore. Nel pool, la località è obbligatoria e deve essere una delle regioni operative configurate al momento della creazione dell'IPAM.

Questo passaggio deve essere eseguito dall'account IPAM.

Per creare un pool Regionale all'interno di un pool di livello superiore

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Se non si desidera utilizzare l'ambito privato di default, scegliere l'ambito che si desidera utilizzare dal menu a tendina nella parte superiore del riquadro dei contenuti. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Scegli Crea pool.

5. (Facoltativo) Aggiungi un Tag nome e una descrizione per il pool.
6. In Source (Origine), scegli il pool di livello superiore che hai creato nella sezione precedente.
7. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito). Per ulteriori informazioni sull'utilizzo di questa opzione per la pianificazione dello spazio IP della sottorete in un VPC, consulta Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti.
8. Scegli la località per il pool. La scelta di una località garantisce che non vi siano dipendenze interregionali tra il pool e le risorse da esso assegnate. Le opzioni qui disponibili provengono dalle Regioni operative scelte al momento della creazione dell'IPAM. In questo tutorial, useremo `us-east-2` come località del pool regionale.

   La lingua è la AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni. Ad esempio, è possibile assegnare un CIDR per un VPC solo da un pool IPAM che condivide una lingua con la Regione del VPC. Tieni presente che dopo aver scelto una lingua per un pool, questa non può essere modificata. Se la regione di origine dell'IPAM non è disponibile a causa di un'interruzione e il pool è in una località differente dalla regione di origine dell'IPAM, il pool può essere ancora utilizzato per assegnare gli indirizzi IP.
9. In Servizio, scegli EC2 (EIP/VPC). Il servizio selezionato determina il servizio in cui il AWS CIDR sarà pubblicizzabile. Attualmente, l'unica opzione è EC2 (EIP/VPC), il che significa che quanto CIDRs allocato da questo pool sarà pubblicizzabile per il servizio Amazon e EC2 il servizio Amazon VPC (per associato a). CIDRs VPCs
10. CIDRs Per quanto riguarda la fornitura, scegli un CIDR da fornire per il pool. Tieni presente che quando esegui il provisioning di un IPv6 CIDR a un pool all'interno del pool di primo livello, l'intervallo di IPv6 indirizzi più specifico che puoi inserire è /48 per quelli pubblicizzabili pubblicamente e /60 per CIDRs quelli non pubblicizzabili pubblicamente. CIDRs
11. Attiva le impostazioni delle regole di allocazione di "Configura questo pool" e scegli le regole di allocazione facoltative per questo pool:

    - Importazione automatica delle risorse rilevale: questa opzione non è disponibile se la Località è impostata su Nessuna. Se selezionato, IPAM cercherà continuamente le risorse all'interno dell'intervallo CIDR di questo pool e le importerà automaticamente come assegnazioni nel tuo IPAM. Tieni presente quanto segue:
      - Le risorse CIDRs che verranno allocate per queste risorse non devono essere già allocate ad altre risorse affinché l'importazione abbia esito positivo.

    - IPAM importerà un CIDR indipendentemente dalla conformità con le regole di allocazione del pool, in modo che una risorsa possa essere importata e successivamente contrassegnata come non conforme.
    - Se IPAM ne rileva più di uno CIDRs che si sovrappone, IPAM importerà solo il CIDR più grande.
    - Se IPAM ne rileva più di uno CIDRs con corrispondenza CIDRs, IPAM ne importerà in modo casuale solo uno.
- Lunghezza minima della netmask: la lunghezza minima della netmask richiesta affinché le assegnazioni CIDR in questo pool IPAM siano conformi e il blocco CIDR di dimensioni maggiori che può essere assegnato dal pool. La lunghezza minima della netmask deve essere inferiore alla lunghezza massima della netmask. Le possibili lunghezze delle maschere di rete per gli indirizzi sono -. IPv4 `0` `32` Le possibili lunghezze delle maschere di rete per IPv6 gli indirizzi sono -. `0` `128`
- Lunghezza di default della netmask: lunghezza di default della netmask per le assegnazioni aggiunte a questo pool.
- Lunghezza massima della netmask: la lunghezza massima della netmask richiesta per le assegnazioni CIDR in questo pool. Questo valore determina il blocco CIDR di dimensioni più piccole che può essere assegnato dal pool. Verifica che questo valore sia almeno **`/48`**.
- Requisiti per l'assegnazione di tag: i tag necessari alle risorse per assegnare spazio dal pool. Se i tag delle risorse sono stati modificati dopo aver assegnato spazio o se le regole di assegnazione di tag di allocazione vengono modificate nel pool, la risorsa potrebbe essere contrassegnata come non conforme.
- Locale: la versione locale che sarà richiesta per le risorse utilizzate CIDRs da questo pool. Le risorse importate automaticamente che non dispongono di questa località saranno contrassegnate come non conformi. Le risorse che non vengono importate automaticamente nel pool non saranno autorizzate ad assegnare spazio dal pool a meno che non si trovino in questa località.

12. (Facoltativo) Scegli Tag per il pool.
13. Quando hai finito di configurare il pool, scegli Crea pool.

Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare. È possibile visualizzare lo stato del provisioning nella CIDRsscheda della pagina dei dettagli del pool.

Fase 3. Condividi il pool regionale

Segui i passaggi di questa sezione per condividere il pool IPAM utilizzando AWS Resource Access Manager (RAM).

Abilitazione della condivisione delle risorse in AWS RAM

Dopo aver creato il tuo IPAM, ti consigliamo di condividere il pool regionale con altri account della tua organizzazione. Prima di condividere un pool IPAM, completa i passaggi di questa sezione per abilitare la condivisione delle risorse con. AWS RAM Se si utilizza AWS CLI per abilitare la condivisione delle risorse, utilizzare l'`--profile` **`management-account`**opzione.

Per abilitare la condivisione delle risorse

1. Utilizzando l'account AWS Organizations di gestione, apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, scegli Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Ora puoi condividere un pool IPAM con altri membri dell'organizzazione.

Condividi un pool IPAM utilizzando AWS RAM

In questa sezione condividerai il pool regionale con un altro account AWS Organizations membro. Per istruzioni complete sulla condivisione dei pool IPAM, comprese le informazioni sulle autorizzazioni IAM richieste, consulta Condivisione di un pool IPAM tramite AWS RAM. Se stai utilizzando AWS CLI per abilitare la condivisione delle risorse, usa l'`--profile` **`ipam-account`**opzione.

Per condividere un pool IPAM utilizzando AWS RAM

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato e il pool IPAM e seleziona Operazioni **>** Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. La AWS RAM console si apre. Condividete il pool utilizzando AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).

6. Nella AWS RAM console, scegli nuovamente Crea una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona il tipo di risorsa, scegli Pool IPAM e poi l'ARN del pool che vuoi condividere.
9. Scegli Next (Successivo).
10. Scegli l'AWSRAMPermissionIpamPoolByoipCidrImportautorizzazione. I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione Condivisione di un pool IPAM tramite AWS RAM.
11. Scegli Next (Successivo).
12. Sotto le voci Principali > Seleziona il tipo principale, scegli Account AWS e inserisci l'ID dell'account che porterà un intervallo di indirizzi IP su IPAM, quindi scegli Aggiungi.
13. Scegli Next (Successivo).
14. Controlla le opzioni di condivisione delle risorse e i principali con cui condividerai, quindi scegli Crea.
15. Per consentire all'account **`member-account`** di assegnare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool`. Il valore per `--resource-arns` è l'ARN del pool IPAM creato nella sezione precedente. Il valore per `--principals` è l'ID account di **`member-account`**. Il valore per `--permission-arns` è l'ARN dell'autorizzazione `AWSRAMDefaultPermissionsIpamPool`.

Passaggio 4: creazione di un VPC

Completa i passaggi descritti in Creare un VPC nella Amazon VPC User Guide.

Questo passaggio deve essere eseguito dall'account membro.

> **Note**
>
> - Quando si apre VPC nella console di AWS gestione, la AWS regione in cui si crea il VPC deve corrispondere all'`Locale`opzione scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP.
> - Quando raggiungi la fase di scelta di un CIDR per il VPC, avrai la possibilità di utilizzare un CIDR da un pool IPAM. Scegli il pool regionale creato in questo tutorial.

Quando si crea il VPC, AWS alloca un CIDR nel pool IPAM al VPC. Puoi visualizzare l'allocazione in IPAM scegliendo un pool dal pannello dei contenuti della console IPAM e visualizzando la scheda Allocations (Allocazioni) per il pool.

Passaggio 5: pubblicizzazione del CIDR

I passaggi in questa sezione devono essere eseguiti dall'account IPAM. Una volta creato il VPC, puoi iniziare a pubblicizzare il CIDR che hai portato e AWS che si trova nel pool in cui è configurato il servizio EC2 (EIP/VPC). In questo tutorial, questo è il tuo pool Regionale. Per impostazione predefinita, il CIDR non è pubblicizzato, il che significa che non è accessibile pubblicamente su Internet.

Questo passaggio deve essere eseguito dall'account IPAM.

Pubblicizzazione del CIDR

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Scegli l'ambito Public (Pubblico). Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Scegli il pool regionale creato in questo tutorial.
5. Scegliere la scheda CIDRs.
6. Seleziona il CIDR BYOIP e scegli Actions (Operazioni) > Advertise (Pubblicizzazione).
7. Scegli Advertise CIDR (Pubblicizza CIDR).

Di conseguenza, il CIDR BYOIP viene pubblicizzato e il valore nella colonna Advertising (Pubblicizzazione) passa da Withdrawn (Ritirato) a Advertised (Pubblicizzato).

Passaggio 6: pulizia

Segui i passaggi in questa sezione per ripulire le risorse che hai creato e di cui hai effettuato il provisioning in questo tutorial.

Passaggio 1: ritiro del CIDR dalla pubblicizzazione

Questo passaggio deve essere eseguito dall'account IPAM.

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Per impostazione predefinita, quando si crea un pool viene selezionato l'ambito privato di default. Scegli l'ambito Public (Pubblico).
4. Scegli il pool regionale creato in questo tutorial.
5. Scegliere la scheda CIDRs.
6. Seleziona il CIDR BYOIP e scegli Actions (Operazioni) >Withdraw from advertising (Ritira dalla pubblicizzazione).
7. Scegli Withdraw CIDR (Ritira CIDR).

Di conseguenza, il CIDR BYOIP non è più pubblicizzato e il valore nella colonna Advertising (Pubblicizzazione) passa da Advertised (Pubblicizzato) a Withdrawn (Ritirato).

Passaggio 2: eliminazione del VPC

Questo passaggio deve essere eseguito dall'account membro.

- Completa i passaggi indicati in Elimina un VPC nella Amazon VPC User Guide per eliminare il VPC. Quando si apre VPC nella console di AWS gestione, la AWS regione da cui eliminare il VPC deve corrispondere all'`Local`eopzione scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP. In questo tutorial, il pool è il pool regionale.

  Quando elimini il VPC, occorre un po' di tempo affinché IPAM rilevi che la risorsa è stata eliminata e annulli l'allocazione del CIDR allocato al VPC. Per procedere al passaggio successivo della pulizia, dovrai attendere fino a quando IPAM avrà rimosso l'allocazione dal pool nella scheda dei dettagli del pool Allocations (Allocazioni).

Passaggio 3: Eliminare le condivisioni RAM e disabilitare l'integrazione della RAM con AWS Organizations

Questo passaggio deve essere eseguito rispettivamente dall'account IPAM e dall'account di gestione.

- Completa i passaggi in Eliminazione di una condivisione di risorse nella AWS RAM e Disabilitazione della condivisione delle risorse con le AWS organizzazioni nella AWS RAM User Guide, in quest'ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione della RAM con Organizations AWS .

Fase 4: Eliminare il rifornimento dal pool regionale e CIDRs dal pool di primo livello

Questo passaggio deve essere eseguito dall'account IPAM.

- Completa i passaggi Deapprovvigionamento CIDRs da un pool per rimuovere il provisioning CIDRs dal pool regionale e quindi dal pool di livello superiore, in quest'ordine.

Passaggio 5: eliminazione del pool regionale e del pool di livello superiore

Questo passaggio deve essere eseguito dall'account IPAM.

- Completa i passaggi descritti in Elimina un pool per eliminare il pool regionale e quindi il pool di livello superiore, in questo ordine.

Porta il tuo IP CIDR su IPAM usando solo la CLI AWS

Bringing Your Own IP (BYOIP) su IPAM consente di utilizzare gli intervalli di indirizzi esistenti e quelli IPv4 della propria organizzazione. IPv6 AWS Ciò consente di mantenere un marchio coerente, migliorare le prestazioni di rete, aumentare la sicurezza e semplificare la gestione unificando gli ambienti on-premises e cloud nello spazio di indirizzi IP.

Segui questi passaggi per portare un IPv4 o IPv6 CIDR a IPAM utilizzando solo la CLI AWS .

> **Note**
>
> Prima di iniziare, devi disporre di un controllo di dominio verificato.

Una volta impostato un intervallo di IPv4 indirizzi AWS, è possibile utilizzare tutti gli indirizzi IP dell'intervallo, incluso il primo indirizzo (l'indirizzo di rete) e l'ultimo indirizzo (l'indirizzo di trasmissione).

Indice

- Porta il tuo IPv4 CIDR pubblico su IPAM usando solo la CLI AWS
- Porta il tuo IPv6 CIDR su IPAM usando solo la CLI AWS

Porta il tuo IPv4 CIDR pubblico su IPAM usando solo la CLI AWS

Segui questi passaggi per portare un IPv4 CIDR in IPAM e allocare un indirizzo IP elastico (EIP) con il CIDR utilizzando solo il. AWS CLI

Important

- Questo tutorial presuppone che tu abbia già completato i passaggi nelle sezioni seguenti:
  - Integrare IPAM con gli account di un'organizzazione AWS.
  - Crea un IPAM.
- Ogni passaggio di questo tutorial deve essere eseguito da uno dei tre account AWS Organizations:
  - L'account di gestione.
  - L'account membro configurato come amministratore IPAM in Integrare IPAM con gli account di un'organizzazione AWS. In questo tutorial, tale account verrà chiamato account IPAM.
  - L'account membro dell'organizzazione che verrà allocato CIDRs da un pool IPAM. In questo tutorial, tale account verrà chiamato account membro.

Indice

- Fase 1: Creare profili AWS CLI denominati e ruoli IAM
- Passaggio 2: creazione di un IPAM
- Passaggio 3: creazione di un pool IPAM di livello superiore
- Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore
- Passaggio 5: creazione di un pool regionale all'interno del pool di livello superiore
- Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale
- Fase 7: pubblicizzare il CIDR
- Passaggio 8: condivisione del pool regionale
- Passaggio 9: assegnazione di un indirizzo IP elastico dal pool
- Passaggio 10: associare l'indirizzo IP elastico a un' EC2 istanza
- Passaggio 11: pulizia
- Alternativa al passaggio 9

Fase 1: Creare profili AWS CLI denominati e ruoli IAM

Per completare questo tutorial come singolo AWS utente, puoi utilizzare i profili AWS CLI denominati per passare da un ruolo IAM a un altro. I profili denominati sono raccolte di impostazioni e credenziali a cui si fa riferimento quando si utilizza l'opzione `--profile` con la AWS CLI. Per ulteriori informazioni su come creare ruoli IAM e profili denominati per AWS gli account, consulta Using an IAM role in AWS CLI.

Crea un ruolo e un profilo denominato per ciascuno dei tre AWS account che utilizzerai in questo tutorial:

- Un profilo chiamato `management-account` per l'account di gestione AWS Organizations.
- Un profilo chiamato `ipam-account` per l'account membro AWS Organizations configurato per essere l'amministratore IPAM.
- Un profilo chiamato `member-account` per l'account membro AWS Organizations dell'organizzazione che verrà allocato CIDRs da un pool IPAM.

Dopo avere creato i ruoli IAM e i profili denominati, torna su questa pagina e vai al passaggio successivo. Nel resto di questo tutorial noterete che AWS CLI i comandi di esempio utilizzano l'`--profile`opzione con uno dei profili denominati per indicare quale account deve eseguire il comando.

Passaggio 2: creazione di un IPAM

Questa fase è facoltativa. Se un IPAM è già stato creato con regioni operative di `us-east-1` e `us-west-2` create, questo passaggio può essere ignorato. Crea un IPAM e specifica una Regione operativa di `us-east-1` e `us-west-2`. È necessario selezionare una Regione operativa in modo da poter utilizzare l'opzione località durante la creazione del pool IPAM. L'integrazione IPAM con BYOIP richiede che la località sia impostata su qualsiasi pool verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account IPAM.

Esegui il comando seguente:

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

Nell'output sarà visualizzato l'IPAM creato. Prendere nota del valore per `PublicDefaultScopeId`. L'ID dell'ambito pubblico è necessario nella fase successiva. Stai utilizzando l'ambito pubblico perché i BYOIP CIDRs sono indirizzi IP pubblici, a cui è destinato l'ambito pubblico.

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

Passaggio 3: creazione di un pool IPAM di livello superiore

Completa i passaggi descritti in questa sezione per creare un pool IPAM di livello superiore.

Questo passaggio deve essere eseguito dall'account IPAM.

Per creare un pool di IPv4 indirizzi per tutte le AWS risorse, utilizza il AWS CLI

1. Esegui il comando seguente per creare un pool IPAM. Utilizza l'ID dell'ambito pubblico dell'IPAM creato nella fase precedente.

   Questo passaggio deve essere eseguito dall'account IPAM.

   ```
   aws ec2 create-ipam-pool --region us-east-1 --ipam-scope-id ipam-
   scope-0087d83896280b594 --description "top-level-IPv4-pool" --address-family ipv4
    --profile ipam-account
   ```

   Nell'output, vedrai `create-in-progress`, il che indica che è in corso la creazione del pool.

   ```
   {
       "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. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `create-complete` nell'output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Il seguente output esemplificativo mostra lo stato del pool.

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

```
        }
    ]
}
```

Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore

Effettua il provisioning di un blocco CIDR al pool di livello superiore. Tieni presente che quando esegui il provisioning di un IPv4 CIDR in un pool all'interno del pool di primo livello, il numero minimo di IPv4 CIDR che puoi fornire è/24; non sono consentiti dati più specifici CIDRs (ad esempio/25).

> **Note**
>
> - Se hai verificato il controllo del dominio con un certificato X.509, devi includere il CIDR e il messaggio BYOIP e la firma del certificato che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.
> - Se hai verificato il controllo del dominio con un record TXT DNS, devi includere il CIDR e il token di verifica IPAM che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.

È necessario solo verificare il controllo del dominio quando si effettua il provisioning del CIDR BYOIP al pool di livello superiore. Per il pool regionale all'interno di quello di livello superiore, è possibile omettere l'opzione di verifica della proprietà del dominio.

Questo passaggio deve essere eseguito dall'account IPAM.

> **Important**
>
> È necessario solo verificare il controllo del dominio quando si effettua il provisioning del CIDR BYOIP al pool di livello superiore. Per il pool regionale all'interno di quello di livello superiore, è possibile omettere l'opzione di controllo del dominio. Una volta effettuato l'accesso al BYOIP su IPAM, non è necessario eseguire la convalida della proprietà quando dividi il BYOIP tra Regioni e account.

Per fornire un blocco CIDR al pool utilizzando il AWS CLI

1. Per eseguire il provisioning del CIDR con le informazioni sul certificato, utilizzare il seguente esempio di comando. Oltre a sostituire i valori necessari nell'esempio, assicurati di sostituire `Message` e `Signature` con i valori `text_message` e `signed_message` che hai inserito in Verifica il dominio con un certificato X.509.

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

Per eseguire il provisioning del CIDR con le informazioni sul token di verifica, utilizzare il seguente esempio di comando. Oltre a sostituire i valori necessari nell'esempio, assicurati di sostituire `ipam-ext-res-ver-token-0309ce7f67a768cf0` e con l'ID token `IpamExternalResourceVerificationTokenId` che hai inserito in Verifica il dominio con un record TXT DNS.

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

Nell'output, sarà visualizzato il provisioning del CIDR in sospeso.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare.

> **Important**
>
> Sebbene la maggior parte del provisioning venga completata entro due ore, il completamento del processo di provisioning per gli intervalli pubblicizzabili pubblicamente può richiedere fino a una settimana.

Esegui il seguente comando fino a quando non viene visualizzato uno stato di `provisioned` nell'output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Il seguente output esemplificativo mostra lo stato.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

Passaggio 5: creazione di un pool regionale all'interno del pool di livello superiore

Crea un pool regionale all'interno del pool di livello superiore.

L'impostazione locale per il pool deve essere una delle seguenti:

- Una AWS regione in cui si desidera che questo pool IPAM sia disponibile per le allocazioni.
- Il gruppo di confine di rete per una zona AWS locale in cui si desidera che questo pool IPAM sia disponibile per le allocazioni (Local Zones supportate). Questa opzione è disponibile solo per i IPv4 pool IPAM di ambito pubblico.
- Una zona locale AWS dedicata. Per creare un pool all'interno di una zona locale AWS dedicata, inserisci la zona locale AWS dedicata nell'input del selettore.

Ad esempio, è possibile assegnare un CIDR per un VPC solo da un pool IPAM che condivide una lingua con la Regione del VPC. Tieni presente che dopo aver scelto una lingua per un pool, questa non può essere modificata. Se la regione di origine dell'IPAM non è disponibile a causa di un'interruzione e il pool è in una località differente dalla regione di origine dell'IPAM, il pool può essere ancora utilizzato per assegnare gli indirizzi IP.

Quando esegui i comandi in questa sezione, il valore per `--region` deve includere l'opzione `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP. Ad esempio, se hai creato il pool BYOIP con un'impostazione locale di us-east-1, `--region` dovrebbe essere us-east-1. Se hai creato il pool BYOIP con un'impostazione locale di us-east-1-scl-1 (un gruppo di confine di rete usato per le zone locali), `--region` dovrebbe essere us-east-1 perché quella regione gestisce l'impostazione locale us-east-1-scl-1.

Questo passaggio deve essere eseguito dall'account IPAM.

La scelta di una località garantisce che non vi siano dipendenze interregionali tra il pool e le risorse da esso assegnate. Le opzioni qui disponibili provengono dalle Regioni operative scelte al momento della creazione dell'IPAM. In questo tutorial, useremo `us-west-2` come località del pool regionale.

> **Important**
>
> Quando crei il pool, devi includere `--aws-service ec2`. Il servizio selezionato determina il AWS servizio in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione è `ec2` che ciò che viene CIDRs allocato da questo pool sarà pubblicizzabile per il EC2 servizio Amazon (per indirizzi IP elastici) e il servizio Amazon VPC (per CIDRs associato a). VPCs

Per creare di un pool Regionale utilizzando la AWS CLI

1. Per creare un pool, esegui il comando seguente.

```
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
```

   Nell'output, potrai visualizzare IPAM mentre crea il pool.

```
{
     "IpamPool": {
```

```
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
        "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0d8f3646b61ca5987",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-west-2",
        "PoolDepth": 2,
        "State": "create-in-progress",
        "Description": "Regional--pool",
        "AutoImport": false,
        "AddressFamily": "ipv4",
        "Tags": [],
        "ServiceType": "ec2"
    }
}
```

2. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `create-complete` nell'output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Nell'output, vedrai i pool contenuti nel tuo IPAM. In questo tutorial è stato creato un pool di livello superiore e un pool Regionale, in modo da vederli entrambi.

Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale

Effettua il provisioning di un blocco CIDR al pool Regionale.

> **Note**
>
> Quando si esegue il provisioning di un CIDR a un pool regionale all'interno del pool di primo livello, è possibile fornire i IPv4 CIDR più specifici/24; non sono consentiti dati più specifici CIDRs (ad esempio). /25 Dopo aver creato il pool regionale, è possibile creare pool più piccoli (ad esempio /25) all'interno dello stesso. Tieni presente che, se condividi il pool regionale o i pool al suo interno, questi pool possono essere utilizzati solo nelle impostazioni locali di quello regionale.

Questo passaggio deve essere eseguito dall'account IPAM.

Per assegnare un blocco CIDR al pool regionale utilizzando il AWS CLI

1. Esegui il comando seguente per effettuare il provisioning del CIDR.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --cidr 130.137.245.0/24 --profile ipam-account
```

   Nell'output, sarà visualizzato il provisioning del CIDR in sospeso.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `provisioned` nell'output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   Il seguente output esemplificativo mostra lo stato corretto.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

Fase 7: pubblicizzare il CIDR

I passaggi in questa sezione devono essere eseguiti dall'account IPAM. Dopo aver associato l'indirizzo IP elastico (EIP) a un'istanza o Elastic Load Balancer, puoi iniziare a pubblicizzare il CIDR che hai AWS portato e che si trova nel pool definito. `--aws-service ec2` In questo tutorial, questo è il tuo pool Regionale. Per impostazione predefinita, il CIDR non è pubblicizzato, il che significa che non è accessibile pubblicamente su Internet. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account IPAM.

> **Note**
>
> Lo stato dell'annuncio non limita la capacità di assegnare indirizzi IP elastici. Anche se il tuo BYOIPv4 CIDR non è pubblicizzato, puoi comunque creare EIPs dal pool IPAM.

Inizia a pubblicizzare il CIDR usando il AWS CLI

- Esegui il comando seguente per pubblicizzare il CIDR.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
profile ipam-account
```

Nell'output, vedrai che il CIDR è pubblicizzato.

```
{
    "ByoipCidr": {
        "Cidr": "130.137.245.0/24",
        "State": "advertised"
    }
}
```

Passaggio 8: condivisione del pool regionale

Segui i passaggi di questa sezione per condividere il pool IPAM utilizzando AWS Resource Access Manager (RAM).

Abilitazione della condivisione delle risorse in AWS RAM

Dopo aver creato il tuo IPAM, ti consigliamo di condividere il pool regionale con altri account della tua organizzazione. Prima di condividere un pool IPAM, completa i passaggi di questa sezione per abilitare la condivisione delle risorse con. AWS RAM Se si utilizza AWS CLI per abilitare la condivisione delle risorse, utilizzare l'`--profile` **`management-account`**opzione.

Per abilitare la condivisione delle risorse

1. Utilizzando l'account AWS Organizations di gestione, apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, scegli Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Ora puoi condividere un pool IPAM con altri membri dell'organizzazione.

Condividi un pool IPAM utilizzando AWS RAM

In questa sezione condividerai il pool regionale con un altro account AWS Organizations membro. Per istruzioni complete sulla condivisione dei pool IPAM, comprese le informazioni sulle autorizzazioni IAM richieste, consulta Condivisione di un pool IPAM tramite AWS RAM. Se stai utilizzando AWS CLI per abilitare la condivisione delle risorse, usa l'`--profile` **`ipam-account`**opzione.

Per condividere un pool IPAM utilizzando AWS RAM

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato e il pool IPAM e seleziona Operazioni > Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. La AWS RAM console si apre. Si condivide il pool utilizzando AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).
6. Nella AWS RAM console, scegli nuovamente Crea una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona il tipo di risorsa, scegli Pool IPAM e poi l'ARN del pool che vuoi condividere.
9. Scegli Next (Successivo).

10. Scegli l'AWSRAMPermissionIpamPoolByoipCidrImportautorizzazione. I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione Condivisione di un pool IPAM tramite AWS RAM.
11. Scegli Next (Successivo).
12. Sotto le voci Principali > Seleziona il tipo principale, scegli Account AWS e inserisci l'ID dell'account che porterà un intervallo di indirizzi IP su IPAM, quindi scegli Aggiungi.
13. Scegli Next (Successivo).
14. Controlla le opzioni di condivisione delle risorse e i principali con cui condividerai, quindi scegli Crea.
15. Per consentire all'account **`member-account`** di assegnare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool`. Il valore per `--resource-arns` è l'ARN del pool IPAM creato nella sezione precedente. Il valore per `--principals` è l'ID account di **`member-account`**. Il valore per `--permission-arns` è l'ARN dell'autorizzazione `AWSRAMDefaultPermissionsIpamPool`.

Passaggio 9: assegnazione di un indirizzo IP elastico dal pool

Completa i passaggi in questa sezione per assegnare un indirizzo IP elastico dal pool. Tieni presente che se utilizzi IPv4 pool pubblici per allocare indirizzi IP elastici, puoi utilizzare i passaggi alternativi descritti in questa sezione Alternativa al passaggio 9 anziché i passaggi descritti in questa sezione.

> **Important**
>
> Se visualizzi un errore relativo alla mancanza delle autorizzazioni per chiamare ec2:AllocateAddress, l'autorizzazione gestita attualmente assegnata al pool IPAM che è stato condiviso con te deve essere aggiornata. Contatta la persona che ha creato la condivisione delle risorse e chiedile di aggiornare l'autorizzazione gestita di `AWSRAMPermissionIpamResourceDiscovery` alla versione predefinita. Per ulteriori informazioni, consulta Creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM .

AWS Management Console

Segui la procedura descritta in Allocare un indirizzo IP elastico nella Amazon EC2 User Guide per allocare l'indirizzo, ma tieni presente quanto segue:

- Questo passaggio deve essere eseguito dall'account membro.
- Assicurati che la AWS regione in cui ti trovi nella EC2 console corrisponda all'opzione Locale che hai scelto quando hai creato il pool regionale.
- Quando scegli il pool di indirizzi, scegli l'opzione Allocazione utilizzando un pool IPv4 IPAM e scegli il pool regionale che hai creato.

Command line

Assegna un indirizzo dal pool con il comando allocate-address. L'opzione `--region` che utilizzi deve corrispondere all'opzione `-locale` scelta al momento della creazione del pool nel passaggio 2. Includi l'ID del pool IPAM creato nel passaggio 2 in `--ipam-pool-id`. Facoltativamente, puoi anche scegliere un `/32` specifico nel tuo pool IPAM utilizzando l'opzione `--address`.

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

Risposta di esempio:

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

Per ulteriori informazioni, consulta Allocate an Elastic IP address nella Amazon EC2 User Guide.

Passaggio 10: associare l'indirizzo IP elastico a un' EC2 istanza

Completa i passaggi di questa sezione per associare l'indirizzo IP elastico a un' EC2istanza.

AWS Management Console

Segui i passaggi in Associare un indirizzo IP elastico nella Amazon EC2 User Guide per allocare un indirizzo IP elastico dal pool IPAM, ma tieni presente quanto segue: Quando utilizzi l'opzione Console di AWS gestione, la AWS regione in cui associ l'indirizzo IP elastico deve corrispondere all'opzione Locale che hai scelto quando hai creato il pool regionale.

Questo passaggio deve essere eseguito dall'account membro.

Command line

Questo passaggio deve essere eseguito dall'account membro. Utilizza l'opzione `--profile` **`member-account`**.

Associa l'indirizzo IP elastico a un'istanza con il comando associate-address. Il `--region` a cui associ l'indirizzo IP elastico deve corrispondere all'opzione `--locale` scelta al momento della creazione del pool regionale.

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

Risposta di esempio:

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

Per ulteriori informazioni, consulta Associare un indirizzo IP elastico a un'istanza o a un'interfaccia di rete nella Amazon EC2 User Guide.

Passaggio 11: pulizia

Segui i passaggi in questa sezione per ripulire le risorse che hai creato e di cui hai effettuato il provisioning in questo tutorial. Quando esegui i comandi in questa sezione, il valore per `--region` deve includere l'opzione `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP.

Pulisci usando il AWS CLI

1. Visualizza l'allocazione dell'EIP gestita in IPAM.

   Questo passaggio deve essere eseguito dall'account IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   L'output mostra l'assegnazione in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

2. Smettila di pubblicizzare il IPv4 CIDR.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
profile ipam-account
```

   Nell'output, potrai vedere che lo stato CIDR è cambiato da pubblicizzato a provisioning effettuato.

```
{
    "ByoipCidr": {
        "Cidr": "130.137.245.0/24",
        "State": "provisioned"
    }
}
```

3. Rilascia l'indirizzo IP elastico.

   Questo passaggio deve essere eseguito dall'account membro.

```
aws ec2 release-address --region us-west-2 --allocation-
id eipalloc-0db3405026756dbf6 --profile member-account
```

   Non vedrai alcun output quando esegui questo comando.

4. Come puoi vedere, l'allocazione dell'EIP non è più gestita in IPAM. IPAM può aver bisogno di tempo per rilevare che l'indirizzo IP elastico è stato rimosso. Non è possibile continuare a ripulire e revocare il provisioning del CIDR del pool IPAM fino a quando non si vede che l'assegnazione

è stata rimossa da IPAM. Quando esegui il comando in questa sezione, il valore per `--region` deve includere l'opzione `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

L'output mostra l'assegnazione in IPAM.

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

5. Revoca il provisioning del CIDR dal pool regionale. Quando esegui il comando in questo passaggio, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account IPAM.

   ```
   aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --cidr 130.137.245.0/24 --profile ipam-account
   ```

   Nell'output, sarà visualizzata la revoca del provisioning del CIDR in sospeso.

   ```
   {
       "IpamPoolCidr": {

           "Cidr": "130.137.245.0/24",

           "State": "pending-deprovision"

       }

   }
   ```

   La revoca del provisioning richiede tempo per il completamento. Controlla lo stato di revoca del provisioning.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Aspetta fino a quando visualizzerai provisioning revocato prima di passare al passaggio successivo.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

6. Elimina le condivisioni RAM e disabilita l'integrazione di RAM con AWS Organizations. Completa i passaggi in Eliminazione di una condivisione di risorse nella AWS RAM e Disabilitazione della condivisione delle risorse con le AWS organizzazioni nella AWS RAM User Guide, in quest'ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione della RAM con Organizations AWS .

   Questo passaggio deve essere eseguito rispettivamente dall'account IPAM e dall'account di gestione. Se stai utilizzando AWS CLI per eliminare le condivisioni RAM e disabilitare l'integrazione della RAM, utilizza le opzioni `--profile` **`ipam-account`** and `--profile` **`management-account`**.

7. Elimina il pool regionale. Quando esegui il comando in questo passaggio, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   Nell'output, è possibile visualizzare lo stato di eliminazione.

```
{
   "IpamPool": {
```

```
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
        "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0d8f3646b61ca5987",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "reg-ipv4-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

8. Revoca il provisioning del CIDR dal pool di livello superiore. Quando esegui il comando in questo passaggio, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account IPAM.

   ```
   aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
   pool-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --profile ipam-account
   ```

   Nell'output, sarà visualizzata la revoca del provisioning del CIDR in sospeso.

   ```
   {
       "IpamPoolCidr": {

           "Cidr": "130.137.245.0/24",

           "State": "pending-deprovision"

       }

   }
   ```

   La revoca del provisioning richiede tempo per il completamento. Utilizzare il seguente comando per controllare lo stato della revoca del provisioning.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Aspetta fino a quando visualizzerai provisioning revocato prima di passare al passaggio successivo.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. Elimina il pool di livello superiore. Quando esegui il comando in questo passaggio, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

   Nell'output, è possibile visualizzare lo stato di eliminazione.

```
{
  "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
```

```
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

10. Elimina l'IPAM. Quando esegui il comando in questo passaggio, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

    Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    Nell'output, visualizzerai la risposta IPAM. Ciò significa che l'IPAM è stato eliminato.

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-090e48e75758de279",

        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",

        "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",

        "ScopeCount": 2,

        "OperatingRegions": [

            {

                "RegionName": "us-east-1"

            },
            {
                "RegionName": "us-west-2"
            }
        ],
    }
```

```
}
```

Alternativa al passaggio 9

Se utilizzi IPv4 pool pubblici per allocare indirizzi IP elastici, puoi utilizzare i passaggi in questa sezione anziché i passaggi seguenti. Passaggio 9: assegnazione di un indirizzo IP elastico dal pool

Indice

- Fase 1: Creare un pool pubblico IPv4
- Fase 2: Fornisci il IPv4 CIDR pubblico al tuo pool pubblico IPv4
- Passaggio 3: creare un indirizzo IP elastico dal pool pubblico IPv4
- Alternativa alla pulizia del passaggio 9

Fase 1: Creare un pool pubblico IPv4

Questo passaggio viene in genere eseguito da un AWS account diverso che desidera fornire un indirizzo IP elastico, come l'account membro.

> **Important**
>
> I IPv4 pool pubblici e i pool IPAM sono gestiti da risorse distinte in AWS. I IPv4 pool pubblici sono risorse con account singolo che consentono di convertire gli indirizzi IP di proprietà pubblica in indirizzi IP CIDRs elastici. I pool IPAM possono essere utilizzati per allocare lo spazio pubblico ai pool pubblici. IPv4

Per creare un IPv4 pool pubblico utilizzando il AWS CLI

- Esegui il comando seguente per effettuare il provisioning del CIDR. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP.

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

  Nell'output, vedrai l'ID del IPv4 pool pubblico. Sarà necessario questo ID nel passaggio successivo.

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

Fase 2: Fornisci il IPv4 CIDR pubblico al tuo pool pubblico IPv4

Fornisci il IPv4 CIDR pubblico al tuo pool pubblico IPv4 . Il valore per `--region` deve corrispondere al valore `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP. La `--netmask-length` meno specifica che puoi definire è `24`.

Questo passaggio deve essere eseguito dall'account membro.

Per creare un IPv4 pool pubblico utilizzando il AWS CLI

1. Esegui il comando seguente per effettuare il provisioning del CIDR.

   ```
   aws ec2 provision-public-ipv4-pool-cidr --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --netmask-length 24
    --profile member-account
   ```

   Nell'output, sarà visualizzato il CIDR su cui è stato effettuato il provisioning.

   ```
   {
       "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
       "PoolAddressRange": {
           "FirstAddress": "130.137.245.0",
           "LastAddress": "130.137.245.255",
           "AddressCount": 256,
           "AvailableAddressCount": 256
       }
   }
   ```

2. Esegui il comando seguente per visualizzare il CIDR distribuito nel pool pubblico IPv4 .

   ```
   aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-
   account
   ```

   Nell'output, sarà visualizzato il CIDR su cui è stato effettuato il provisioning. Per impostazione predefinita, il CIDR non è pubblicizzato, il che significa che non è accessibile pubblicamente su

Internet. Avrai la possibilità di impostare questo CIDR su pubblicizzato nell'ultimo passaggio di questo tutorial.

```
{
    "ByoipCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "StatusMessage": "Cidr successfully provisioned",
            "State": "provisioned"
        }
    ]
}
```

Passaggio 3: creare un indirizzo IP elastico dal pool pubblico IPv4

Crea un indirizzo IP elastico (EIP) dal IPv4 pool pubblico. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account membro.

Per creare un EIP dal IPv4 pool pubblico utilizzando il AWS CLI

1. Per creare l'EIP, esegui il comando seguente.

   ```
   aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
   ec2-0019eed22a684e0b2 --profile member-account
   ```

   Nell'output, potrai vedere l'assegnazione.

   ```
   {
       "PublicIp": "130.137.245.100",
       "AllocationId": "eipalloc-0db3405026756dbf6",
       "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
       "NetworkBorderGroup": "us-east-1",
       "Domain": "vpc"
   }
   ```

2. Esegui il comando seguente per visualizzare l'assegnazione EIP gestita in IPAM.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

L'output mostra l'assegnazione in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Alternativa alla pulizia del passaggio 9

Completa questi passaggi per pulire i IPv4 pool pubblici creati con l'alternativa al passaggio 9. È necessario completare questi passaggi dopo aver rilasciato l'indirizzo IP elastico durante il processo di pulizia standard in Passaggio 10: eliminazione.

1. Visualizza il tuo BYOIP CIDRs.

   Questo passaggio deve essere eseguito dall'account membro.

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

   Nell'output, vedrai gli indirizzi IP nel tuo CIDR BYOIP.

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
               "Description": "",
               "PoolAddressRanges": [
                   {
   ```

```
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 256
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 256,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

2. Rilascia il CIDR dal pool pubblico. IPv4 Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account membro.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-ec2-0019eed22a684e0b2 --cidr 130.137.245.0/24 --profile member-account
```

3. Visualizza CIDRs nuovamente il tuo BYOIP e assicurati che non ci siano altri indirizzi forniti. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account membro.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
```

   Nell'output, vedrai il numero di indirizzi IP nel tuo pool pubblico. IPv4

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

```
        }
    ]
}
```

Porta il tuo IPv6 CIDR su IPAM usando solo la CLI AWS

Segui questi passaggi per portare un IPv6 CIDR a IPAM e allocare un VPC utilizzando solo il. AWS CLI

Se non è necessario pubblicizzare i propri IPv6 indirizzi su Internet, è possibile fornire un indirizzo GUA privato a IPv6 un IPAM. Per ulteriori informazioni, consulta Abilita il provisioning GUA privato IPv6 CIDRs.

Important

- Questo tutorial presuppone che tu abbia già completato i passaggi nelle sezioni seguenti:
  - Integrare IPAM con gli account di un'organizzazione AWS.
  - Crea un IPAM.
- Ogni passaggio di questo tutorial deve essere eseguito da uno dei tre account AWS Organizations:
  - L'account di gestione.
  - L'account membro configurato come amministratore IPAM in Integrare IPAM con gli account di un'organizzazione AWS. In questo tutorial, tale account verrà chiamato account IPAM.
  - L'account membro dell'organizzazione che verrà allocato CIDRs da un pool IPAM. In questo tutorial, tale account verrà chiamato account membro.

Indice

- Fase 1: Creare profili AWS CLI denominati e ruoli IAM
- Passaggio 2: creazione di un IPAM
- Passaggio 3: creazione di un pool IPAM
- Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore
- Passaggio 5: creazione di un pool regionale all'interno del pool di livello superiore

- Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale
- Fase 7. Condividi il pool regionale
- Fase 8: Creare un VPC utilizzando il CIDR IPv6
- Passaggio 9: pubblicizzare il CIDR
- Passaggio 10: eliminazione

Fase 1: Creare profili AWS CLI denominati e ruoli IAM

Per completare questo tutorial come singolo AWS utente, puoi utilizzare i profili AWS CLI denominati per passare da un ruolo IAM a un altro. I profili denominati sono raccolte di impostazioni e credenziali a cui si fa riferimento quando si utilizza l'opzione `--profile` con la AWS CLI. Per ulteriori informazioni su come creare ruoli IAM e profili denominati per AWS gli account, consulta Using an IAM role in AWS CLI.

Crea un ruolo e un profilo denominato per ciascuno dei tre AWS account che utilizzerai in questo tutorial:

- Un profilo chiamato `management-account` per l'account di gestione AWS Organizations.
- Un profilo chiamato `ipam-account` per l'account membro AWS Organizations configurato per essere l'amministratore IPAM.
- Un profilo chiamato `member-account` per l'account membro AWS Organizations dell'organizzazione che verrà allocato CIDRs da un pool IPAM.

Dopo avere creato i ruoli IAM e i profili denominati, torna su questa pagina e vai al passaggio successivo. Nel resto di questo tutorial noterete che AWS CLI i comandi di esempio utilizzano l'`--profile`opzione con uno dei profili denominati per indicare quale account deve eseguire il comando.

Passaggio 2: creazione di un IPAM

Questa fase è facoltativa. Se un IPAM è già stato creato con regioni operative di `us-east-1` e `us-west-2` create, questo passaggio può essere ignorato. Crea un IPAM e specifica una Regione operativa di `us-east-1` e `us-west-2`. È necessario selezionare una Regione operativa in modo da poter utilizzare l'opzione località durante la creazione del pool IPAM. L'integrazione IPAM con BYOIP richiede che la località sia impostata su qualsiasi pool verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account IPAM.

Esegui il comando seguente:

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

Nell'output sarà visualizzato l'IPAM creato. Prendere nota del valore per `PublicDefaultScopeId`. L'ID dell'ambito pubblico è necessario nella fase successiva.

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

Passaggio 3: creazione di un pool IPAM

Poiché si intende creare un pool IPAM di livello superiore con un pool Regionale al suo interno e si andrà ad assegnare spazio a una risorsa (un VPC) dal pool Regionale, la località andrà impostata sul pool Regionale e non sul pool di livello superiore. La località sarà aggiunta al pool regionale una volta creato il pool Regionale in un passaggio successivo. L'integrazione IPAM con BYOIP richiede che la località sia impostata su qualsiasi pool verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account IPAM.

Scegli se vuoi che questo pool IPAM CIDR sia pubblicizzabile AWS su Internet pubblico (`--publicly-advertisable`o). `--no-publicly-advertisable`

> **Note**
>
> Tieni presente che l'ID dell'ambito deve essere l'ID per l'ambito pubblico e la famiglia di indirizzi deve essere`ipv6`.

Per creare un pool di IPv6 indirizzi per tutte le tue AWS risorse, utilizza il AWS CLI

1. Esegui il comando seguente per creare un pool IPAM. Utilizza l'ID dell'ambito pubblico dell'IPAM creato nella fase precedente.

```
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
```

   Nell'output, vedrai `create-in-progress`, il che indica che è in corso la creazione del pool.

```
{
    "IpamPool": {

        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-07f2466c7158b50c4",

        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-07f2466c7158b50c4",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",

        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",

        "Locale": "None",

        "PoolDepth": 1,

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

        "Description": "top-level-Ipv6-pool",

        "AutoImport": false,
```

```
        "Advertisable": true,

        "AddressFamily": "ipv6",

        "Tags": []

    }

}
```

2. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `create-complete` nell'output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Il seguente output esemplificativo mostra lo stato del pool.

```
{
    "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": []

    }

}
```

Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore

Effettua il provisioning di un blocco CIDR al pool di livello superiore. Tieni presente che quando esegui il provisioning di un IPv6 CIDR a un pool all'interno del pool di primo livello, l'intervallo di IPv6 indirizzi più specifico che puoi inserire è /48 per quelli pubblicizzabili pubblicamente e /60 per CIDRs CIDRs quelli non pubblicizzabili pubblicamente.

> **Note**
>
> - Se hai verificato il controllo del dominio con un certificato X.509, devi includere il CIDR e il messaggio BYOIP e la firma del certificato che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.
> - Se hai verificato il controllo del dominio con un record TXT DNS, devi includere il CIDR e il token di verifica IPAM che hai creato in quel passaggio in modo da poter verificare il controllo dello spazio pubblico.

È necessario solo verificare il controllo del dominio quando si effettua il provisioning del CIDR BYOIP al pool di livello superiore. Per il pool regionale all'interno del pool di livello superiore, è possibile omettere l'opzione della proprietà del dominio.

Questo passaggio deve essere eseguito dall'account IPAM.

Per fornire un blocco CIDR al pool utilizzando il AWS CLI

1. Per eseguire il provisioning del CIDR con le informazioni sul certificato, utilizzare il seguente esempio di comando. Oltre a sostituire i valori necessari nell'esempio, assicurati di sostituire `Message` e `Signature` con i valori `text_message` e `signed_message` che hai inserito in Verifica il dominio con un certificato X.509.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-
x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|
20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

Per eseguire il provisioning del CIDR con le informazioni sul token di verifica, utilizzare il seguente esempio di comando. Oltre a sostituire i valori necessari nell'esempio, assicurati di sostituire `ipam-ext-res-ver-token-0309ce7f67a768cf0` e con l'ID token `IpamExternalResourceVerificationTokenId` che hai inserito in Verifica il dominio con un record TXT DNS.

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

Nell'output, sarà visualizzato il provisioning del CIDR in sospeso.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "pending-provision"

    }

}
```

2. Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare.

> **Important**
>
> Sebbene la maggior parte del provisioning venga completata entro due ore, il completamento del processo di provisioning per gli intervalli pubblicizzabili pubblicamente può richiedere fino a una settimana.

Esegui il seguente comando fino a quando non viene visualizzato uno stato di `provisioned` nell'output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Il seguente output esemplificativo mostra lo stato.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Passaggio 5: creazione di un pool regionale all'interno del pool di livello superiore

Crea un pool Regionale all'interno del pool di livello superiore. Il codice `--locale` è obbligatorio nel pool e deve essere una delle Regioni operative configurate al momento della creazione dell'IPAM.

Questo passaggio deve essere eseguito dall'account IPAM.

> **Important**
>
> Quando crei il pool, devi includere `--aws-service ec2`. Il servizio selezionato determina il AWS servizio in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione è `ec2` che ciò che viene CIDRs allocato da questo pool sarà pubblicizzabile per il EC2 servizio Amazon e il servizio Amazon VPC (per CIDRs associato a). VPCs

Per creare di un pool Regionale utilizzando la AWS CLI

1. Per creare un pool, esegui il comando seguente.

```
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
```

Nell'output, potrai visualizzare IPAM mentre crea il pool.

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0053b7d2b4fc3f730",
        "SourceIpamPoolId": "ipam-pool-07f2466c7158b50c4",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0053b7d2b4fc3f730",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-west-2",
        "PoolDepth": 2,
        "State": "create-in-progress",
        "Description": "reg-ipv6-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv6",
        "Tags": [],
        "ServiceType": "ec2"
    }
}
```

2. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `create-complete` nell'output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Nell'output, vedrai i pool contenuti nel tuo IPAM. In questo tutorial è stato creato un pool di livello superiore e un pool Regionale, in modo da vederli entrambi.

Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale

Effettua il provisioning di un blocco CIDR al pool Regionale. Tieni presente che quando fornisci il CIDR a un pool all'interno del pool di primo livello, l'intervallo di IPv6 indirizzi più specifico che

puoi inserire è /48 per quelli CIDRs che sono pubblicizzabili pubblicamente e /60 per quelli non pubblicizzabili pubblicamente. CIDRs

Questo passaggio deve essere eseguito dall'account IPAM.

Per assegnare un blocco CIDR al pool regionale utilizzando il AWS CLI

1. Esegui il comando seguente per effettuare il provisioning del CIDR.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   Nell'output, sarà visualizzato il provisioning del CIDR in sospeso.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
}
```

2. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `provisioned` nell'output.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   Il seguente output esemplificativo mostra lo stato corretto.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Fase 7. Condividi il pool regionale

Segui i passaggi di questa sezione per condividere il pool IPAM utilizzando AWS Resource Access Manager (RAM).

Abilitazione della condivisione delle risorse in AWS RAM

Dopo aver creato il tuo IPAM, ti consigliamo di condividere il pool regionale con altri account della tua organizzazione. Prima di condividere un pool IPAM, completa i passaggi di questa sezione per abilitare la condivisione delle risorse con. AWS RAM Se si utilizza AWS CLI per abilitare la condivisione delle risorse, utilizzare l'`--profile` **`management-account`**opzione.

Per abilitare la condivisione delle risorse

1. Utilizzando l'account AWS Organizations di gestione, apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, scegli Abilita condivisione con AWS Organizations, quindi scegli Salva impostazioni.

Ora puoi condividere un pool IPAM con altri membri dell'organizzazione.

Condividi un pool IPAM utilizzando AWS RAM

In questa sezione condividerai il pool regionale con un altro account AWS Organizations membro. Per istruzioni complete sulla condivisione dei pool IPAM, comprese le informazioni sulle autorizzazioni IAM richieste, consulta Condivisione di un pool IPAM tramite AWS RAM. Se stai utilizzando AWS CLI per abilitare la condivisione delle risorse, usa l'`--profile` **`ipam-account`**opzione.

Per condividere un pool IPAM utilizzando AWS RAM

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato e il pool IPAM e seleziona Operazioni > Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. La AWS RAM console si apre. Si condivide il pool utilizzando AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).
6. Nella AWS RAM console, scegli nuovamente Crea una condivisione di risorse.

7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona il tipo di risorsa, scegli Pool IPAM e poi l'ARN del pool che vuoi condividere.
9. Scegli Next (Successivo).
10. Scegli l'AWSRAMPermissionIpamPoolByoipCidrImportautorizzazione. I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione Condivisione di un pool IPAM tramite AWS RAM.
11. Scegli Next (Successivo).
12. Sotto le voci Principali > Seleziona il tipo principale, scegli Account AWS e inserisci l'ID dell'account che porterà un intervallo di indirizzi IP su IPAM, quindi scegli Aggiungi.
13. Scegli Next (Successivo).
14. Controlla le opzioni di condivisione delle risorse e i principali con cui condividerai, quindi scegli Crea.
15. Per consentire all'account **`member-account`** di assegnare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool`. Il valore per `--resource-arns` è l'ARN del pool IPAM creato nella sezione precedente. Il valore per `--principals` è l'ID account di **`member-account`**. Il valore per `--permission-arns` è l'ARN dell'autorizzazione `AWSRAMDefaultPermissionsIpamPool`.

Fase 8: Creare un VPC utilizzando il CIDR IPv6

Crea un VPC utilizzando l'ID del pool IPAM. È necessario associare anche un blocco IPv4 CIDR al VPC utilizzando l'opzione o `--cidr-block` la richiesta avrà esito negativo. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account membro.

Per creare un VPC con il IPv6 CIDR utilizzando il AWS CLI

1. Esegui il comando seguente per effettuare il provisioning del CIDR.

```
aws ec2 create-vpc --region us-west-2 --ipv6-ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr-block 10.0.0.0/16 --ipv6-netmask-length 56 --
profile member-account
```

   Nell'output, visualizzerai il VPC mentre viene creato.

```
{
    "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. Visualizza l'assegnazione VPC in IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

Nell'output, potrai vedere l'assegnazione.

```
{
    "IpamPoolAllocations": [
        {
```

```
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Passaggio 9: pubblicizzare il CIDR

Dopo aver creato il VPC con CIDR allocato in IPAM, puoi iniziare a pubblicizzare il CIDR a cui hai portato AWS che si trova nel pool definito. `--aws-service ec2` In questo tutorial, questo è il tuo pool Regionale. Per impostazione predefinita, il CIDR non è pubblicizzato, il che significa che non è accessibile pubblicamente su Internet. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool Regionale che verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account IPAM.

Inizia a pubblicizzare il CIDR usando il AWS CLI

- Esegui il comando seguente per pubblicizzare il CIDR.

  ```
  aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
  profile ipam-account
  ```

  Nell'output, vedrai che il CIDR è pubblicizzato.

  ```
  {
      "ByoipCidr": {
          "Cidr": "2605:9cc0:409::/48",
          "State": "advertised"
      }
  }
  ```

Passaggio 10: eliminazione

Segui i passaggi in questa sezione per ripulire le risorse che hai creato e di cui hai effettuato il provisioning in questo tutorial. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool Regionale che verrà utilizzato per il CIDR BYOIP.

Pulisci usando il AWS CLI

1. Esegui il comando seguente per visualizzare l'assegnazione VPC gestita in IPAM.

   Questo passaggio deve essere eseguito dall'account IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   L'output mostra l'assegnazione in IPAM.

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "2605:9cc0:409::/56",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
               "ResourceId": "vpc-00b5573ffc3b31a29",
               "ResourceType": "vpc",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

2. Esegui il comando seguente per smettere di pubblicizzare il CIDR. Quando esegui il comando in questo passaggio, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool Regionale che verrà utilizzato per il CIDR BYOIP.

   Questo passaggio deve essere eseguito dall'account IPAM.

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
   profile ipam-account
   ```

   Nell'output, potrai vedere che lo stato CIDR è cambiato da pubblicizzato a provisioning effettuato.

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "provisioned"
    }
}
```

3. Esegui il seguente comando per eliminare il VPC. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool Regionale che verrà utilizzato per il CIDR BYOIP.

   Questo passaggio deve essere eseguito dall'account membro.

   ```
   aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
   profile member-account
   ```

   Non vedrai alcun output quando esegui questo comando.

4. Esegui il comando seguente per visualizzare l'assegnazione VPC gestita in IPAM. IPAM può aver bisogno di tempo per rilevare che il VPC è stato eliminato e rimuovere questa assegnazione. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--locale` che hai inserito quando hai creato il pool Regionale che verrà utilizzato per il CIDR BYOIP.

   Questo passaggio deve essere eseguito dall'account IPAM.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   L'output mostra l'assegnazione in IPAM.

   ```
   {
      "IpamPoolAllocations": [

           {

               "Cidr": "2605:9cc0:409::/56",

               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
   ```

```
            "ResourceId": "vpc-00b5573ffc3b31a29",

            "ResourceType": "vpc",

            "ResourceOwner": "123456789012"

        }

    ]

}
```

Esegui di nuovo il comando e cerca l'assegnazione da rimuovere. Non è possibile continuare a ripulire e revocare il provisioning del CIDR del pool IPAM fino a quando non si vede che l'assegnazione è stata rimossa da IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

L'output mostra l'assegnazione rimossa da IPAM.

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

5. Elimina le condivisioni RAM e disabilita l'integrazione di RAM con AWS Organizations. Completa i passaggi in Eliminazione di una condivisione di risorse nella AWS RAM e Disabilitazione della condivisione delle risorse con le AWS organizzazioni nella AWS RAM User Guide, in quest'ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione della RAM con Organizations AWS .

   Questo passaggio deve essere eseguito rispettivamente dall'account IPAM e dall'account di gestione. Se stai utilizzando AWS CLI per eliminare le condivisioni RAM e disabilitare l'integrazione della RAM, utilizza le opzioni `--profile` **`ipam-account`** and `--profile` **`management-account`**.

6. Esegui il seguente comando per revocare il provisioning del CIDR del pool Regionale.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

Nell'output, sarà visualizzata la revoca del provisioning del CIDR in sospeso.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

La revoca del provisioning richiede tempo per il completamento. Continua a eseguire il comando fino a quando non viene visualizzato lo stato CIDR provisioning revocato.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

Nell'output, sarà visualizzata la revoca del provisioning del CIDR in sospeso.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "deprovisioned"
    }
}
```

7. Esegui il seguente comando per eliminare il pool Regionale.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   Nell'output, è possibile visualizzare lo stato di eliminazione.

```
{
    "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. Esegui il seguente comando per revocare il provisioning del CIDR del pool di livello superiore.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   Nell'output, sarà visualizzata la revoca del provisioning del CIDR in sospeso.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   La revoca del provisioning richiede tempo per il completamento. Utilizzare il seguente comando per controllare lo stato della revoca del provisioning.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Aspetta fino a quando visualizzerai provisioning revocato prima di passare al passaggio successivo.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. Esegui il seguente comando per eliminare il pool di livello superiore.

   Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

   Nell'output, è possibile visualizzare lo stato di eliminazione.

```
{
    "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. Esegui il seguente comando per eliminare l'IPAM.

    Questo passaggio deve essere eseguito dall'account IPAM.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    Nell'output, visualizzerai la risposta IPAM. Ciò significa che l'IPAM è stato eliminato.

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-090e48e75758de279",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",
        "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",
        "ScopeCount": 2,
        "OperatingRegions": [
            {

                "RegionName": "us-east-1"

            },
            {
                "RegionName": "us-west-2"
            }
        ]
    }
}
```

Tutorial: trasferimento di un IPv4 CIDR BYOIP a IPAM

Segui questi passaggi per trasferire un IPv4 CIDR esistente in IPAM. Se disponi già di un CIDR IPv4 BYOIP con AWS, puoi spostare il CIDR in IPAM da un pool pubblico. IPv4 Non è possibile spostare un CIDR in IPAM. IPv6

Questo tutorial presuppone che tu abbia già introdotto con successo un intervallo di indirizzi IP AWS utilizzando il processo descritto in Bring your own IP address (BYOIP) in Amazon EC2 e ora desideri

trasferire quell'intervallo di indirizzi IP su IPAM. Se stai inserendo un nuovo indirizzo IP AWS per la prima volta, completa i passaggi indicati in. Tutorial: trasferisci i tuoi indirizzi IP su IPAM

Se si trasferisce un IPv4 pool pubblico a IPAM, non vi è alcun impatto sulle allocazioni esistenti. Dopo aver trasferito un IPv4 pool pubblico in IPAM, a seconda del tipo di risorsa, potresti essere in grado di monitorare le allocazioni esistenti. Per ulteriori informazioni, consulta Monitoraggio dell'utilizzo del CIDR per risorsa.

> **Note**
>
> - Questo tutorial presuppone che tu abbia già completato i passaggi nella sezione Crea un IPAM.
> - Ogni passaggio di questo tutorial deve essere eseguito da uno dei due account: AWS
>   - L'account amministratore dell'amministratore di IPAM. In questo tutorial, tale account verrà chiamato account IPAM.
>   - L'account dell'organizzazione che possiede il CIDR BYOIP. In questo tutorial, tale account verrà chiamato account proprietario del CIDR BYOIP.

Indice

- Fase 1: Creare profili AWS CLI denominati e ruoli IAM
- Passaggio 2: ottenimento dell'ID di ambito pubblico dell'IPAM
- Passaggio 3: creazione di un pool IPAM
- Passaggio 4: condividere il pool IPAM utilizzando AWS RAM
- Passaggio 5: trasferimento di un CIDR BYOIP IPV4 esistente in IPAM
- Passaggio 6: visualizzazione del CIDR in IPAM
- Passaggio 7: pulizia

Fase 1: Creare profili AWS CLI denominati e ruoli IAM

Per completare questo tutorial come singolo AWS utente, puoi utilizzare i profili AWS CLI denominati per passare da un ruolo IAM a un altro. I profili denominati sono raccolte di impostazioni e credenziali a cui si fa riferimento quando si utilizza l'opzione `--profile` con la AWS CLI. Per ulteriori informazioni su come creare ruoli IAM e profili denominati per AWS gli account, consulta Using an IAM role in AWS CLI.

Crea un ruolo e un profilo con nome per ciascuno dei tre AWS account che utilizzerai in questo tutorial:

- Un profilo chiamato `ipam-account` per l' AWS account che è l'amministratore IPAM.
- Un profilo chiamato `byoip-owner-account` per l' AWS account dell'organizzazione che possiede il CIDR BYOIP.

Dopo avere creato i ruoli IAM e i profili denominati, torna su questa pagina e vai al passaggio successivo. Nel resto di questo tutorial noterete che AWS CLI i comandi di esempio utilizzano l'`--profile`opzione con uno dei profili denominati per indicare quale account deve eseguire il comando.

Passaggio 2: ottenimento dell'ID di ambito pubblico dell'IPAM

Per ottenere l'ID di ambito pubblico dell'IPAM, segui la procedura descritta in questa sezione. Questo passaggio deve essere eseguito dall'account **`ipam-account`**.

Esegui il comando seguente per ottenere l'ID di ambito pubblico.

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

Nell'output, vedrai il tuo ID di ambito pubblico. Tieni presente i valori di `PublicDefaultScopeId`. Questo valore servirà nella fase successiva.

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

Passaggio 3: creazione di un pool IPAM

Per creare un pool IPAM, segui i passaggi riportati in questa sezione. Questo passaggio deve essere eseguito dall'account **`ipam-account`**. Il pool IPAM creato deve essere un pool di livello superiore con l'opzione `--locale` corrispondente alla Regione AWS del CIDR BYOIP. È possibile trasferire un BYOIP solo a un pool IPAM di livello superiore.

> **Important**
>
> Quando crei il pool, devi includere `--aws-service ec2`. Il servizio selezionato determina il AWS servizio in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione è `ec2` che ciò che viene CIDRs allocato da questo pool sarà pubblicizzabile per il EC2 servizio Amazon (per indirizzi IP elastici) e il servizio Amazon VPC (per CIDRs associato a). VPCs

Per creare un pool di IPv4 indirizzi per il CIDR BYOIP trasferito utilizzando il AWS CLI

1. Esegui il comando seguente per creare un pool IPAM. Utilizza l'ID dell'ambito pubblico dell'IPAM recuperato nella fase precedente.

   ```
   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
   ```

   Nell'output, vedrai `create-in-progress`, il che indica che è in corso la creazione del pool.

   ```
   {
       "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. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `create-complete` nell'output.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

Il seguente output esemplificativo mostra lo stato del pool. Ti servirà OwnerIdnel passaggio successivo.

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

Passaggio 4: condividere il pool IPAM utilizzando AWS RAM

Segui i passaggi di questa sezione per condividere un pool IPAM in AWS RAM modo che un altro AWS account possa trasferire un IPV4 CIDR BYOIP esistente nel pool IPAM e utilizzare il pool IPAM. Questo passaggio deve essere eseguito dall'account **`ipam-account`**.

Per condividere un pool di indirizzi utilizzando il IPv4 AWS CLI

1. Visualizza le AWS RAM autorizzazioni disponibili per i pool IPAM. Sono necessari entrambi ARNs per completare i passaggi descritti in questa sezione.

```
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. Crea una condivisione di risorse per consentire all'**byoip-owner-account**account di importare BYOIP CIDRs in IPAM. Il valore per `--resource-arns` è l'ARN del pool IPAM creato nella sezione precedente. Il valore per `--principals` è l'ID account dell'account che detiene il CIDR BYOIP. Il valore per `--permission-arns` è l'ARN dell'autorizzazione `AWSRAMPermissionIpamPoolByoipCidrImport`.

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare2 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMPermissionIpamPoolByoipCidrImport
```

```
{

    "resourceShare": {

        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7993758c-a4ea-43ad-be12-b3abaffe361a",
        "name": "PoolShare2",

        "owningAccountId": "123456789012",

        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:32:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:32:25.536000-07:00"

        }

}
```

3. (Facoltativo) Se desideri consentire all'**byoip-owner-account**account di allocare gli indirizzi IP CIDR dal pool IPAM ai IPv4 pool pubblici dopo il completamento del trasferimento, copia l'ARN per `AWSRAMDefaultPermissionsIpamPool` e crea una seconda condivisione di risorse. Il valore per `--resource-arns` è l'ARN del pool IPAM creato nella sezione precedente. Il valore per `--principals` è l'ID account dell'account che detiene il CIDR BYOIP. Il valore per `--permission-arns` è l'ARN dell'autorizzazione `AWSRAMDefaultPermissionsIpamPool`.

```
aws ram create-resource-share --region us-east-1 --profile ipam-account
 --name PoolShare1 --resource-arns arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a03d430ca3f5c035 --principals 111122223333 --permission-arns
 arn:aws:ram::aws:permission/AWSRAMDefaultPermissionsIpamPool
```


```
{

    "resourceShare": {

        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f",
        "name": "PoolShare1",

        "owningAccountId": "123456789012",

        "allowExternalPrincipals": true,

        "status": "ACTIVE",

        "creationTime": "2023-04-28T07:31:25.536000-07:00",

        "lastUpdatedTime": "2023-04-28T07:31:25.536000-07:00"

        }

}
```


Dopo aver creato la condivisione di risorse nella RAM, l' byoip-owner-accountaccount può ora passare a IPAM. CIDRs

Passaggio 5: trasferimento di un CIDR BYOIP IPV4 esistente in IPAM

Segui i passaggi in questa sezione per trasferire un CIDR IPV4 BYOIP esistente in IPAM. Questo passaggio deve essere eseguito dall'account **byoip-owner-account**.

> **Important**
>
> Una volta impostato un intervallo di IPv4 indirizzi AWS, è possibile utilizzare tutti gli indirizzi IP dell'intervallo, incluso il primo indirizzo (l'indirizzo di rete) e l'ultimo indirizzo (l'indirizzo di trasmissione).

Per trasferire il CIDR BYOIP su IPAM, il proprietario del CIDR BYOIP deve disporre di queste autorizzazioni nella policy IAM:

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> È possibile utilizzare il AWS Management Console o il AWS CLI per questo passaggio.

AWS Management Console

Per trasferire un CIDR BYOIP nel pool IPAM:

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/come **`byoip-owner-account`** account.
2. Nel pannello di navigazione, seleziona Pool.
3. Sceglie il pool di primo livello creato e condiviso in questo tutorial.
4. Scegli Azioni > Trasferisci CIDR BYOIP.
5. Scegli Trasferisci CIDR BYOIP.
6. Scegli il tuo CIDR BYOIP.
7. Scegli Provision (Esegui il provisioning).

Command line

Utilizza i seguenti AWS CLI comandi per trasferire un CIDR BYOIP al pool IPAM utilizzando: AWS CLI

1. Esegui il comando seguente per trasferire il CIDR. Assicuratevi che il `--region` valore sia la AWS regione del CIDR BYOIP.

```
aws ec2 move-byoip-cidr-to-ipam --region us-west-2 --profile byoip-owner-account
 --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --ipam-pool-owner 123456789012 --
cidr 130.137.249.0/24
```

   Nell'output, sarà visualizzato il provisioning del CIDR in sospeso.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "pending-transfer"

    }

}
```

2. Assicurarsi che il CIDR sia stato trasferito. Esegui il seguente comando fino a quando non viene visualizzato uno stato di `complete-transfer` nell'output.

```
aws ec2 move-byoip-cidr-to-ipam --region us-west-2  --profile byoip-
owner-account --ipam-pool-id ipam-pool-0a03d430ca3f5c035 --ipam-pool-
owner 123456789012 --cidr 130.137.249.0/24
```

   Il seguente output esemplificativo mostra lo stato.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

Passaggio 6: visualizzazione del CIDR in IPAM

Per visualizzare il CIDR in IPAM, segui i passaggi riportati in questa sezione. Questo passaggio deve essere eseguito dall'account **`ipam-account`**.

Per visualizzare il CIDR BYOIP trasferito nel pool IPAM utilizzando il AWS CLI

- Esegui il comando seguente per visualizzare l'assegnazione gestita in IPAM. Assicurati che il `--region` valore sia la AWS regione del CIDR BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

  L'output mostra l'assegnazione in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

Passaggio 7: pulizia

Segui i passaggi in questa sezione per rimuovere le risorse che hai creato in questo tutorial. Questo passaggio deve essere eseguito dall'account **`ipam-account`**.

Per pulire le risorse create in questo tutorial usando il AWS CLI

1. Per eliminare la risorsa condivisa del pool IPAM, esegui il seguente comando per ottenere il primo ARN di condivisione delle risorse:

```
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. Copia l'ARN della condivisione di risorse e utilizzalo per eliminare la condivisione di risorse del pool IPAM.

```
aws ram delete-resource-share --region us-east-1 --profile ipam-account
 --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/8d1e229b-2830-4cf4-8b10-19c889235a2f
```

```
{
    "returnValue": true
}
```

3. Se hai creato una condivisione di risorse aggiuntiva in Passaggio 4: condividere il pool IPAM utilizzando AWS RAM, ripeti i due passaggi precedenti per ottenere l'ARN della seconda condivisione di risorse per `PoolShare2` ed eliminare la seconda condivisione di risorse.

4. Esegui il comando seguente per ottenere l'ID di assegnazione per il CIDR BYOIP. Assicurati che il `--region` valore corrisponda alla AWS regione del CIDR BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

L'output mostra l'assegnazione in IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

5. Rilascia il CIDR dal pool pubblico. IPv4 Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account **`byoip-owner-account`**.

   ```
   aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1  --profile byoip-
   owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.0/24
   ```

6. Visualizza CIDRs nuovamente il tuo BYOIP e assicurati che non ci siano altri indirizzi forniti. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere alla Regione del tuo IPAM.

   Questo passaggio deve essere eseguito dall'account **`byoip-owner-account`**.

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
   ```

   Nell'output, vedrai il conteggio degli indirizzi IP nel tuo pool pubblico. IPv4

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
               "Description": "",
               "PoolAddressRanges": [],
               "TotalAddressCount": 0,
               "TotalAvailableAddressCount": 0,
   ```

```
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

7. Esegui il seguente comando per eliminare il pool di livello superiore.

```
aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
id ipam-pool-0a03d430ca3f5c035
```

Nell'output, è possibile visualizzare lo stato di eliminazione.

```
{
    "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4",
        "AwsService": "ec2"
    }
}
```

Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti

Completa questo tutorial per pianificare lo spazio degli indirizzi IP VPC per l'allocazione degli indirizzi IP alle sottoreti VPC e monitorare le metriche correlate agli indirizzi IP a livello di sottorete e VPC.

> **Note**
>
> Questo tutorial illustra l'allocazione dello spazio degli IPv4 indirizzi privati in un ambito IPAM privato alle sottoreti VPCs e alle sottoreti. Puoi anche completare questo tutorial utilizzando un intervallo IPv6 CIDR creando il VPC con un'opzione di blocco CIDR IPv6 fornita da Amazon sulla console VPC.

La pianificazione dello spazio degli indirizzi IP VPC per le sottoreti consente di effettuare le seguenti operazioni:

- Pianificare e organizzare gli indirizzi IP del tuo VPC per l'allocazione alle sottoreti: puoi dividere lo spazio degli indirizzi IP VPC in blocchi CIDR più piccoli ed eseguire il provisioning di tali blocchi CIDR a sottoreti con esigenze aziendali diverse, ad esempio se esegui carichi di lavoro in sottoreti di sviluppo o produzione.
- Semplificare l'allocazione degli indirizzi IP per le sottoreti VPC: una volta pianificato e organizzato lo spazio degli indirizzi VPC, puoi scegliere la lunghezza della maschera di rete anziché inserire manualmente un CIDR. Ad esempio, se uno sviluppatore sta creando una sottorete per ospitare carichi di lavoro di sviluppo, deve scegliere un pool e una lunghezza della maschera di rete per la sottorete, e IPAM allocherà automaticamente il blocco CIDR alla sottorete.

L'esempio seguente mostra la gerarchia del pool e la struttura delle risorse che creerai con questo tutorial:

- Ambito privato
  - Pool di pianificazione delle risorse (10.0.0.0/20)
    - Pool di sottoreti di sviluppo (10.0.0.0/24)
      - Sottorete di sviluppo (10.0.0.0/28)
    - Pool di sottoreti di produzione (10.0.0.1/24)
      - Sottorete di produzione (10.0.0.16/28)

> **Important**
>
> - Il pool di pianificazione delle risorse può essere utilizzato per l'allocazione CIDRs a sottoreti o può essere utilizzato come pool di sorgenti in cui è possibile creare altri pool. In questo

tutorial, utilizziamo il pool di pianificazione delle risorse come pool di origini per i pool di sottoreti.

- È possibile creare più pool di pianificazione delle risorse utilizzando lo stesso VPC se al VPC è stato assegnato più di un CIDR; se a un VPC ne sono CIDRs assegnati due, ad esempio, è possibile creare due pool di pianificazione delle risorse, uno per ogni CIDR. Ogni CIDR può essere assegnato a un pool alla volta.

Fase 1. Creazione di un VPC

Completa i passaggi descritti in questa sezione per creare un VPC da utilizzare per la pianificazione degli indirizzi IP delle sottoreti. Per ulteriori informazioni sulle autorizzazioni IAM necessarie per la creazione VPCs, consulta gli esempi di policy di Amazon VPC nella Amazon VPC User Guide.

> **Note**
>
> Puoi utilizzare un VPC esistente anziché crearne uno nuovo, ma questo tutorial è incentrato sullo scenario in cui il VPC è configurato con un blocco CIDR allocato manualmente, non con un blocco CIDR allocato automaticamente tramite IPAM.

Per creare un VPC

1. Utilizzando l'account amministratore IPAM, apri la console VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. Seleziona Crea VPC.
3. Inserisci un nome per il VPC, ad esempio tutorial-vpc.
4. Scegli l'immissione manuale IPv4 CIDR e inserisci un IPv4 blocco CIDR. In questo tutorial, utilizziamo 10.0.0.0/20.
5. Salta l'opzione per aggiungere un IPv6 blocco CIDR.
6. Seleziona Crea VPC.
7. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
8. Nel riquadro di navigazione a sinistra, scegli Resources (Risorse).

9. Attendi che appaia il VPC creato. Questa operazione richiede tempo e potrebbe essere necessario aggiornare la finestra per vederlo apparire. Per continuare con il passaggio successivo, il VPC deve essere rilevato da IPAM.

Passaggio 2: Creazione di un pool di pianificazione delle risorse

Completa i passaggi descritti in questa sezione per creare un pool di pianificazione delle risorse.

Creazione di un pool di pianificazione delle risorse

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato.
4. Scegli Crea pool.
5. Sotto la voce Ambito IPAM lascia selezionato l'ambito privato.
6. (Facoltativo) Aggiungi un tag Name per il pool, ad esempio «Resource-planning-pool».
7. In Source (Origine), scegli IPAM scope (Ambito IPAM).
8. In Resource planning (Pianificazione delle risorse), scegli Plan IP space within a VPC (Pianifica lo spazio IP in un VPC) e scegli il VPC che hai creato nel passaggio precedente. Il VPC è la risorsa utilizzata per il provisioning del pool CIDRs di pianificazione delle risorse.
9. In CIDRs to provisioning, scegli il VPC CIDR di cui effettuare il provisioning per il pool di risorse. Il CIDR di cui hai eseguito il provisioning al pool di pianificazione delle risorse deve corrispondere al CIDR di cui hai eseguito il provisioning al VPC. In questo tutorial, utilizziamo 10.0.0.0/20.
10. Scegli Crea pool.
11. Una volta creato il pool, scegli la scheda CIDR per vedere lo stato del CIDR di cui hai eseguito il provisioning. Aggiorna la pagina e attendi che lo stato CIDR cambi da Pending-provisioning (Provisioning in sospeso) a Provisioned (Provisioning eseguito) prima di procedere con il passaggio successivo.

Passaggio 3: Creazione di pool di sottoreti

Completa i passaggi descritti in questa sezione per creare due pool di sottoreti da utilizzare per allocare lo spazio IP alle sottoreti.

Creazione di pool di sottoreti

1. Utilizzando l'account di amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato.
4. Scegli Crea pool.
5. Sotto la voce Ambito IPAM lascia selezionato l'ambito privato.
6. (Facoltativo) Aggiungi un tag Name per il pool, ad esempio «»dev-subnet-pool.
7. In Source (Origine), scegli IPAM pool (Pool IPAM) e seleziona il pool di pianificazione delle risorse che hai creato nel passaggio 3. La famiglia di indirizzi, la configurazione della pianificazione delle risorse e la locale vengono ereditate automaticamente dal pool di origine.
8. Nella sezione CIDRs Da fornire, scegli il CIDR di cui effettuare il provisioning per il pool di sottoreti. In questo tutorial, utilizziamo 10.0.0.0/24.
9. Scegli Crea pool.
10. Una volta creato il pool, scegli la scheda CIDR per vedere lo stato del CIDR di cui hai eseguito il provisioning. Aggiorna la pagina e attendi che lo stato CIDR cambi da Pending-provisioning (Provisioning in sospeso) a Provisioned (Provisioning eseguito) prima di procedere con il passaggio successivo.
11. Ripeti questo processo per creare un'altra sottorete chiamata «». prod-subnet-pool

A questo punto, se si desidera rendere disponibile questo pool di sottoreti ad altri AWS account, è possibile condividere il pool di sottoreti. Per istruzioni su come eseguire questa operazione, consulta Condivisione di un pool IPAM tramite AWS RAM. Poi torna qui per completare il tutorial.

Passaggio 4: Creazione di sottoreti

Completa questi passaggi per creare due sottoreti.

Creazione di sottoreti

1. Utilizzando l'account appropriato, apri la console VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. Scegli Subnets (Sottoreti) > Create subnet (Crea sottorete).
3. Scegli il VPC che hai creato all'inizio di questo tutorial.

4. Inserisci un nome per la sottorete, ad esempio "tutorial-subnet".
5. (Facoltativo) Scegli un'Availability Zone (Zona di disponibilità).
6. In blocco IPv4 CIDR, scegli il blocco CIDR allocato da IPAM e scegli il pool di IPV4 sottoreti di sviluppo e una netmask /28.
7. Scegliere Create subnet (Crea sottorete).
8. Ripeti questo processo per creare un'altra sottorete. Questa volta scegli il pool di sottoreti di produzione e una maschera di rete /28.
9. Torna alla console IPAM e scegli Resources (Risorse) nel riquadro di navigazione a sinistra.
10. Cerca i pool di sottoreti che hai creato e attendi che le sottoreti che hai creato appaiano sotto. Questa operazione richiede tempo e potrebbe essere necessario aggiornare la finestra per vederle apparire.

Il tutorial è terminato. È possibile creare pool di sottoreti aggiuntivi in base alle esigenze oppure avviarli ad esempio in una delle sottoreti. EC2

IPAM pubblica le metriche relative all'utilizzo degli indirizzi IP nelle sottoreti. È possibile impostare CloudWatch allarmi sulla IPUsage metrica Subnet, in modo da intervenire in caso di violazione delle soglie di utilizzo IP. Se, ad esempio, avete un CIDR /24 (256 indirizzi IP) assegnato a una sottorete e desiderate ricevere una notifica quando l'80% di essi è stato utilizzato, potete impostare un allarme IPs per avvisarvi quando viene raggiunta questa soglia. CloudWatch Per ulteriori informazioni sulla creazione di un allarme di utilizzo degli IP di una sottorete, consulta Suggerimento rapido per la creazione di allarmi.

Fase 5: eliminazione

Completa questi passaggi per eliminare le risorse create con questo tutorial.

Come ripulire le risorse

1. Utilizzando l'account amministratore IPAM, apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli l'ambito privato.
4. Scegli il pool di pianificazione delle risorse, quindi scegli Action (Azione) > Delete (Elimina).

5. Seleziona Cascade delete (Elimina a cascata). Il pool di pianificazione delle risorse e i pool di sottoreti verranno eliminati. Ciò non eliminerà le sottoreti. Rimarranno quelli che gli sono CIDRs stati assegnati, anche se non provengono più da un pool IPAM. CIDRs
6. Scegli Elimina.
7. Elimina le sottoreti.
8. Elimina il VPC.

La pulizia è completa.

Assegna indirizzi IP elastici sequenziali da un pool IPAM

IPAM consente di fornire IPv4 blocchi pubblici di proprietà di Amazon ai pool IPAM e di allocare indirizzi IP elastici sequenziali da tali pool alle risorse. AWS

Gli indirizzi IP elastici allocati in modo contiguo sono indirizzi pubblici allocati in sequenza. IPv4 Ad esempio, se Amazon ti fornisce un blocco IPv4 CIDR pubblico di `192.0.2.0/30` e allochi i quattro IPv4 indirizzi pubblici disponibili da quel blocco CIDR, un esempio di quattro indirizzi IP elastici sequenziali è`192.0.2.0`,, `192.0.2.1` e. `192.0.2.2` `192.0.2.3`

Gli indirizzi IP elastici allocati in modo contiguo consentono di semplificare le regole di sicurezza e di rete nei seguenti modi:

- Amministrazione della sicurezza: l'utilizzo di IPv4 indirizzi sequenziali riduce il sovraccarico di gestione del firewall. È possibile aggiungere un intero prefisso con un'unica regola e associarlo IPs dallo stesso prefisso in base alla scalabilità, risparmiando tempo e fatica.
- Accesso aziendale: puoi semplificare lo spazio di indirizzi condiviso con i tuoi clienti utilizzando un intero blocco CIDR anziché un lungo elenco di singoli indirizzi pubblici. IPv4 In questo modo si evita di dover comunicare costantemente le modifiche all'IP man mano che l'applicazione scala su AWS.
- Gestione IP semplificata: l'utilizzo di IPv4 indirizzi sequenziali semplifica la gestione degli IP pubblici per il team di rete centrale, in quanto riduce la necessità di tenere traccia dei singoli utenti pubblici IPs e consente loro di concentrarsi invece su un numero limitato di prefissi IP.

In questa esercitazione verranno mostrati i passaggi necessari per assegnare indirizzi IP elastici sequenziali da un pool IPAM. Creerai un pool IPAM con un blocco IPv4 CIDR pubblico contiguo fornito da Amazon, allocerai indirizzi IP elastici dal pool e imparerai a monitorare le allocazioni dei pool IPAM.

Note

- Sono previsti costi associati al provisioning di blocchi CIDR pubblici IPv4 di proprietà di Amazon. Per ulteriori informazioni, consulta la scheda IPv4 Blocchi contigui fornita da Amazon nella pagina dei prezzi di Amazon VPC.
- In questa esercitazione si presuppone che tu voglia creare un IPAM utilizzando IPAM con un solo account. Se desideri condividere IPv4 blocchi pubblici contigui di proprietà di Amazon tra più account, prima e poi. Integrare IPAM con gli account di un'organizzazione AWS Condivisione di un pool IPAM tramite AWS RAM Se effettui l'integrazione con AWS Organizations, hai la possibilità di creare una policy di controllo del servizio per impedire il deprovisioning dei IPv4 blocchi contig assegnati al pool.
- Non è possibile trasferire indirizzi IP elastici sequenziali allocati da un pool IPAM ad altri account AWS . Invece, IPAM consente di condividere i pool IPAM tra AWS account integrando IPAM con AWS Organizations (come menzionato sopra).
- Esistono limiti al numero di blocchi IPv4 CIDR pubblici di proprietà di Amazon che puoi fornire e alla loro dimensione. Per ulteriori informazioni, consulta Quote per l'IPAM.

Indice

- Fase 1: creare un IPAM
- Passaggio 2: creazione di un pool IPAM e provisioning di un CIDR
- Passaggio 3: assegnazione di un indirizzo IP elastico dal pool
- Fase 4: Associare l'indirizzo IP elastico a un'istanza EC2
- Passaggio 5: tracciamento e monitoraggio dell'utilizzo del pool
- Rimozione

Fase 1: creare un IPAM

Completa i passaggi descritti in questa sezione per creare un IPAM.

AWS Management Console

Per creare un IPAM

1. Apri la console IPAM all'indirizzo. https://console.aws.amazon.com/ipam/

2. Nella console di AWS gestione, scegli la AWS regione in cui desideri creare l'IPAM. Crea l'IPAM nella tua Regione operativa principale.
3. Nella home page del servizio, scegli Crea IPAM.
4. Seleziona Consenti a IP Address Manager di Amazon VPC di replicare i dati dagli account sorgente verso l'account IPAM delegato. Se non si seleziona questa opzione, non sarà possibile creare un IPAM.
5. Scegli un IPAM tier (Livello IPAM). Per ulteriori informazioni sulle funzionalità disponibili in ogni livello e sui costi associati ai livelli, consulta la scheda IPAM nella pagina dei prezzi di Amazon VPC.
6. Alla voce Regioni operative, seleziona le Regioni AWS in cui questo IPAM è in grado di gestire e scovare le risorse. La AWS regione in cui si sta creando l'IPAM è selezionata come una delle regioni operative per impostazione predefinita. Ad esempio, se stai creando questo IPAM in AWS Regione `us-east-1` ma desideri creare successivamente pool IPAM regionali che lo CIDRs forniscano VPCs `us-west-2`, seleziona qui. `us-west-2` Se si dimentica una Regione operativa, sarà possibile ritornarvi in un secondo momento e modificare le impostazioni IPAM.

   > **Note**
   >
   > Se stai creando un IPAM nel livello gratuito, puoi selezionare più regioni operative per il tuo IPAM, ma l'unica funzionalità IPAM che sarà disponibile nelle regioni operative è Informazioni sugli IP pubblici. Non puoi utilizzare altre funzionalità nel livello gratuito, come BYOIP, nelle regioni operative dell'IPAM. Puoi utilizzarle solo nella regione di origine dell'IPAM. Per utilizzare tutte le funzionalità IPAM nelle regioni operative, crea un IPAM nel livello avanzato.

7. Scegli Create IPAM (Crea IPAM).

Command line

I comandi in questa sezione rimandano alla documentazione di riferimento della AWS CLI. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Crea l'IPAM con il comando create-ipam:

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

Risposta di esempio:

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

Ti serviranno PublicDefaultScopeId nel passaggio successivo. Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.

Passaggio 2: creazione di un pool IPAM e provisioning di un CIDR

Completa i passaggi in questa sezione per creare un pool IPAM da cui assegnare gli indirizzi IP elastici.

AWS Management Console

Per creare un pool

1. Apri la console IPAM all'indirizzo https://console.aws.amazon.com/ipam/.
2. Nel pannello di navigazione, seleziona Pool.

3. Scegli l'ambito Public (Pubblico). Per ulteriori informazioni sugli ambiti, consulta Funzionamento di IPAM.
4. Scegli Crea pool.
5. (Facoltativo) Aggiungi un Name tag (Tag nome) e una Description (Descrizione) per il pool.
6. In Source (Origine), scegli IPAM scope (Ambito IPAM).
7. In Famiglia di indirizzi, scegli IPv4.
8. In Resource planning (Pianificazione delle risorse), lascia selezionato Plan IP space within the scope (Pianifica spazio IP nell'ambito).
9. In Locale (Località), scegli la località per il pool. La lingua è la AWS regione in cui desideri che questo pool IPAM sia disponibile per le allocazioni. Le opzioni qui disponibili provengono dalle Regioni operative scelte al momento della creazione dell'IPAM.
10. In Servizio, scegli EC2 (EIP/VPC). Il servizio selezionato determina il servizio in cui verrà AWS pubblicizzato il CIDR. Attualmente, l'unica opzione è EC2 (EIP/VPC), il che significa che l' CIDRs allocazione da questo pool verrà pubblicizzata per il EC2 servizio Amazon (per gli indirizzi IP elastici).
11. In Origine IP pubblica, scegli Di proprietà di Amazon.
12. In CIDR da fornire, scegli Aggiungi CIDR pubblico di proprietà di Amazon. Scegli una lunghezza della maschera di rete compresa tra `/29` (8 indirizzi IP) e `/30` (4 indirizzi IP). Per impostazione predefinita, puoi aggiungerne fino a 2. CIDRs Per informazioni sull'aumento dei limiti per il pubblico contiguo fornito da Amazon, consulta. IPv4 CIDRs Quote per l'IPAM
13. Lascia le impostazioni delle regole di allocazione di "Configura questo pool" deselezionate.
14. (Facoltativo) Scegli Tag per il pool.
15. Scegli Crea pool.

Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare. Puoi vedere lo stato del provisioning nella CIDRsscheda della pagina dei dettagli del pool.

Command line

Per creare un pool

1. Crea un pool IPAM con il create-ipam-poolcomando. La località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. Le opzioni qui disponibili provengono dalle Regioni operative scelte al momento della creazione dell'IPAM.

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

Esempio di risposta con lo stato `create-in-progress`:

```
{

    "IpamPool": {

        "OwnerId": "320805250157",

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

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

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

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

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

        "PoolDepth": 1,

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

        "AutoImport": false,

        "AddressFamily": "ipv4",

        "Tags": [],

        "AwsService": "ec2",

        "PublicIpSource": "amazon"

    }
```

```
}
```

2. Verifica che il pool sia stato creato correttamente con il describe-ipam-poolscomando.

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

Esempio di risposta con lo stato `create-complete`:

```
{

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

3. Fornisci un CIDR al pool con il provision-ipam-pool-cidrcomando. Scegli una `--netmask-length` compresa tra `/29` (8 indirizzi IP) e `/30` (4 indirizzi IP). Per impostazione predefinita, puoi aggiungerne fino CIDRs a 2. Per informazioni sull'aumento dei limiti per il pubblico contiguo fornito da Amazon, consulta. IPv4 CIDRs Quote per l'IPAM

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

Esempio di risposta con lo stato `pending-provision`:

```
{

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

4. Assicurati che su questo CIDR sia stato effettuato il provisioning prima di continuare. È possibile visualizzare lo stato del provisioning utilizzando il comando. get-ipam-pool-cidrs

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

Esempio di risposta con lo stato `provisioned`:

```
{

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

Passaggio 3: assegnazione di un indirizzo IP elastico dal pool

Completa i passaggi in questa sezione per assegnare un indirizzo IP elastico dal pool.

AWS Management Console

Segui la procedura descritta in Allocare un indirizzo IP elastico nella Amazon EC2 User Guide per allocare l'indirizzo, ma tieni presente quanto segue:

- Assicurati che la AWS regione in cui ti trovi nella EC2 console corrisponda all'opzione Locale che hai scelto quando hai creato il pool nel passaggio 2.
- Quando scegli il pool di indirizzi, scegli l'opzione Allocazione utilizzando un pool IPv4 IPAM e scegli il pool che hai creato nel passaggio 1.

Command line

Assegna un indirizzo dal pool con il comando allocate-address. L'opzione `--region` che utilizzi deve corrispondere all'opzione `-locale` scelta al momento della creazione del pool nel passaggio 2. Includi l'ID del pool IPAM creato nel passaggio 2 in `--ipam-pool-id`.

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

Risposta di esempio:

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

Facoltativamente, puoi anche scegliere un `/32` specifico nel tuo pool IPAM utilizzando l'opzione `--address`.

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

Risposta di esempio:

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

Per ulteriori informazioni, consulta Allocate an Elastic IP address nella Amazon EC2 User Guide.

Fase 4: Associare l'indirizzo IP elastico a un'istanza EC2

Completa i passaggi di questa sezione per associare l'indirizzo IP elastico a un' EC2istanza.

AWS Management Console

Segui i passaggi in Associare un indirizzo IP elastico nella Amazon EC2 User Guide per allocare un indirizzo IP elastico dal pool IPAM, ma tieni presente quanto segue: Quando utilizzi l'opzione Console di AWS gestione, la AWS regione in cui associ l'indirizzo IP elastico deve corrispondere all'opzione Locale che hai scelto quando hai creato il pool nello Step 2.

Command line

Associa l'indirizzo IP elastico a un'istanza con il comando associate-address. La `--region` a cui associ l'indirizzo IP elastico deve corrispondere all'opzione `--locale` scelta al momento della creazione del pool nel passaggio 2.

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

Risposta di esempio:

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

Per ulteriori informazioni, consulta Associare un indirizzo IP elastico a un'istanza o a un'interfaccia di rete nella Amazon EC2 User Guide.

Passaggio 5: tracciamento e monitoraggio dell'utilizzo del pool

Dopo aver allocato gli indirizzi IP elastici dal pool IPAM, puoi tracciare e monitorare le allocazioni del pool IPAM.

AWS Management Console

- Visualizza i dettagli del pool IPAM nella scheda Allocazioni nella console IPAM. Tutti gli indirizzi IP elastici allocati dal pool IPAM hanno un tipo di risorsa di EIP.
- Usa Informazioni sugli IP pubblici:
  - In Tipi di IP pubblici, filtra per proprietà di Amazon EIPs. Questo mostra il numero totale di IPv4 indirizzi pubblici assegnati agli indirizzi IP elastici di proprietà di Amazon. Se filtri in base a questa misura e scorri fino a Indirizzi IP pubblici nella parte inferiore della pagina, vedrai gli indirizzi IP elastici che hai allocato.
  - In Utilizzo EIP, filtra per Proprietà associata di Amazon EIPs o Proprietà non associata di Amazon. EIPs Questo mostra il numero totale di indirizzi IP elastici che hai allocato nel tuo AWS account e che hai o non hai associato a un' EC2 istanza, interfaccia di rete o risorsa. AWS Se filtri in base a questa misura e scorri fino a Indirizzi IP pubblici nella parte inferiore della pagina, vedrai i dettagli sulle risorse filtrate.
  - In Uso IPv4 contiguo di proprietà di Amazon, monitora IPs l'utilizzo sequenziale degli IPv4 indirizzi pubblici nel tempo e i relativi pool IPAM di proprietà di Amazon. IPv4
- Usa Amazon CloudWatch per tracciare e monitorare le metriche relative ai IPv4 blocchi pubblici contigui forniti da Amazon che sono stati assegnati ai pool IPAM. Per le metriche disponibili specifiche per i blocchi contigui, consulta le metriche relative agli IP pubblici sotto IPv4 . Metriche IPAM Oltre a visualizzare le metriche, puoi creare allarmi in Amazon CloudWatch per avvisarti quando vengono raggiunte le soglie. La creazione di allarmi e l'impostazione di notifiche con Amazon CloudWatch non rientrano nell'ambito di questo tutorial. Per ulteriori informazioni, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

Command line

- Visualizza le allocazioni dei pool IPAM con il comando. get-ipam-pool-allocations Tutti gli indirizzi IP elastici allocati dal pool IPAM hanno un tipo di risorsa di eip.

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

Risposta di esempio:

```
{
```

```
     "IpamPoolAllocations": [
        {
            "Cidr": "18.97.0.40/32",
            "IpamPoolAllocationId": "ipam-pool-
alloc-0bd07df786e8148aba2763e2b6c1c44bd",
            "ResourceId": "eipalloc-0c9decaa541d89aa9",
            "ResourceType": "eip",
            "ResourceRegion": "us-east-1",
            "ResourceOwner": "320805250157"
        }
    ]
}
```

- Usa Amazon CloudWatch per tracciare e monitorare le metriche relative ai IPv4 blocchi pubblici contigui forniti da Amazon che sono stati assegnati ai pool IPAM. Per le metriche disponibili specifiche per i blocchi contigui, consulta le metriche relative agli IP pubblici sotto IPv4 . Metriche IPAM Oltre a visualizzare le metriche, puoi creare allarmi in Amazon CloudWatch per avvisarti quando vengono raggiunte le soglie. La creazione di allarmi e l'impostazione di notifiche con Amazon CloudWatch non rientrano nell'ambito di questo tutorial. Per ulteriori informazioni, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

L'esercitazione è ora completa. Hai creato un pool IPAM con un blocco IPv4 CIDR pubblico contiguo fornito da Amazon, hai allocato indirizzi IP elastici dal pool e hai imparato a monitorare le allocazioni dei pool IPAM. Continua con la sezione successiva per eliminare le risorse che hai creato in questa esercitazione.

Rimozione

Segui i passaggi in questa sezione per ripulire le risorse che hai creato in questa esercitazione.

Passaggio 1: annullamento dell'associazione dell'indirizzo IP elastico

Completa la procedura descritta in Dissociazione di un indirizzo IP elastico nella Amazon EC2 User Guide per dissociare l'indirizzo IP elastico.

Passaggio 2: rilascio dell'indirizzo IP elastico

Completa i passaggi in Release an Elastic IP address nella Amazon EC2 User Guide per rilasciare un indirizzo IP elastico dal IPv4 pool pubblico.

Passaggio 3: annullamento del provisioning del CIDR dal pool IPAM

Completa i passaggi in Deapprovvigionamento CIDRs da un pool per annullare il provisioning del CIDR pubblico di proprietà di Amazon dal pool IPAM. Questo passaggio è obbligatorio per l'eliminazione del pool. Ti verrà addebitato il costo del IPv4 blocco contiguo fornito da Amazon fino al completamento di questo passaggio.

Passaggio 4: eliminazione del pool IPAM

Completa i passaggi in Elimina un pool per eliminare il pool IPAM.

Passaggio 5: eliminazione dell'IPAM

Completa i passaggi in Elimina un IPAM per eliminare l'IPAM.

La pulizia dell'esercitazione è ora completa.

Identity and Access Management in IPAM

AWS utilizza credenziali di sicurezza per identificarti e concederti l'accesso alle tue AWS risorse. Puoi utilizzare le funzionalità di AWS Identity and Access Management (IAM) per consentire ad altri utenti, servizi e applicazioni di utilizzare le tue AWS risorse completamente o in modo limitato, senza condividere le tue credenziali di sicurezza.

Questa sezione descrive i ruoli AWS collegati ai servizi creati specificamente per IPAM e le politiche gestite associate ai ruoli collegati ai servizi IPAM. Per ulteriori informazioni sui ruoli e le policy IAM di AWS , consulta Termini e concetti dei ruoli nella Guida per l'utente di IAM.

Per ulteriori informazioni sulla gestione delle identità e degli accessi per VPC, consulta Gestione delle identità e degli accessi per Amazon VPC nella Amazon VPC User Guide.

Indice

- Ruoli collegati al servizio per IPAM
- AWS politiche gestite per IPAM
- Policy di esempio

Ruoli collegati al servizio per IPAM

IPAM utilizza ruoli AWS Identity and Access Management collegati ai servizi (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM. I ruoli collegati ai servizi sono predefiniti da IPAM e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione di IPAM perché non è necessario aggiungere manualmente le autorizzazioni necessarie. IPAM definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo IPAM può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Autorizzazioni del ruolo collegato ai servizi

IPAM utilizza il ruolo collegato al servizio AWSServiceRoleForIPAM per richiamare le azioni nella politica gestita allegata. AWSIPAMServiceRolePolicy Per ulteriori informazioni sulle operazioni consentite in tale policy, consulta AWS politiche gestite per IPAM.

Al ruolo collegato al servizio è inoltre associata una policy di fiducia IAM che consente al servizio di assumere il ruolo collegato al `ipam.amazonaws.com` servizio.

Creazione del ruolo collegato ai servizi

IPAM monitora l'utilizzo dell'indirizzo IP in uno o più account assumendo il ruolo collegato al servizio in un account, individuando le risorse e le relative risorse e integrando le risorse con IPAM. CIDRs

Il ruolo collegato al servizio viene creato in due modi:

- Quando si integra con AWS Organizations

  Se Integrare IPAM con gli account di un'organizzazione AWS utilizzi la console IPAM o utilizzi il `enable-ipam-organization-admin-account` AWS CLI comando, il ruolo collegato al servizio AWSServiceRoleForIPAM viene creato automaticamente in ciascuno degli account membro di Organizations AWS . Di conseguenza, le risorse all'interno di tutti gli account membri sono individuabili da IPAM.

  > **Important**
  >
  > Affinché IPAM crei per tuo conto il ruolo collegato al servizio:
  >
  > - All'account di gestione AWS Organizations che consente l'integrazione IPAM con AWS Organizations deve essere associata una policy IAM che consenta le seguenti azioni:
  >   - `ec2:EnableIpamOrganizationAdminAccount`
  >   - `organizations:EnableAwsServiceAccess`
  >   - `organizations:RegisterDelegatedAdministrator`
  >   - `iam:CreateServiceLinkedRole`
  > - L'account IPAM deve disporre di una policy IAM che consenta l'operazione `iam:CreateServiceLinkedRole`.

- Quando si crea un IPAM utilizzando un singolo account AWS

  Se sei tuUtilizza IPAM con un singolo account, il ruolo collegato al servizio AWSServiceRoleForIPAM viene creato automaticamente quando crei un IPAM come account.

> **Important**
>
> Se utilizzi IPAM con un singolo AWS account, prima di creare un IPAM, devi assicurarti che all' AWS account che stai utilizzando sia associata una policy IAM che consenta l'azione. `iam:CreateServiceLinkedRole` Quando crei l'IPAM, crei automaticamente il ruolo collegato al AWSService RoleFor servizio IPAM. Per ulteriori informazioni sulla gestione delle policy IAM, consulta Modifica della descrizione di un ruolo collegato ai servizi nella IAM User Guide.

Modifica del ruolo collegato ai servizi

Non è possibile modificare il ruolo collegato al servizio AWSServiceRoleForIPAM.

Eliminazione del ruolo collegato ai servizi

Se non è più necessario utilizzare IPAM, si consiglia di eliminare il ruolo collegato al AWSService RoleFor servizio IPAM.

> **Note**
>
> Puoi eliminare il ruolo collegato al servizio solo dopo aver eliminato tutte le risorse IPAM nell'account AWS . Questo impedisce di rimuovere involontariamente la capacità di monitoraggio dell'IPAM.

Segui questi passaggi per eliminare il ruolo collegato al servizio tramite la CLI AWS :

1. Elimina le tue risorse IPAM utilizzando and delete-ipam. deprovision-ipam-pool-cidr Per ulteriori informazioni, consulta Deapprovvigionamento CIDRs da un pool e Elimina un IPAM.
2. Disattiva l'account IPAM con -account. disable-ipam-organization-admin
3. Disabilita il servizio IPAM disable-aws-service-accessutilizzando l'opzione. `--service-principal ipam.amazonaws.com`
4. Elimina il ruolo collegato al servizio:. delete-service-linked-role Quando elimini il ruolo collegato al servizio, viene eliminata anche la policy gestita da IPAM. Per ulteriori informazioni, consultare Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

AWS politiche gestite per IPAM

Se utilizzi IPAM con un singolo AWS account e crei un IPAM, la policy AWSIPAMServiceRolePolicygestita viene creata automaticamente nel tuo account IAM e allegata al ruolo collegato al servizio AWSServiceRoleForIPAM.

Se abiliti l'integrazione IPAM con AWS Organizations, la policy AWSIPAMServiceRolePolicygestita viene creata automaticamente nel tuo account IAM e in ciascuno degli account membro di AWS Organizations, e la policy gestita viene allegata al ruolo collegato al servizio AWSServiceRoleForIPAM.

Questa policy gestita consente a IPAM di eseguire le operazioni seguenti:

- Monitora le risorse di rete CIDRs associate a tutti i membri della tua organizzazione. AWS
- Archivia le metriche relative all'IPAM in Amazon CloudWatch, come lo spazio degli indirizzi IP disponibile nei pool IPAM e il numero di risorse conformi alle regole di CIDRs allocazione.

L'esempio che segue mostra i dettagli relativi alle policy gestite create.

JSON

```
{
    "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",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsPublishActions",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

La prima dichiarazione dell'esempio precedente consente a IPAM di monitorare l' CIDRs utilizzo dal singolo AWS account o dai membri della propria organizzazione. AWS

La seconda istruzione dell'esempio precedente utilizza la chiave `cloudwatch:PutMetricData` condition per consentire a IPAM di archiviare i parametri IPAM nel tuo spazio dei nomi Amazon. `AWS/IPAM` CloudWatch Queste metriche vengono utilizzate da per visualizzare i dati sulle allocazioni nei AWS Management Console pool e negli ambiti IPAM. Per ulteriori informazioni, consulta Monitora l'utilizzo del CIDR con il pannello di controllo IPAM.

Aggiornamenti alla politica gestita AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per IPAM da quando questo servizio ha iniziato a tenere traccia di queste modifiche.

Modifica	Descrizione	Data
AWSIPAMServiceRolePolicy	Azioni aggiunte alla policy AWSIPAMSe rvice RolePolicy gestita (`organizations:List Children organizat ions:ListParents` , `eorganizations:Desc ribeOrganizational Unit`) per consentire a IPAM di ottenere i dettagli delle unità organizzative (OUs) nelle AWS organizzazioni in modo che i clienti possano utilizzare IPAM a livello di unità organizzativa.	21 novembre 2024
AWSIPAMServiceRolePolicy	Azione aggiunta alla policy AWSIPAMService RolePolic y gestita (`ec2:GetIp amDiscoveredPublic Addresses`) per consentir e a IPAM di ottenere indirizzi IP pubblici durante l'individ uazione delle risorse.	13 novembre 2023
AWSIPAMServiceRolePolicy	Azioni aggiunte alla politica AWSIPAMService RolePolic y gestita (`ec2:Descr ibeAccountAttribut es` ,,`ec2:Descr ibeNetworkInterfac es` ,, `ec2:Descr ibeSecurityGroups` `ec2:DescribeSecuri tyGroupRules`	1 novembre 2023

Modifica	Descrizione	Data
	`ec2:DescribeVpnConnections globalaccelerator:ListAccelerators` , `eglobalaccelerator:ListByoipCidrs`) per consentire a IPAM di ottenere indirizzi IP pubblici durante l'individuazione delle risorse.	
AWSIPAMServiceRolePolicy	Sono state aggiunte due azioni alla policy AWSIPAMService RolePolicy gestita (`ec2:GetIpamDiscoveredAccounts eec2:GetIpamDiscoveredResourceCidrs`) per consentire a IPAM di monitorare AWS gli account e le risorse durante l' CIDRs individuazione delle risorse.	25 gennaio 2023
IPAM ha iniziato a monitorare le modifiche	IPAM ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	2 dicembre 2021

Policy di esempio

La politica di esempio in questa sezione contiene tutte le azioni AWS Identity and Access Management (IAM) pertinenti per l'utilizzo completo dell'IPAM. In base all'utilizzo di IPAM, potrebbe non essere necessario effettuare tutte le operazioni IAM. Per un'esperienza completa con la console IPAM, potrebbe essere necessario includere azioni IAM aggiuntive per servizi come AWS Organizations, AWS Resource Access Manager(RAM) e Amazon CloudWatch.

JSON

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIpamByoasn",
                "ec2:DeprovisionIpamByoasn",
                "ec2:DescribeIpamByoasn",
                "ec2:DisassociateIpamByoasn",
                "ec2:ProvisionIpamByoasn",
                "ec2:CreateIpam",
                "ec2:DescribeIpams",
                "ec2:ModifyIpam",
                "ec2:DeleteIpam",
                "ec2:CreateIpamScope",
                "ec2:DescribeIpamScopes",
                "ec2:ModifyIpamScope",
                "ec2:DeleteIpamScope",
                "ec2:CreateIpamPool",
                "ec2:DescribeIpamPools",
                "ec2:ModifyIpamPool",
                "ec2:DeleteIpamPool",
                "ec2:ProvisionIpamPoolCidr",
                "ec2:GetIpamPoolCidrs",
                "ec2:DeprovisionIpamPoolCidr",
                "ec2:AllocateIpamPoolCidr",
                "ec2:GetIpamPoolAllocations",
                "ec2:ReleaseIpamPoolAllocation",
                "ec2:CreateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveries",
                "ec2:ModifyIpamResourceDiscovery",
                "ec2:DeleteIpamResourceDiscovery",
                "ec2:AssociateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveryAssociations",
                "ec2:DisassociateIpamResourceDiscovery",
                "ec2:GetIpamResourceCidrs",
                "ec2:ModifyIpamResourceCidr",
                "ec2:GetIpamAddressHistory",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetIpamDiscoveredAccounts",
```

```
                "ec2:GetIpamDiscoveredPublicAddresses"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ipam.amazonaws.com"
                }
            }
        }
    ]
}
```

Quote per l'IPAM

Questa sezione elenca le quote relative all'IPAM. La console Service Quotas fornisce inoltre le informazioni sulle quote di IPAM. È possibile utilizzare la console Service Quotas per visualizzare le quote di default e richiedere aumenti delle quote per le quote regolabili. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente di Service Quotas.

Nome	Predefinita	Adattabile
Blocchi CIDR pubblici contigui forniti da Amazon IPv4	2	Sì. Contatta il AWS Support Center come descritto nelle quote di AWS servizio nel Riferimenti generali di AWS.
Lunghezza della netmask del blocco CIDR pubblico IPv4 contiguo fornita da Amazon	/29	La dimension e accettabile è compresa tra /29 e /30. Per richiedere un aumento, contattar e il AWS Support Center come descritto nelle quote di AWS servizio nel Riferimen ti generali di AWS.
Lunghezza della netmask del blocco IPv6 CIDR fornita da Amazon	/52	Sì. Contatta il AWS Support Center come descritto nelle quote di AWS servizio nel Riferimenti generali di AWS.
Blocchi IPv6 CIDR forniti da Amazon per pool regionale	1	Sì. Contatta il AWS Support Center come descritto nelle quote

Nome	Predefinita	Adattabile
		di AWS servizio nel Riferimenti generali di AWS.
Numeri di sistema autonomi (ASNs) che puoi portare a IPAM	5	Sì. Contatta il AWS Support Center come descritto nelle quote di AWS servizio nel Riferimenti generali di AWS.
CIDRs per pool	50	Sì
Amministratori IPAM per organizzazione	1	No
IPAMs per regione	1	No
Esclusioni di unità organizzative per rilevamento di risorse	10	Sì. Contatta il AWS Support Center come descritto nelle quote di AWS servizio nel Riferimenti generali di AWS.
Profondità del pool (numero di pool all'interno dei pool)	10	Sì
Pool per ambito	50	Sì
Associazioni dei rilevamenti delle risorse per ogni IPAM	5	Sì
Rilevamenti delle risorse per ogni regione	1	No

Nome	Predefinita	Adattabile
Parametri di utilizzo delle risorse	50	Sì. Contatta il AWS Support Center come descritto nelle quote di AWS servizio nel Riferimenti generali di AWS.
Ambiti per IPAM	5	Sì. Quando crei un IPAM, vengono creati un ambito privato e un ambito pubblico predefiniti. Gli eventuali ambiti aggiuntivi che vuoi creare saranno privati. Non è possibile creare ambiti pubblici aggiuntivi.

Prezzi per IPAM

Amazon VPC IP Address Manager (IPAM) è un servizio che ti aiuta a gestire lo spazio degli indirizzi IP tra AWS le risorse e le reti locali. IPAM offre un modo centralizzato per pianificare, monitorare e controllare gli indirizzi IP utilizzati dalle tue risorse e da quelle locali. AWS

Questa sezione spiega come visualizzare le informazioni relative ai prezzi e i costi attuali dell'IPAM.

Indice

- Visualizza informazioni sui prezzi
- Visualizza i costi e l'utilizzo attuali utilizzando AWS Cost Explorer

Visualizza informazioni sui prezzi

IPAM è disponibile con due livelli: livello gratuito e livello avanzato. Per ulteriori informazioni sulle funzionalità disponibili in ogni livello e sui costi associati ai livelli, consulta la scheda IPAM nella pagina dei prezzi di Amazon VPC.

Visualizza i costi e l'utilizzo attuali utilizzando AWS Cost Explorer

Quando utilizzi IPAM livello avanzato, paghi un prezzo orario per indirizzo IP attivo gestito da IPAM. Se desideri visualizzare e analizzare i costi e l'utilizzo dell'IPAM, puoi utilizzare il AWS Cost Explorer.

1. Apri la AWS Cost Management console a https://console.aws.amazon.com/cost-management/casa.
2. Avvia Cost Explorer.
3. Filtra per utilizzo IPAM selezionando Tipo di utilizzo e inserendo **`IPAddressManager`**.
4. Seleziona una o più caselle di controllo. Ciascuno di essi rappresenta una AWS regione diversa.
5. Fare clic su Apply (Applica).

Se, ad esempio, selezioni USE1- IPAddress Manager-IP-Hours (Hrs) e us-east-1 è la tua regione di origine IPAM, vedrai il numero di ore IP attive fatturate da IPAM in tutte le regioni e il costo. Se, ad esempio, l'utilizzo è di 18 ore, potresti avere 1 indirizzo IP attivo per 18 ore, 3 indirizzi IP attivi ciascuno per 6 ore in 3 regioni diversi o qualsiasi combinazione di questi per un totale di 18 ore.

Per ulteriori informazioni in merito, consulta la sezione Analisi dei costi nella Guida per AWS Cost Explorer l'utente. AWS Cost ExplorerAWS Cost Management

Informazioni correlate

Sebbene il sito della documentazione AWS tecnica sia una risorsa completa, esistono molti altri luoghi in cui trovare informazioni sui AWS servizi. AWS blog, white paper, case study e forum della community possono fornire informazioni preziose, esempi reali e prospettive alternative oltre ai dettagli tecnici ufficiali. L'esplorazione di queste diverse fonti può darti una comprensione più completa delle offerte. AWS

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di Gestione indirizzi IP di Amazon VPC:

- Best practice di Amazon VPC IP Address Manager: un AWS blog sulle best practice per la pianificazione e la creazione di uno schema di indirizzi scalabile con Amazon VPC IP Address Manager.
- Gestione e controllo degli indirizzi di rete su larga scala con Amazon VPC IP Address Manager: AWS un blog che presenta Amazon VPC IP Address Manager e mostra come utilizzare il servizio nella console. AWS
- Configura l'accesso granulare alle risorse condivise utilizzando AWS Resource Access Manager: Un AWS blog che spiega come condividere un pool IPAM con gli account di un'unità organizzativa Organizations AWS .
- Visualizza la gestione e la pianificazione degli indirizzi IP aziendali con la mappa CIDR: un AWS blog che spiega come visualizzare l'intero IPv4 IPv6 ambiente utilizzando la mappa IPAM CIDR nella console IPAM.

Cronologia dei documenti per IPAM

La tabella seguente illustra le versioni di IPAM.

Funzionalità	Descrizione	Data di rilascio
Abilita la distribuzione dei costi	Quando si abilita la distribuzione dei costi, si distribuiscono gli addebiti per gli indirizzi IP attivi agli account che utilizzano gli indirizzi IP anziché al proprietario dell'IPAM. Ciò è utile per le grandi organizzazioni in cui l'amministratore IPAM delegato gestisce gli indirizzi IP a livello centrale utilizzando IPAM e ogni account è responsabile del proprio utilizzo, eliminando la necessità di calcoli di fatturazione manuali.	1 maggio 2025
Escludi unità organizzative da IPAM	Se il tuo IPAM è integrato con AWS Organizations, ora puoi escludere le unità organizzative da IPAM. IPAM non gestirà gli indirizzi IP negli account nelle unità organizzative escluse.	21 novembre 2024
AWS aggiornamenti gestiti delle politiche: aggiornamento a una politica esistente	AWSIPAMServiceRolePolicy Aggiornato esistente.	21 novembre 2024
Assegna indirizzi IP elastici sequenziali da un pool IPAM	IPAM ora consente di fornire IPv4 blocchi pubblici di proprietà di Amazon ai pool IPAM e di allocare indirizzi IP elastici sequenziali da tali pool alle risorse. AWS Gli indirizzi IP elastici sequenziali consentono di semplificare le esigenze di rete e sicurezza nell'elenco delle autorizzazioni.	28 agosto 2024
GUA privati e IPv6 ULAs	Ora puoi fornire intervalli IPv6 GUA e ULA privati a un pool IPAM in un ambito privato. IPv6 Gli indirizzi privati sono disponibili solo	8 agosto 2024

Funzionalità	Descrizione	Data di rilascio
	in IPAM. Per ulteriori informazioni sull' IPv6 indirizzamento privato, IPv6 consulta Indirizzi privati nella Amazon VPC User Guide.	
Livelli IPAM gratuiti e avanzati	Ora puoi scegliere tra il livello gratuito e il livello avanzato per il tuo IPAM.	17 novembre 2023
Public IP insights	In precedenza, potevi visualizzare informazi oni sugli IP pubblici in una singola regione. Ora puoi visualizzare Informazioni sugli IP pubblici in tutte le regioni. Inoltre, ora puoi visualizz are informazioni sugli indirizzi IP pubblici in Amazon CloudWatch.	17 novembre 2023
Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti	Ora puoi utilizzare IPAM per pianificare lo spazio IP della sottorete in un VPC e monitorar e le metriche correlate agli indirizzi IP a livello di sottorete e VPC.	17 novembre 2023
Bring your own ASN (BYOASN)	Ora puoi aggiungere il tuo numero di sistema autonomo (ASN) a AWS.	17 novembre 2023
AWS aggiornamenti gestiti delle politiche: aggiornamento a una politica esistente	AWSIPAMServiceRolePolicy Aggiornato esistente.	17 novembre 2023
AWS aggiornamenti gestiti delle politiche: aggiornamento a una politica esistente	AWSIPAMServiceRolePolicy Aggiornato esistente.	1 novembre 2023
Parametri di utilizzo delle risorse	IPAM ora pubblica su Amazon i parametri di utilizzo degli IP per le risorse monitorate dall'IPAM. CloudWatch	2 agosto 2023

Funzionalità	Descrizione	Data di rilascio
Public IP insights	Public IP Insights mostra tutti gli IPv4 indirizzi pubblici utilizzati dai servizi di questa regione nel tuo account. Puoi utilizzare queste informazioni per identificare l'utilizzo degli IPv4 indirizzi pubblici e visualizzare i consigli per rilasciare indirizzi IP elastici non utilizzati.	28 luglio 2023
AWS aggiornamenti delle politiche gestite: aggiornamento a una politica esistente	AWSIPAMServiceRolePolicy Aggiornato esistente.	25 gennaio 2023
Come integrare IPAM con account esterni alla tua organizzazione	Ora puoi gestire gli indirizzi IP all'esterno della tua organizzazione da un singolo account IPAM e condividere i pool IPAM con gli account di altre Organizzazioni AWS .	25 gennaio 2023
Blocco CIDR IPv6 contiguo fornito da Amazon per pool IPAM	Quando crei un pool IPAM nell'ambito pubblico, ora puoi fornire al pool un blocco CIDR IPv6 contiguo fornito da Amazon. Per ulteriori informazioni, consulta Crea pool di IPv6 indirizzi nel tuo IPAM.	25 gennaio 2023
Rilascio iniziale	Questa versione introduce IP Address Manager di Amazon VPC.	2 dicembre 2021

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.