



IP Address Manager

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: IP Address Manager

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

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 autorizzazioni per il tuo IPAM	5
Integrare IPAM con gli account di un'organizzazione AWS	5
Come integrare IPAM con account esterni alla tua organizzazione	8
Utilizza IPAM con un singolo account	11
Crea un IPAM	11
Pianificare il provisioning degli indirizzi IP	14
Esempio di piani di pool IPAM	15
Come creare pool IPv4	17
Come creare pool IPv6	27
Assegnare i CIDR	34
Creare un VPC che utilizza un CIDR del pool IPAM	35
Assegna manualmente un CIDR a un pool per riservare lo spazio degli indirizzi IP	35
Gestione dello spazio degli indirizzi IP in IPAM	37
Applicazione dell'uso di IPAM per la creazione di VPC	37
Applica IPAM durante la creazione di VPC	38
Applicare un pool IPAM durante la creazione di VPC	38
Applica IPAM per tutte le unità organizzative, tranne un determinato elenco di esse	39
Condividi un pool IPAM utilizzando AWS RAM	40
Effettua il provisioning di CIDR a un pool	43
Revoca del provisioning di CIDR da un pool	44
Modifica di un pool	45
Elimina un pool	46
Come rilevare le risorse	47
Come creare un rilevamento delle risorse	48
Come visualizzare i dettagli del rilevamento delle risorse	50
Come condividere un rilevamento delle risorse	52
Come associare un rilevamento delle risorse a un IPAM	54
Come annullare l'associazione di un rilevamento delle risorse	55
Come eliminare un rilevamento delle risorse	56
Crea ambiti aggiuntivi	57

Spostamento dei CIDR del VPC tra ambiti	58
Modifica dello stato di monitoraggio dei CIDR VPC	59
Elimina un ambito	61
Rilasciare un'assegnazione	62
Modifica un IPAM	64
Modifica un livello IPAM	64
Modifica le regioni operative IPAM	65
Elimina un IPAM	66
Monitoraggio dell'utilizzo dell'indirizzo IP in IPAM	69
Monitora l'utilizzo del CIDR con il pannello di controllo IPAM	69
Monitoraggio dell'utilizzo del CIDR per risorsa	72
Monitoraggio IPAM con Amazon CloudWatch	76
Pool e parametri ambito IPAM	76
Parametri di utilizzo delle risorse	78
Visualizzazione della cronologia degli indirizzi IP	83
Visualizzazione di informazioni dettagliate relative agli indirizzi IP pubblici	87
Tutorial	92
Creazione di IPAM e pool utilizzando la console	92
Prerequisiti	93
In che modo AWS Organizations si integra con IPAM	93
Fase 1: delega di un amministratore IPAM	94
Passaggio 2: creazione di un IPAM	96
Passaggio 3: creazione di un pool IPAM di livello superiore	98
Fase 4: creazione di pool IPAM regionali	103
Fase 5: creazione di un pool di sviluppo di pre-produzione	107
Fase 6: condivisione del pool IPAM	111
Fase 7: creazione di un VPC con un CIDR assegnato da un pool IPAM	116
Fase 8: eliminazione	120
Creazione di IPAM e pool utilizzando la AWS CLI	122
Passaggio 1: abilitare IPAM nella tua organizzazione	123
Passaggio 2: creare un IPAM	123
Passaggio 3: creazione di un pool di indirizzi IPv4	125
Passaggio 4: effettuare il provisioning di un CIDR al pool di livello superiore	127
Fase 5: Crea un pool Regionale con CIDR proveniente dal pool di livello superiore	128
Passaggio 6: effettuare il provisioning di un CIDR al pool Regionale	130
Fase 7. Creare una condivisione RAM per abilitare le assegnazioni IP tra gli account	132

Fase 8. Crea un VPC	133
Fase 9. Pulizia	133
Visualizzazione della cronologia degli indirizzi IP utilizzando la AWS CLI	134
Panoramica	134
Scenari	135
Porta il tuo ASN in IPAM	143
Prerequisiti di onboarding per l'ASN	144
Passaggi del tutorial	145
Trasferisci i tuoi indirizzi IP su IPAM	149
AWS CLI e console	150
Solo AWS CLI	176
Trasferimento di un CIDR BYOIP IPv4 in IPAM	219
Fase 1: creazione di profili denominati della AWS CLI e ruoli IAM	220
Passaggio 2: ottenimento dell'ID di ambito pubblico dell'IPAM	221
Passaggio 3: creazione di un pool IPAM	221
Passaggio 4: condivisione del pool IPAM utilizzando la AWS RAM	223
Passaggio 5: trasferimento di un CIDR BYOIP IPv4 esistente su IPAM	226
Passaggio 6: visualizzazione del CIDR in IPAM	228
Passaggio 7: pulizia	229
Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti	232
Fase 1. Creazione di un VPC	234
Passaggio 2: Creazione di un pool di pianificazione delle risorse	235
Passaggio 3: Creazione di pool di sottoreti	235
Passaggio 4: Creazione di sottoreti	236
Fase 5: eliminazione	237
Identity and Access Management in IPAM	239
Ruoli collegati al servizio per IPAM	239
Autorizzazioni concesse al ruolo collegato al servizio	239
Creazione del ruolo collegato ai servizi	240
Modifica del ruolo collegato ai servizi	241
Eliminazione del ruolo collegato ai servizi	241
Policy gestite per IPAM	241
Aggiornamenti sulla policy gestita da AWS	243
Policy di esempio	245
Quote	247
Prezzi	249

Visualizza informazioni sui prezzi	249
Visualizza i costi e l'utilizzo correnti utilizzando AWS Cost Explorer	249
Informazioni correlate	250
Cronologia dei documenti	251
.....	ccliii

Che cos'è IPAM?

Amazon VPC IP Address Manager (IPAM) è una caratteristica del VPC che semplifica la pianificazione, il tracciamento 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
- Assegnare automaticamente i CIDR ai VPC utilizzando regole aziendali specifiche
- Risolvere i problemi di connettività
- Abilita la condivisione tra regioni e tra account degli indirizzi Porta il tuo indirizzo IP (BYOIP)
- Come eseguire il provisioning di blocchi CIDR IPv6 contigui forniti da Amazon sui pool per la creazione di VPC

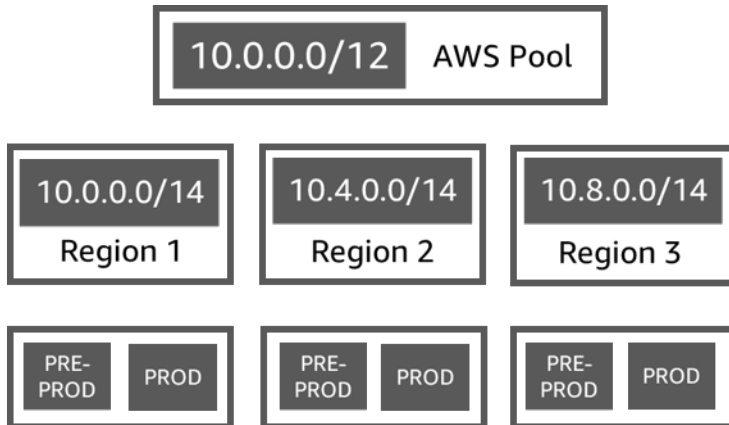
Questa guida contiene le sezioni seguenti:

- [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, crea un IPAM e pianifica l'utilizzo dell'indirizzo 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](#): tutorial dettagliati per creare un IPAM e i rispettivi pool, allocare un CIDR VPC e portare i CIDR di indirizzo IP pubblico su IPAM.

Funzionamento di IPAM

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

Il seguente diagramma mostra una gerarchia del pool IPAM per più Regioni AWS all'interno di un pool IPAM di livello superiore. Ogni pool Regionale di AWS ha due pool di sviluppo IPAM al suo interno, un pool per la pre-produzione e uno per la produzione di risorse. 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 si crea l'IPAM, bisogna scegliere in quale Regione AWS crearlo. Quando si crea un IPAM, l'IPAM di AWS VPC 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. Un IPAM contiene due ambiti di default. 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. All'interno di un ambito, si creano pool IPAM.
- Un pool è una raccolta di intervalli di indirizzi IP contigui (o CIDR). 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, è possibile assegnare i CIDR 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 è in grado di gestire e monitorare CIDR IPv4 privati, CIDR IPv4/IPv6 pubblici di tua proprietà e spazio IPv6 pubblico di proprietà di Amazon.

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. Inizierai accedendo a IPAM e decidendo se vuoi 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.

Indice

- [Accedi a IPAM](#)
- [Configura le autorizzazioni per il tuo IPAM](#)
- [Crea un IPAM](#)
- [Pianificare il provisioning degli indirizzi IP](#)
- [Assegnare i CIDR](#)

Accedi a IPAM

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

- Console di gestione AWS: fornisce un'interfaccia web da utilizzare per creare e gestire il tuo IPAM. Consulta <https://console.aws.amazon.com/ipam/>.
- Interfaccia a riga di comando AWS (CLI di AWS): Offre comandi per un'ampia gamma di servizi AWS, incluso Amazon VPC. CLI di AWS è supportata su Windows, macOS e Linux. Per ottenere la CLI di AWS, consulta [AWS Command Line Interface](#).
- SDK di AWS: fornisce API specifiche per le lingue. Gli SDK di AWS gestiscono molti dei dettagli della connessione, ad esempio il calcolo delle firme, la gestione dei nuovi tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta [SDK di AWS](#).
- 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 operazioni IPAM di Amazon, nella [Documentazione di riferimento delle API di Amazon EC2](#).

Questa guida si concentra principalmente sull'utilizzo della Console di gestione AWS per creare, accedere e gestire il tuo IPAM. In ogni descrizione su come completare un processo nella console

sono inclusi i link alla documentazione della CLI di AWS che illustra come fare la stessa cosa utilizzando la CLI di AWS.

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 autorizzazioni per il tuo IPAM](#).

Configura le autorizzazioni per il tuo IPAM

Prima di iniziare a utilizzare IPAM, è necessario scegliere una delle opzioni in questa sezione per consentire a IPAM di monitorare i CIDR associati alle risorse di rete EC2 e archiviare i parametri:

- Per abilitare l'integrazione di un IPAM con AWS Organizations per consentire al servizio IPAM di Amazon VPC di gestire e monitorare le risorse di rete create da tutti gli account membri delle organizzazioni AWS, 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 usare un singolo account AWS 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 i CIDR dai pool IPAM condivisi utilizzando Resource Access Manager (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 i CIDR utilizzati dai VPC esistenti negli account membri di altre AWS Organizations.

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

Important

- 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.

Note

Durante l'integrazione con AWS Organizations:

- 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 essere un account membro di AWS Organizations. Non è possibile utilizzare l'account di gestione di AWS Organizations come account IPAM.
- 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 `AWSServiceRoleForIPAM` servizio.
- 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/](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. Seleziona Salvataggio delle 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 dell'indirizzo IP in questi account assumendo il ruolo IAM collegato al servizio in ciascun account membro, individuando le risorse e i relativi CIDR e integrandoli con IPAM. 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. Puoi visualizzare questi dati prima della condivisione utilizzando i comandi CLI [get-ipam-discovered-resource-cidrs](#) e [get-ipam-discovered-accounts](#) oppure le API [GetIpamDiscoveredResourceCidrs](#) e [GetIpamDiscoveredAccounts](#).. 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 account AWS di un servizio di terzi che crea risorse per diversi suoi clienti, tali risorse verranno rilevate durante il rilevamento delle risorse. Se l'account AWS di un servizio di terzi condivide il rilevamento delle risorse con un account AWS utente finale, l'utente finale potrà visualizzare le risorse degli altri clienti del servizio AWS di terzi. Per tale motivo, il servizio AWS di terzi parti deve prestare attenzione nella creazione e nella condivisione di rilevamenti delle risorse o deve utilizzare un account AWS separato per ogni cliente.

Panoramica del processo

Questa sezione spiega come integrare il tuo IPAM con account AWS esterni alla tua 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 in modo da poter tornare a questa pagina per ottenere assistenza.

Quando integri un IPAM con account AWS esterni alla tua organizzazione, gli account AWS coinvolti nel processo sono quattro:

- Proprietario dell'organizzazione primaria: l'account di gestione AWS Organizations per l'organizzazione 1.
- Account IPAM dell'organizzazione primaria: l'account amministratore delegato IPAM per l'organizzazione 1.
- Proprietario dell'organizzazione secondaria: l'account di gestione AWS Organizations per l'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 dell'organizzazione secondaria crea un rilevamento delle risorse e lo condivide con l'account IPAM dell'organizzazione primaria tramite AWS RAM (consulta [Come creare un rilevamento delle risorse](#) e [Come condividere un rilevamento delle risorse](#)). Il rilevamento delle risorse deve essere creato nella stessa regione di origine dell'IPAM dell'organizzazione primaria.
5. L'account IPAM dell'organizzazione primaria accetta l'invito alla condivisione delle risorse tramite AWS RAM (consulta [Accettazione e rifiuto di inviti alla condivisione di risorse](#) nella Guida per l'utente di AWS RAM).
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 [Condividi un pool IPAM utilizzando 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 si sceglie di non selezionare [Integrare IPAM con gli account di un'organizzazione AWS](#), è possibile utilizzare IPAM da un solo account AWS.

Quando crei un IPAM nella sezione successiva, viene creato automaticamente un ruolo collegato ai servizi per il servizio IPAM di Amazon VPC in AWS Identity and Access Management. IPAM utilizza il ruolo collegato al servizio per monitorare e archiviare le metriche per i CIDR associati alle risorse di rete 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 account AWS, è necessario assicurarsi che l'account AWS utilizzato per creare l'IPAM utilizzi un ruolo IAM con una policy collegata che consenta di effettuare l'operazione `iam:CreateServiceLinkedRole`. Quando si crea l'IPAM, si crea automaticamente il ruolo collegato di servizio `AWSServiceRoleForIPAM`. Per maggiori informazioni sulla gestione di policy IAM, consultare [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Una volta che il singolo account AWS ha il permesso di creare il ruolo collegato al servizio IPAM, visitare [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, è necessaria l'autorizzazione per replicare i dettagli di utilizzo delle risorse e dell'IP tra gli account (dagli account membri all'account membro IPAM delegato) e tra tutte le Regioni AWS (dalle Regioni operative alla Regione di origine del tuo 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 crei l'IPAM, scegli le Regioni AWS in cui l'IPAM è autorizzato a gestire i CIDR degli indirizzi IP. Queste Regioni AWS sono chiamate Regioni operative. IPAM rileva e monitora le risorse solo nelle Regioni AWS selezionate come Regioni operative. IPAM non archivia dati al di fuori delle Regioni operative selezionate.

La gerarchia di esempio seguente mostra come le Regioni AWS assegnate al momento della creazione dell'IPAM influiranno sulle Regioni disponibili per i pool creati in un secondo momento.

- IPAM operativo nella Regione AWS 1 e nella Regione AWS 2
 - 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 gestione AWS, scegliere la Regione AWS in cui si desidera 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 Regione AWS in cui si sta creando l'IPAM è selezionata come una delle Regioni operative per impostazione di predefinita. Ad esempio, se si sta creando questo IPAM nella Regione AWS us-east-1 ma si desidera creare successivamente pool IPAM Regionali che forniscano CIDR ai VPC nella Regione us-west-2, selezionare 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti comandi AWS CLI per creare, modificare e visualizzare i dettagli relativi all'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 scegliendo IPAM nel pannello di navigazione sinistro 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.

Important

Per utilizzare i pool IPAM negli account AWS, è necessario integrare IPAM con AWS Organizations o alcune funzioni 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 CIDR). I pool IPAM consentono di organizzare gli indirizzi IP in base alle esigenze di routing e sicurezza. È possibile creare pool per Regioni AWS esterne alla tua 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 operante nella Regione AWS 1 e nella Regione AWS 2
 - Ambito privato
 - Pool di livello superiore
 - Pool IPAM Regionale nella Regione AWS 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 [Come creare un pool di livello superiore IPv4](#), quindi passa a [Assegnare i CIDR](#).

Indice

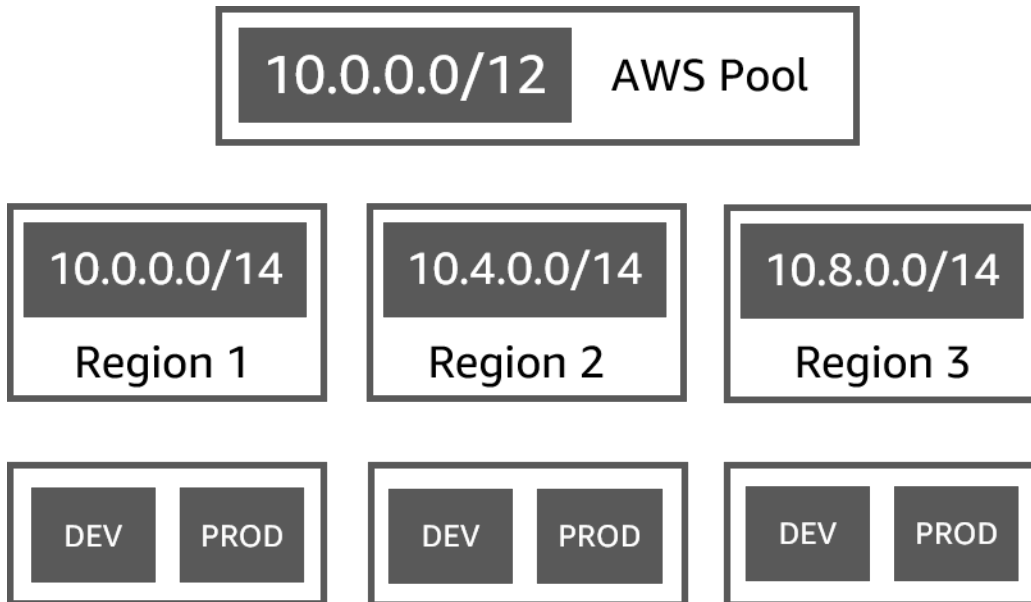
- [Esempio di piani di pool IPAM](#)
- [Come creare pool IPv4](#)
- [Come creare pool IPv6](#)

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.

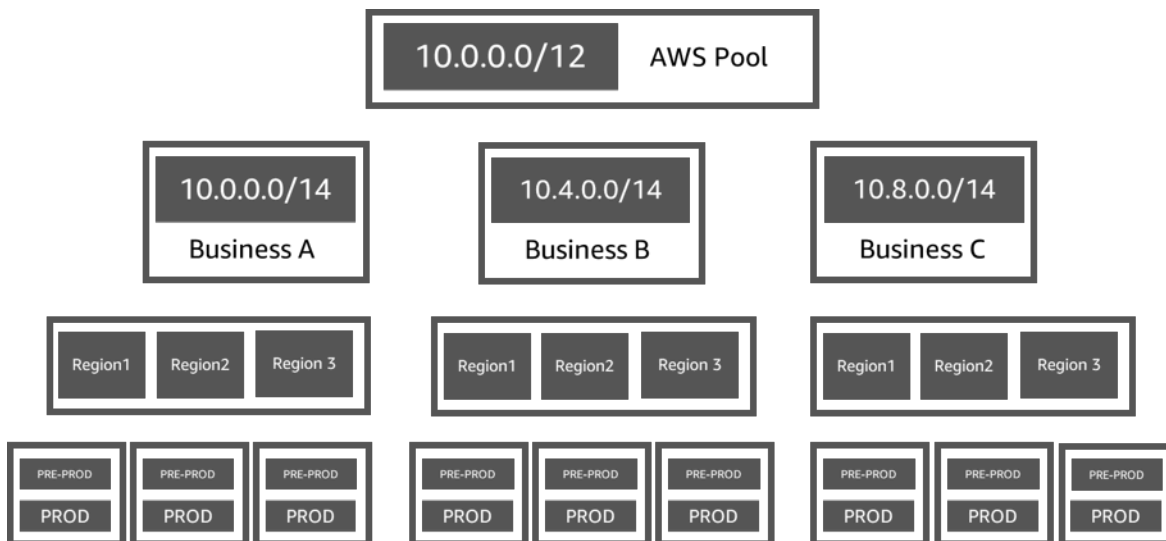
Pool IPv4 in più regioni AWS

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



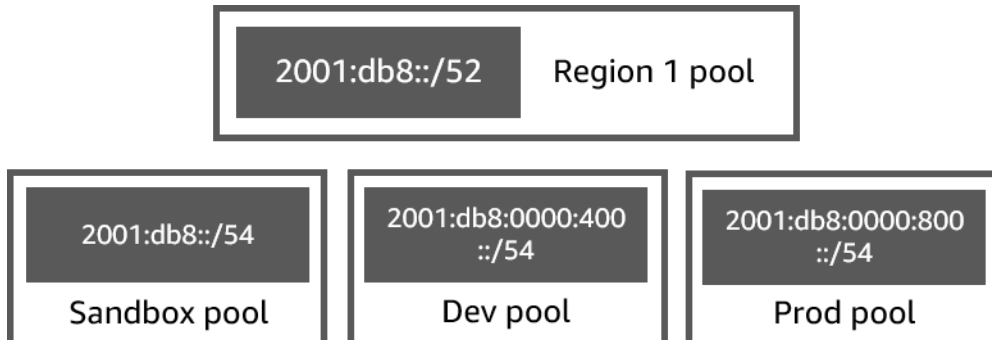
Pool Ipv4 per più linee di business

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 ciascuna linea di business contiene tre pool Regionali di AWS. 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.



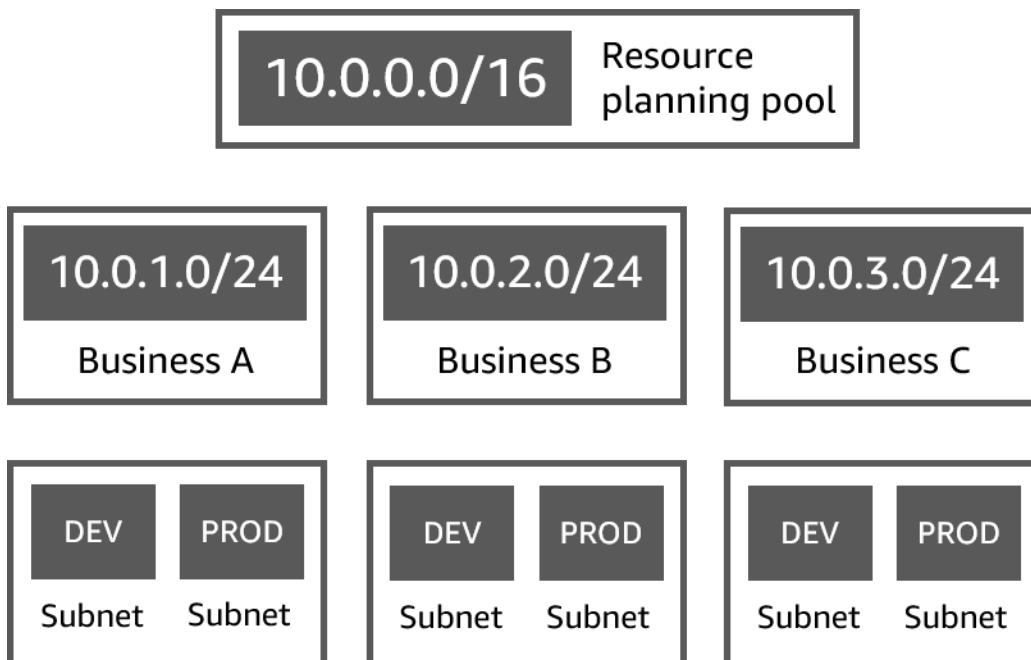
Pool IPv6 in una regione AWS

L'esempio seguente mostra una gerarchia di pool IPv6 IPAM per più linee di business in 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](#).



Come creare pool IPv4

Per creare una gerarchia di pool IPAM IPv4, segui i passaggi riportati in questa sezione.

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

- IPAM operante nella Regione AWS 1 e nella Regione AWS 2
 - Ambito privato
 - Pool di livello superiore (10.0.0.0/8)
 - Pool regionale nella regione AWS 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, i CIDR utilizzati sono solo a scopo esemplificativo. Essi mostrano che ogni pool all'interno del pool di alto livello è dotato di una parte del CIDR di alto livello.

Indice

- [Come creare un pool di livello superiore IPv4](#)
- [Come creare un pool IPv4 regionale](#)
- [Come creare un pool IPv4 di sviluppo](#)

Come creare un pool di livello superiore IPv4

Segui la procedura riportata in questa sezione per creare un pool IPAM di livello superiore IPv4. 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 operante nella Regione AWS 1 e nella Regione AWS 2
 - Ambito privato
 - Pool di livello superiore (10.0.0.0/8)
 - Pool regionale nella regione AWS 1 (10.0.0.0/16)
 - Pool di sviluppo di VPC non di produzione (10.0.0.0/24)
 - Allocazione per un VPC (10.0.0.0/25)

Nell'esempio precedente, i CIDR utilizzati sono solo a scopo esemplificativo. Essi mostrano che ogni pool all'interno del pool di livello superiore è dotato di una parte del CIDR di livello superiore.

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 debba importare automaticamente i CIDR nel pool IPAM qualora li trovi 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 località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni.

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 principal in AWS RAM. Per ulteriori informazioni sulla condivisione di pool con RAM, consulta [Condividi un pool IPAM utilizzando 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 assegnazione indicante che solo i VPC con il tag prod possono ottenere i CIDR da un pool IPAM. È inoltre possibile impostare una regola indicante che i CIDR allocati da

questo pool non possono essere superiori a /24. In questo caso una risorsa potrebbe ancora essere creata utilizzando un CIDR superiore a /24 da questo pool se lo spazio è disponibile, ma poiché ciò viola una regola di assegnazione sul pool, IPAM contrassegna questa risorsa come non conforme.

Important

Questo argomento spiega come creare un pool IPv4 di livello superiore con un intervallo di indirizzi IP fornito da AWS. Per includere un intervallo di indirizzi IPv4 personalizzato in AWS (BYOIP), sono previsti alcuni prerequisiti. Per ulteriori informazioni, consulta [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#).

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 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 pool IPv4. I pool nell'ambito pubblico possono essere pool IPv4 o IPv6. 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 Address family (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 località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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. Inserisci un CIDR IPv4 per il eseguire il provisioning per il pool. Per includere un intervallo di indirizzi IP IPv4 o IPv6 personalizzato in AWS, sono previsti alcuni 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 rilevante: 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:
 - I CIDR che saranno assegnati per queste risorse non devono già essere assegnati 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 rileva più CIDR che si sovrappongono, IPAM importerà solo il CIDR più grande.
 - Se IPAM rileva più CIDR con CIDR corrispondenti, 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 della netmask possibili per gli indirizzi IPv4 vanno da 0 a 32. Le lunghezze della netmask possibili per gli indirizzi IPv6 vanno da 0 a 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.
- **Località:** la località necessaria alle risorse che utilizzano i CIDR di 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. Scegli Crea pool.

14. Per informazioni, consultare [Come creare un pool IPv4 regionale](#).

Command line

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

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

1. Crea un pool: [create-ipam-pool](#).

2. Modifica il pool dopo averlo creato per modificare le regole di assegnazione: [modify-ipam-pool](#).

Come creare un pool IPv4 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 [Assegnare i CIDR](#).

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 operante nella Regione AWS 1 e nella Regione AWS 2
 - Ambito privato
 - Pool di livello superiore (10.0.0.0/8)
 - Pool regionale nella regione AWS 1 (10.0.0.0/16)
 - Pool di sviluppo di VPC non di produzione (10.0.0.0/24)
 - Allocazione per un VPC (10.0.0.0/25)

Nell'esempio precedente, i CIDR utilizzati sono solo a scopo esemplificativo. 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. 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 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. 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.

La località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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](#).

9. (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. È possibile aggiungere i CIDR a un pool in qualsiasi momento modificando il pool.
10. Qui hai a disposizione le stesse opzioni delle regole di assegnazione rispetto a quando hai creato il pool Regionale di alto livello. Consulta [Come creare un pool di livello superiore 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.
11. (Facoltativo) Scegli Tag per il pool.
12. Quando hai finito di configurare il pool, scegli Crea pool.
13. Per informazioni, consultare [Come creare un pool IPv4 di sviluppo](#).

Command line

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

Utilizza i seguenti comandi AWS CLI per creare un pool Regionale nel tuo IPAM:

1. Ottieni l'ID dell'ambito in cui vuoi 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.

Come creare un pool IPv4 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 [Assegnare i CIDR](#).

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 operante nella Regione AWS 1 e nella Regione AWS 2
 - Ambito privato
 - Pool di livello superiore (10.0.0.0/8)
 - Pool regionale nella regione AWS 1 (10.0.0.0/16)
 - Pool di sviluppo di VPC non di produzione (10.0.0.0/24)
 - Allocazione di un VPC (10.0.1.0/25)

Nell'esempio precedente, i CIDR utilizzati sono solo a scopo esemplificativo. 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 di sviluppo all'interno di un pool 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 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 i CIDR 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 [Come creare un pool di livello superiore 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, consultare [Assegnare i CIDR](#).

Command line

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

Utilizza i seguenti comandi AWS CLI per creare un pool Regionale nel tuo IPAM:

1. Ottieni l'ID dell'ambito in cui vuoi 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.

Come creare pool IPv6

Per creare una gerarchia di pool IPAM IPv6, segui i passaggi riportati in questa sezione. 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.

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

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

Indice

- [Come creare un pool regionale IPv6](#)
- [Come creare un pool IPv6 di sviluppo](#)

Come creare un pool regionale IPv6

Segui al procedura riportata in questa sezione per creare un pool IPAM regionale IPv6. Quando esegui il provisioning di un blocco CIDR IPv6 fornito da Amazon in un pool, il provisioning deve essere eseguito in un pool con locale (regione AWS) 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. Con questo passaggio viene creato un pool IPAM regionale IPv6:

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

Nell'esempio precedente, i CIDR utilizzati sono solo a scopo esemplificativo. I CIDR mostrano che il provisioning di ogni pool nel pool regionale IPv6 è stato eseguito con una parte del CIDR regionale IPv6.

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. La località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni.

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 principal in AWS RAM. Per ulteriori informazioni sulla condivisione di pool con RAM, consulta [Condividi un pool IPAM utilizzando 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 assegnazione indicante che solo i VPC con il tag prod possono ottenere i CIDR da un pool IPAM.

Important

Questo argomento descrive la creazione di un pool regionale IPv6 con un intervallo di indirizzi IP fornito da AWS. Per includere intervalli di indirizzi IP IPv4 o IPv6 personalizzati in AWS (BYOIP), sono previsti alcuni prerequisiti. Per ulteriori informazioni, consulta [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#).

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. 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 pool IPv4. I pool di ambito pubblico possono essere pool IPv4 o IPv6. L'ambito pubblico è destinato a tutto lo spazio che può essere o è attualmente pubblicizzato da AWS su Internet.

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. Viene visualizzata l'opzione di attivazione/disattivazione Consenti la divulgazione pubblica dei CIDR in questo pool. Per impostazione

predefinita, tutti i CIDR in questo pool saranno divulgabili pubblicamente. Non puoi abilitare o disabilitare questa opzione.

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. Quando esegui il provisioning di un blocco CIDR IPv6 fornito da Amazon in un pool, devi eseguire il provisioning in un pool con una locale (regione AWS) 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 località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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. In Service (Servizio), scegli EC2 (EIP/VPC). Il servizio selezionato determina il servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione possibile è EC2 (EIP/VPC), il che significa che i CIDR allocati da questo pool saranno pubblicizzabili per il servizio Amazon EC2 (per gli indirizzi IP elastici) e per il servizio Amazon VPC (per i CIDR associati ai VPC).
11. Per l'opzione Origine IP pubblico, scegli Di proprietà di Amazon affinché AWS fornisca un intervallo di indirizzi IPv6 per questo pool. Come indicato nella parte superiore di questa pagina, questo argomento spiega come creare un pool regionale IPv6 con un intervallo di indirizzi IP fornito da AWS. Per includere un intervallo di indirizzi IPv4 o IPv6 personalizzato in AWS (BYOIP), sono previsti alcuni prerequisiti. Per ulteriori informazioni, consulta [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#).

12. Per i pool nell'ambito pubblico che utilizzano BYOIP come origine IP pubblico, puoi verificare se AWS è in grado di divulgare pubblicamente i CIDR tramite Consenti la divulgazione pubblica dei CIDR in questo pool. Per impostazione predefinita, questa opzione è abilitata. Disattiva questa opzione se non desideri consentire la divulgazione pubblica dei CIDR in questo pool da parte di AWS.
13. (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, scegli Aggiungi CIDR di proprietà di Amazon e scegli la dimensione della maschera di rete del CIDR tra /40 e /52.

 Note

Tieni presente quanto segue:

- Per impostazione predefinita, puoi aggiungere un blocco CIDR IPv6 fornito da Amazon al pool regionale. Per informazioni sull'incremento del limite predefinito, consulta [Quote per l'IPAM](#).
- Quando scegli la lunghezza di una maschera di rete nel menu a discesa, viene visualizzata la lunghezza della maschera di rete e il numero dei /56 CIDR rappresentati dalla maschera di rete.

14. 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 della netmask possibili per gli indirizzi IPv6 vanno da 0 a 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 qui inserisci /56, la lunghezza minima della maschera di rete che può essere allocata per i CIDR da questo pool è /56.

- 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.
- Località: la località necessaria alle risorse che utilizzano i CIDR di 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.

15. (Facoltativo) Scegli Tag per il pool.

16. Scegli Crea pool.

17. Per informazioni, consultare [Come creare un pool IPv6 di sviluppo](#).

Command line

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

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

1. Crea un pool: [create-ipam-pool](#).
2. Modifica il pool dopo averlo creato per modificare le regole di assegnazione: [modify-ipam-pool](#).

Come creare un pool IPv6 di sviluppo

Segui la procedura riportata in questa sezione per creare un pool di sviluppo nel tuo pool regionale IPv6. Se hai bisogno solo di un pool regionale e non ti occorre di pool di sviluppo, passa a [Assegnare i CIDR](#).

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 operante nella Regione AWS 1 e nella Regione AWS 2
 - Ambito pubblico

- Pool regionale nella regione AWS 1 (2001:db8::/52)
 - Pool di sviluppo (2001:db8::/54)
 - Allocazione per un VPC (2001:db8::/56)

Nell'esempio precedente, i CIDR utilizzati sono solo a scopo esemplificativo. 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

Come creare un pool di sviluppo in un pool regionale IPv6

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. 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 pool IPv4. I pool di ambito pubblico possono essere pool IPv4 o IPv6. L'ambito pubblico è destinato a tutto lo spazio che può essere o è attualmente pubblicizzato da AWS su Internet.

5. (Facoltativo) Aggiungi un Tag nome e una descrizione per il pool.
6. In Source (Origine), scegli IPAM pool (Pool IPAM). Quindi sotto la voce Pool di origine scegli il pool regionale IPv6.
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 i CIDR a un pool in qualsiasi momento modificando il pool.
9. Sono disponibili le stesse opzioni delle regole di assegnazione che erano disponibili quando hai creato il pool regionale IPv6. Consulta [Come creare un pool regionale IPv6](#) 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, consultare [Assegnare i CIDR](#).

Command line

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

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

1. Ottieni l'ID dell'ambito in cui vuoi 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 questa procedura per creare pool di sviluppo aggiuntivi nel pool regionale IPv6, se necessario.

Assegnare i CIDR

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 assegnare i CIDR da un pool IPAM nei modi seguenti:

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

Questa sezione illustra entrambe le opzioni: come utilizzare i servizi AWS integrati con IPAM per effettuare il provisioning di un CIDR del pool IPAM e come riservare 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

Segui la procedura descritta in [Creazione di un VPC](#) nella Guida per l'utente di Amazon VPC. Quando raggiungi la fase di scelta di un CIDR per il VPC, avrai la possibilità di utilizzare un CIDR da un pool IPAM.

Se scegli l'opzione di utilizzare un pool IPAM quando crei il VPC, AWS assegnerà 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 CLI di AWS, 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 gestisce la prenotazione per conto dell'utente e indica se i CIDR si sovrappongono allo spazio IP On-Premise.

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 10.0.0.0/24 per IPv4 o 2001:db8::/52 per IPv6) oppure aggiungi un CIDR in base alla dimensione scegliendo solo la lunghezza della maschera di rete (ad esempio /24 per IPv4 o /52 per IPv6).
7. Selezionare 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti comandi AWS CLI per assegnare manualmente un CIDR a un pool:

1. Ottieni l'ID del pool IPAM in cui desideri creare l'assegnazione su: [describe-ipam-pool](#).
2. Crea l'assegnazione: [allocate-ipam-pool-cidr](#).
3. Visualizza l'assegnazione: [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. 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

- [Applicazione dell'uso di IPAM per la creazione di VPC](#)
- [Condividi un pool IPAM utilizzando AWS RAM](#)
- [Effettua il provisioning di CIDR a un pool](#)
- [Revoca del provisioning di CIDR da un pool](#)
- [Modifica di un pool](#)
- [Elimina un pool](#)
- [Come rilevare le risorse](#)
- [Crea ambiti aggiuntivi](#)
- [Spostamento dei CIDR del VPC tra ambiti](#)
- [Modifica dello stato di monitoraggio dei CIDR VPC](#)
- [Elimina un ambito](#)
- [Rilasciare un'assegnazione](#)
- [Modifica un IPAM](#)
- [Elimina un IPAM](#)

Applicazione dell'uso di IPAM per la creazione di VPC

Note

Questa sezione è applicabile solo se hai abilitato l'integrazione di IPAM con AWS Organizations. Per ulteriori informazioni, consulta [Integrare IPAM con gli account di un'organizzazione AWS](#).

Questa sezione descrive come creare una policy di controllo del servizio in AWS Organizations che richiede ai membri dell'organizzazione di utilizzare IPAM quando creano un VPC. Le policy di

controllo dei servizi (SCP) sono un tipo di policy dell'organizzazione che consentono di gestire le autorizzazioni nell'organizzazione. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.

Applica IPAM durante la creazione di VPC

Segui i passaggi riportati in questa sezione per richiedere ai membri dell'organizzazione di utilizzare IPAM durante la creazione di VPC.

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

1. Segui la procedura riportata in [Creazione di una SCP](#) nella Guida per l'utente di AWS Organizations e immetti il testo seguente nell'editor JSON:

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

2. Allega la policy a una o più unità organizzative della tua organizzazione. Per ulteriori informazioni, consulta [Collegamento e scollegamento delle policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.

Applicare un pool IPAM durante la creazione di VPC

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

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

1. Segui la procedura riportata in [Creazione di una SCP](#) nella Guida per l'utente di AWS Organizations e immetti il testo seguente nell'editor JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": ["ec2:CreateVpc", "ec2:AssociateVpcCidrBlock"],
    "Resource": "arn:aws:ec2:*:*:vpc/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:Ipv4IpamPoolId": "ipam-pool-0123456789abcdefg"
      }
    }
  }]
}
```

2. Modifica il valore di esempio `ipam-pool-0123456789abcdefg` per l'ID del pool IPv4 di cui desideri limitare gli utenti.
3. Allega la policy a una o più unità organizzative della tua organizzazione. Per ulteriori informazioni, consulta [Collegamento e scollegamento delle policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.

Applica IPAM per tutte le unità organizzative, tranne un determinato elenco di esse

Segui i passaggi in questa sezione per applicare IPAM per tutte le unità organizzative (OU), tranne un determinato elenco di esse. La policy descritta in questa sezione richiede che le unità organizzative nell'organizzazione, ad eccezione delle unità organizzative specificate in `aws:PrincipalOrgPaths`, utilizzino IPAM per creare ed espandere i VPC. Le unità organizzative elencate possono utilizzare IPAM durante la creazione di VPC o specificare manualmente un intervallo di indirizzi IP.

Per creare un SCP e applicare IPAM per tutte le unità organizzative, tranne un determinato elenco di esse

1. Segui la procedura riportata in [Creazione di una SCP](#) nella Guida per l'utente di AWS Organizations e immetti il testo seguente nell'editor JSON:

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

```

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

```

2. Rimuovi i valori di esempio (come o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/) e aggiungi i percorsi delle entità AWS Organizations delle unità organizzative per le quali desideri avere l'opzione (ma non richiedere) di utilizzare IPAM. Per ulteriori informazioni sul percorso dell'entità, consulta [Comprendere il percorso dell'entità AWS Organizations](#) e [aws:PrincipalOrgPaths](#) nella Guida per l'utente AWS Identity and Access Management.
3. Collega la policy alla root dell'organizzazione. Per ulteriori informazioni, consulta [Collegamento e scollegamento delle policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.

Condividi un pool IPAM utilizzando AWS RAM

Segui la procedura descritta in questa sezione per condividere un pool IPAM utilizzando AWS Resource Access Manager (RAM). Quando condividi un pool IPAM con RAM, i "principal" possono assegnare CIDR dal pool a risorse AWS, come ad esempio i VPC, dai rispettivi account. Un principale è un concetto nella RAM che indica qualsiasi account AWS, ruolo IAM o unità organizzativa in AWS Organizations. Per ulteriori informazioni, consulta [Condividere risorse AWS](#) nella Guida per l'utente di AWS RAM.

Note

- È possibile condividere un pool IPAM solo con AWS RAM se hai integrato IPAM con AWS Organizations. Per ulteriori informazioni, consulta [Integrare IPAM con gli account di un'organizzazione AWS](#). Non è possibile condividere un pool IPAM con AWS RAM se sei un utente IPAM ad account singolo.
- È necessario abilitare la condivisione di risorse con AWS Organizations in AWS RAM. Per ulteriori informazioni, consulta [Abilitazione della condivisione delle risorse con AWS Organizations](#) nella Guida per l'utente di AWS RAM.
- La condivisione RAM è disponibile solo nella Regione AWS di origine dell'IPAM. È necessario creare la condivisione nella Regione AWS 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.

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 aprirà la console AWS RAM. Creerai il pool condiviso in 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. Seleziona Successivo.
10. Scegli una delle autorizzazioni per la condivisione di risorse:
 - `AWSRAMDefaultPermissionsIpamPool`: scegli questa autorizzazione per consentire ai principal di visualizzare i CIDR e le assegnazioni nel pool IPAM condiviso e assegnare/ rilasciare i CIDR nel pool.
 - `AWSRAMPermissionIpamPoolByoipCidrImport`: scegli questa autorizzazione per consentire ai principal di importare i CIDR BYOIP nel pool IPAM condiviso. Questa autorizzazione è necessaria solo se si dispone di CIDR BYOIP esistenti e si desidera importarli in IPAM e condividerli con i principal. Per ulteriori informazioni sui CIDR BYOIP su IPAM, consulta [Tutorial: Trasferimento di un CIDR BYOIP IPv4 in IPAM](#).
11. Scegli i principal a cui è consentito accedere a questa risorsa. Se i principal importeranno CIDR BYOIP esistenti 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. Qui troverai descrizioni dettagliate delle opzioni che puoi usare quando esegui i comandi.

Utilizza i seguenti comandi AWS CLI per condividere un pool IPAM utilizzando RAM:

1. Ottieni l'ARN dell'IPAM: [describe-ipam-pools](#)
2. Crea la condivisione di risorse: [create-resource-share](#)
3. Visualizza la condivisione di risorse: [get-resource-share](#)

Come risultato della creazione della condivisione di risorse in RAM, altri principal possono ora assegnare CIDR alle 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 assegnare un CIDR da un pool IPAM condiviso, consulta [Creare un VPC](#) nella Guida per l'utente di Amazon VPC.

Effettua il provisioning di CIDR a un pool

Per effettuare il provisioning di CIDR a un pool, segui la procedura descritta in questa sezione. Se hai già eseguito il provisioning di un CIDR quando hai creato il pool, potrebbe essere necessario effettuare il provisioning di CIDR aggiuntivi se un pool si avvicina all'assegnazione 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 CIDR a un pool

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, scegliere il pool a cui si desidera aggiungere un CIDR.
5. Scegli Operazioni > Effettua il provisioning di CIDR.
6. Inserire il CIDR che si desidera aggiungere, quindi scegliere Aggiungi nuovo CIDR per CIDR aggiuntivi.

Note

- Per impostazione predefinita, puoi aggiungere un blocco CIDR IPv6 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 si esegue il provisioning di CIDR a un pool all'interno di un pool, lo spazio CIDR di cui si desidera eseguire il provisioning deve essere disponibile nel pool.

7. Scegli Richiedi provisioning.
8. È possibile visualizzare il CIDR in IPAM selezionando Pool nel pannello di navigazione, scegliendo un pool e visualizzando la scheda CIDR per il pool.

Command line

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

Utilizza i seguenti comandi AWS CLI per effettuare il provisioning dei CIDR a un pool:

1. Ottieni un ID del pool IPAM: [describe-ipam-pools](#)
2. Ottieni i CIDR che vengono sottoposti a provisioning al pool: [get-ipam-pool-cidrs](#)
3. Effettua il provisioning di un nuovo CIDR al pool: [provision-ipam-pool-cidr](#)
4. Ottieni i CIDR che vengono sottoposti a provisioning al pool e visualizza il nuovo CIDR: [get-ipam-pool-cidrs](#)

Revoca del provisioning di CIDR da un pool

Per revocare i CIDR di un pool IPAM, segui i passaggi descritti in questa sezione. Quando si revocano tutti i CIDR del pool, il pool non può più essere utilizzato per le assegnazioni. È necessario innanzitutto effettuare il provisioning di un nuovo CIDR nel pool prima di poter utilizzare il pool per le assegnazioni.

Important

Non è possibile revocare il CIDR se sono presenti assegnazioni nel pool. Per rimuovere le assegnazioni, consulta [Rilasciare un'assegnazione](#).

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, scegli il pool di cui si desidera revocare i CIDR.
5. Scegli la scheda CIDR.
6. Seleziona uno o più CIDR e scegli Revoca CIDR.
7. Scegli Revoca CIDR.

Command line

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

Utilizza i seguenti comandi AWS CLI per revocare un CIDR del pool:

1. Ottieni un ID del pool IPAM: [describe-ipam-pools](#)
2. Visualizza i CIDR attuali per il pool: [get-ipam-pool-cidrs](#)
3. Revoca i CIDR: [deprovision-ipam-pool-cidr](#)
4. Visualizza i CIDR aggiornati: [get-ipam-pool-cidrs](#)

Per effettuare il provisioning di un nuovo CIDR nel pool, consulta [Revoca del provisioning di CIDR da un pool](#). Se desideri eliminare il pool, consulta [Elimina un pool](#).

Modifica di un pool

Per modificare un pool IPAM, segui i passaggi riportati in questa sezione. È possibile modificare un pool per cambiare le regole di assegnazione nel pool. Per ulteriori informazioni sulle regole di assegnazione, consulta [Come creare un pool di livello superiore IPv4](#).

AWS Management Console

Per modificare un pool

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, 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 [Come creare un pool di livello superiore IPv4](#).
7. Scegli Update (Aggiorna).

Command line

Utilizza i seguenti comandi AWS CLI per modificare un pool:

1. Ottieni un ID del pool IPAM: [describe-ipam-pools](#)
2. Modifica il pool: [modify-ipam-pool](#)

Elimina un pool

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

Important

Non è possibile eliminare un pool di indirizzi IP se vi sono assegnazioni. È necessario rilasciare le assegnazioni e [Revoca del provisioning di CIDR da un pool](#) prima di poter eliminare il pool.

AWS Management Console

Per eliminare un 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, 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti comandi AWS CLI per eliminare un pool:

1. Visualizza i pool e ottieni un ID pool IPAM: [describe-ipam-pools](#)
2. Elimina un pool: [delete-ipam-pool](#)
3. Visualizza i pool: [describe-ipam-pools](#)

Per creare un nuovo pool, consulta [Come creare un pool di livello superiore IPv4](#).

Come rilevare le risorse

Un rilevamento delle risorse è un componente IPAM che consente a IPAM di gestire e monitorare le risorse appartenenti all'account proprietario. 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.

Indice

- [Come creare un rilevamento delle risorse](#)
- [Come visualizzare i dettagli del rilevamento delle risorse](#)
- [Come condividere un rilevamento delle risorse](#)
- [Come associare un rilevamento delle risorse a un IPAM](#)
- [Come annullare l'associazione di un rilevamento delle risorse](#)
- [Come eliminare un rilevamento delle risorse](#)

Come creare un rilevamento delle risorse

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 assegni a una risorsa AWS. Ciascun tag è formato da una chiave e da un valore opzionale. È possibile utilizzare i tag per cercare e filtrare le risorse o monitorare i costi AWS.
6. (Opzionale) Aggiungi una descrizione.
7. In Regioni operative, seleziona le regioni AWS in cui verranno rilevate 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. Seleziona Crea.

Command line

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

- Come crea un rilevamento delle risorse: [create-ipam-resource-discovery](#)

Come visualizzare i dettagli del rilevamento delle risorse

Questa sezione spiega come visualizzare i dettagli per un rilevamento delle risorse. Sono inclusi stati del rilevamento e CIDR delle risorse degli account monitorati durante il rilevamento delle risorse.

AWS Management Console

Come visualizzare i dettagli del 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 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 monitora i CIDR dai seguenti tipi di risorse VPC, pool IPv4 pubblici, sottoreti VPC e indirizzi IP elastici.
 - Nome (ID risorsa): ID del rilevamento delle risorse.
 - Utilizzo IP: 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 risorse costituite da VPC, questa è la percentuale di spazio degli indirizzi IP nel VPC che è stata occupata dai CIDR di sottorete.
 - Per le risorse che sono sottoreti, se alla sottorete è stato assegnato un CIDR IPv4, si tratta della percentuale di spazio di indirizzi IPv4 nella sottorete in uso. Se alla sottorete è stato eseguito il provisioning di un CIDR IPv6, la percentuale di spazio di indirizzi IPv6 in uso non è rappresentata. Al momento non è possibile calcolare la percentuale di spazio degli indirizzi IPv6 in uso.
 - Per risorse costituite da pool IPv4 pubblici, questa è la percentuale di spazio degli indirizzi IP nel pool che è stata allocata a indirizzi IP elastici (EIP).
 - 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 rilevati: account AWS monitorati con un rilevamento delle risorse. Se hai integrato un IPAM con organizzazioni AWS, verranno rilevati tutti gli account nell'organizzazione.
- ID account: ID dell'account.
- Regione: la regione AWS da cui vengono restituite 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 assegna a una risorsa AWS. 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Come visualizzare i dettagli del rilevamento delle risorse: [describe-ipam-resource-discovery](#)

Come condividere un rilevamento delle risorse

Segui la procedura riportata in questa sezione per condividere un rilevamento delle risorse tramite AWS Resource Access Manager. Per ulteriori informazioni sulla AWS RAM, consulta [Condivisione delle risorse AWS](#) nella Guida dell'utente di AWS RAM.

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.

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 crei una condivisione di risorse tramite AWS RAM per condividere un rilevamento delle risorse, devi creare la condivisione di risorse nella regione di origine dell'organizzazione IPAM 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 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. Apri 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. Selezionare Create resource share (Crea condivisione di risorse). Si apre la console AWS RAM in cui creerai la condivisione di risorse.
5. Nella console AWS RAM, seleziona Settings (Impostazioni).
6. Scegli Abilita condivisione conAWS 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. Seleziona 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. Seleziona 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. 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 di risorse: [get-resource-share](#)

Come associare un rilevamento delle risorse a un IPAM

Questa sezione spiega come associare un rilevamento delle risorse a un IPAM. Quando associ un rilevamento delle risorse a un IPAM, l'IPAM monitora tutti i CIDR delle risorse e gli account rilevati con il rilevamento 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. Apri la console IPAM all'indirizzo <https://console.aws.amazon.com/ipam/>.
2. Nel pannello di navigazione, scegli IPAM.

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

- Come associare un rilevamento delle 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 annulli l'associazione di rilevamento delle risorse a un IPAM, l'IPAM non monitora più tutti i CIDR delle risorse e gli account rilevati con il rilevamento 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. Apri la console IPAM all'indirizzo <https://console.aws.amazon.com/ipam/>.
2. Nel pannello di navigazione, scegli IPAM.
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. Seleziona Annulla associazione.

Command line

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

- Come annullare l'associazione di un rilevamento delle risorse: [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. Apri 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

- Come eliminare un rilevamento delle risorse: [delete-ipam-resource-discovery](#)

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 con CIDR IPv4 privati, i CIDR della risorsa vengono importati nell'ambito privato di default e non verranno visualizzati negli ambiti privati aggiuntivi creati. È possibile spostare i CIDR dall'ambito privato di default a un altro ambito privato. Per informazioni, consultare [Spostamento dei CIDR del VPC tra 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 CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

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

1. Visualizza gli ambiti correnti: [describe-ipam-scope](#)
2. Crea un nuovo ambito privato: [create-ipam-scope](#)
3. Visualizza gli ambiti attuali per visualizzare il nuovo ambito: [describe-ipam-scope](#)

Spostamento dei CIDR del VPC tra ambiti

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

Important

- Puoi spostare solo i CIDR dei VPC. Quando si sposta un CIDR VPC, anche i CIDR della sottorete del VPC vengono spostati automaticamente.
- È possibile spostare i CIDR VPC solo da un ambito privato a un altro. Non è possibile spostare i CIDR VPC da un ambito pubblico a un ambito privato o da un ambito privato a un ambito pubblico.
- Lo stesso account AWS 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. Alla voce VPC CIDRs (CIDR VPC), seleziona uno dei CIDR assegnati alla risorsa e scegli Actions (Operazioni) > Move CIDR to different scope (Sposta il CIDR su 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

Per spostare un CIDR VPC, usa i seguenti comandi della AWS CLI:

1. Ottieni un CIDR VPC nell'ambito corrente: [get-ipam-pool-cidrs](#)
2. Sposta un CIDR VPC: [modify-ipam-resource-cidr](#)
3. Ottieni un CIDR VPC nell'altro ambito: [get-ipam-pool-cidrs](#)

Modifica dello stato di monitoraggio dei CIDR VPC

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 è possibile ignorare i CIDR VPC 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 CIDR VPC è stato rilevato da IPAM e viene monitorato per la sovrapposizione con altri CIDR e conformità alle regole di allocazione.
- Ignorato: il CIDR VPC è stato scelto per non essere incluso nel monitoraggio. I CIDR VPC ignorati non vengono valutati per la sovrapposizione con altri CIDR o per 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. Alla voce CIDR VPC, seleziona uno dei CIDR assegnati al VPC, quindi scegli Operazioni > Contrassegna come ignorato o Non contrassegnare come ignorato.
6. Scegli Contrassegna come ignorato o Non contrassegnare come ignorato.

Command line

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

1. Ottieni un ID dell'ambito: [describe-ipam-scopes](#)
2. Visualizza lo stato di monitoraggio corrente per il CIDR VPC: [get-ipam-resource-cidrs](#)

3. Modifica lo stato del CIDR della risorsa: [modify-ipam-resource-cidr](#)
4. Visualizza il nuovo stato di monitoraggio per il CIDR VPC: [get-ipam-resource-cidrs](#)

Elimina un ambito

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

Important

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

Utilizza i seguenti comandi AWS CLI per eliminare un ambito:

1. Visualizza gli ambiti: [describe-ipam-scopes](#)

2. Elimina 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](#).

Rilasciare un'assegnazione

Per rilasciare un'assegnazione CIDR da un pool IPAM, seguire la procedura descritta in questa sezione. Un'assegnazione è un incarico CIDR da un pool IPAM a un'altra risorsa o pool IPAM.

Se si prevede di eliminare un pool, potrebbe essere necessario rilasciare un'assegnazione del pool. Non è possibile eliminare i pool se quest'ultimi hanno eseguito il provisioning dei CIDR e non è possibile annullare il provisioning dei CIDR se questi sono assegnati alle risorse.

Note

- Per rilasciare un'allocazione manuale, utilizzare la procedura descritta in questa sezione o chiamare [ReleaseIpamPoolAllocation API](#).
- Per rilasciare un'allocazione in un ambito privato, è necessario ignorare o eliminare il CIDR della risorsa. Per ulteriori informazioni, consulta [Modifica dello stato di monitoraggio dei CIDR VPC](#). 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 è possibile ignorare i CIDR delle risorse pubbliche. Per ulteriori informazioni, consultare Cleanup in [Portare un CIDR IPv4 pubblico su IPAM usando solo la AWS CLI](#) o Cleanup in [Portare un CIDR IPv6 su IPAM usando solo la AWS CLI](#). 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. Sono necessari alcuni minuti perché il CIDR diventi disponibile per le allocazioni 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: un'allocazione pubblica di pool IPv4.
7. Scegli Actions (Operazioni) > Release custom allocation (Rilascia allocazione personalizzata).
8. Scegli De-assegna CIDR.

Command line

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

Utilizza i seguenti comandi AWS CLI per rilasciare un'assegnazione del pool:

1. Ottieni un ID del pool IPAM: [describe-ipam-pools](#)
2. Visualizza l'assegnazione corrente nel pool: [get-ipam-pool-allocations](#)
3. Rilasciare un'assegnazione: [release-ipam-pool-allocation](#)
4. Visualizza le assegnazioni aggiornate: [get-ipam-pool-allocations](#)

Per aggiungere una nuova assegnazione, consulta [Assegnare i CIDR](#). Per eliminare il pool dopo aver rilasciato le assegnazioni, è necessario innanzitutto eseguire [Revoca del provisioning di CIDR da un pool](#).

Modifica un IPAM

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

Indice

- [Modifica un livello IPAM](#)
- [Modifica le regioni operative IPAM](#)

Modifica un livello IPAM

Per modificare un livello IPAM, segui i passaggi riportati in questa sezione. IPAM offre due livelli: livello gratuito e livello avanzato. 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](#).

Important

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. Apri la console IPAM all'indirizzo <https://console.aws.amazon.com/ipam/>.
2. Nel pannello di navigazione, scegli IPAM.
3. Nel riquadro dei contenuti, seleziona il tuo IPAM.
4. Scegli Operazioni > Modifica.
5. Scegli il livello IPAM da utilizzare per l'IPAM.
6. Seleziona Salva modifiche.

Command line

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

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

1. Visualizza gli IPAM correnti: [describe-ipams](#)
2. Modifica il livello IPAM: [modify-ipam](#)
3. Visualizza gli IPAM aggiornati: [describe-ipams](#)

Modifica le regioni operative IPAM

Per modificare le regioni operative IPAM, segui i passaggi riportati in questa sezione. Le Regioni operative sono Regioni AWS in cui l'IPAM è autorizzato a gestire i CIDR degli indirizzi IP. IPAM rileva e monitora le risorse solo le Regioni AWS selezionate come Regioni operative.

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 IPAM.
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. Seleziona Salva modifiche.

Command line

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

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

1. Visualizza gli IPAM correnti: [describe-ipams](#)
2. Aggiungere o rimuovere regioni operative IPAM: [modify-ipam](#)
3. Visualizza gli IPAM aggiornati: [describe-ipams](#)

Elimina un IPAM

Per eliminare un IPAM, segui i passaggi descritti in questa sezione. Per informazioni su come aumentare il numero di default di IPAM che è possibile avere anziché eliminare un IPAM esistente, consulta [Quote per l'IPAM](#).

Important


L'eliminazione di un IPAM rimuove tutti i dati monitorati associati all'IPAM, inclusi i dati storici per i CIDR.

AWS Management Console

Per eliminare un IPAM

1. Apri la console IPAM all'indirizzo <https://console.aws.amazon.com/ipam/>.
2. Nel pannello di navigazione, scegli IPAM.
3. Nel riquadro dei contenuti, seleziona il tuo IPAM.
4. Seleziona Azioni > Elimina IPAM.
5. Completa una delle seguenti 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:
 - Annulla l'allocazione di tutti i CIDR allocati alle risorse VPC (come i VPC) in 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 provisioning di tutti i CIDR IPv4 sottoposti a provisioning ai 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](#).
 - Revocare i CIDR sottoposti a provisioning nei pool all'interno dell'IPAM. Per ulteriori informazioni, consulta [Revoca del provisioning di CIDR 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti comandi AWS CLI per eliminare un IPAM:

1. Visualizza gli IPAM correnti: [describe-ipams](#)
2. Elimina un IPAM: [delete-ipam](#)
3. Visualizza gli IPAM aggiornati: [describe-ipams](#)

Per creare un nuovo IPAM, consulta [Crea un IPAM](#).

Monitoraggio dell'utilizzo dell'indirizzo IP in IPAM

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.

Segui i passaggi in questa sezione per monitorare l'utilizzo degli indirizzi IP con IPAM.

Indice

- [Monitora l'utilizzo del CIDR con il pannello di controllo IPAM](#)
- [Monitoraggio dell'utilizzo del CIDR per risorsa](#)
- [Monitoraggio 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

Segui i passaggi in questa sezione per accedere al pannello di controllo IPAM e visualizzare lo stato di tutti i CIDR all'interno di un determinato ambito IPAM.

AWS Management Console

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

1. Apri la console IPAM all'indirizzo <https://console.aws.amazon.com/ipam/>.
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. Il pannello di controllo presenta una panoramica dei pool IPAM e dei CIDR all'interno di un ambito. Puoi aggiungere, rimuovere, 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 CIDR per le risorse: i tipi di CIDR per le risorse all'interno dell'ambito.
 - Sottoreti: il numero di CIDR per le sottoreti.
 - VPC: il numero di CIDR per i VPC.
 - EIP: il numero di CIDR per gli indirizzi IP elastici.
 - Pool IPv4 pubblici: il numero di CIDR per i pool IPv4 pubblici.
- Stato di gestione: lo stato di gestione dei CIDR.
 - CIDR non gestiti: Il numero di CIDR della risorsa per le risorse non gestite in questo ambito.
 - CIDR ignorati: Il numero di CIDR della risorsa che si è 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).
 - CIDR gestiti: Il numero di CIDR della risorsa per risorse gestibili (VPC o pool IPv4 pubblici) assegnati da un pool IPAM nell'ambito.
- CIDR di risorse sovrapposte : il numero di CIDR sovrapposti e non sovrapposti. I CIDR sovrapposti possono portare a un routing errato nei VPC.
 - CIDR sovrapposti: Il numero di CIDR della risorsa che si sovrappongono all'interno di un pool nell'ambito. I CIDR sovrapposti possono portare a un routing errato nei VPC.
 - CIDR non sovrapposti: il numero di CIDR della risorsa non sovrapposti all'interno dei pool IPAM di questo ambito.

- CIDR conformi: Il numero di CIDR della risorsa conformi alle regole di assegnazione per i pool IPAM nell'ambito.
- CIDR conformi: Il numero di CIDR della risorsa conformi alle regole di assegnazione per i pool IPAM nell'ambito.
- Stato di sovrapposizione: il numero di CIDR che si sovrappongono nel corso del tempo.
 - OverlappingResourceCidrs: il numero di CIDR della risorsa che si sovrappongono all'interno dei pool IPAM di questo ambito. I CIDR sovrapposti possono portare a un routing errato nei VPC.
- Stato di conformità: Il numero di CIDR conformi e non conformi alle regole di allocazione per i pool IPAM dell'ambito nel corso del tempo.
 - CompliantResourceCidrs: il numero di CIDR delle risorse conformi alle regole di allocazione.
 - NoncompliantResourceCidrs: il numero di CIDR delle risorse non conformi alle regole di allocazione.
- Utilizzo del VPC: VPC (IPv4 e IPv6) con l'utilizzo IP più alto o più basso. Puoi utilizzare queste informazioni per configurare gli allarmi Amazon CloudWatch e ricevere un avviso in caso di violazione di una soglia di utilizzo IP. Per ulteriori informazioni, consulta [Parametri di utilizzo delle risorse](#).
- Utilizzo della sottorete: sottoreti (solo IPv4) con l'utilizzo IP più alto o più basso. Puoi utilizzare queste informazioni per decidere se mantenere o eliminare le risorse sottoutilizzate. Per ulteriori informazioni, consulta [Parametri di utilizzo delle risorse](#).
- VPC con il maggior numero di IP allocati: i VPC con la più alta percentuale di spazio di indirizzi IP allocato alle sottoreti. Questa informazione è utile a capire se hai bisogno di fornire spazio aggiuntivo ai VPC per gli indirizzi IP.
- Sottoreti con il maggior numero di IP allocati: le sottoreti con la più alta percentuale 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 nel pannello di controllo provengono da parametri memorizzati in Amazon CloudWatch. Per ulteriori informazioni sui parametri archiviati in Amazon CloudWatch, consulta [Monitoraggio IPAM con Amazon CloudWatch](#). Utilizza le opzioni Amazon CloudWatch nella [Documentazione di riferimento della CLI di AWS](#) per visualizzare i parametri per le assegnazioni nei pool e negli ambiti IPAM.

Se si riscontra che il CIDR su cui è stato effettuato il provisioning per un pool è quasi completamente allocato, potrebbe essere necessario effettuare il provisioning di CIDR aggiuntivi. Per ulteriori informazioni, consulta [Effettua il provisioning di CIDR a un pool](#).

Monitoraggio dell'utilizzo del CIDR per risorsa

In IPAM, una risorsa è un'entità del servizio AWS a cui è assegnato un indirizzo IP o un blocco CIDR. IPAM gestisce alcune risorse, ma monitora solo altre risorse.

- **Risorsa gestita:** Una risorsa gestita ha un CIDR assegnato da un pool IPAM. IPAM monitora il CIDR per la potenziale sovrapposizione di indirizzi IP con altri CIDR presenti nel pool e monitora la conformità del CIDR alle regole di assegnazione di un pool. IPAM supporta la gestione del seguente tipo di risorse:
 - VPC
 - Pool IPv4 pubblici

Important

I pool IPv4 pubblici e i pool IPAM sono gestiti da risorse distinte in AWS. I pool IPv4 pubblici sono risorse per account singolo che consentono di convertire i CIDR di proprietà pubblica in indirizzi IP elastici. I pool IPAM possono essere utilizzati per assegnare lo spazio pubblico ai pool IPv4 pubblici.

- **Risorse monitorate:** 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 `get-ipam-resource-cidrs` con la CLI di AWS o quando visualizzi Risorse nel pannello di navigazione. IPAM supporta il monitoraggio delle seguenti risorse:
 - VPC
 - Pool IPv4 pubblici

- Sottoreti VPC
- Indirizzi IP elastici

I passaggi seguenti mostrano come monitorare l'utilizzo del CIDR e la conformità delle regole di assegnazione in base alla risorsa.

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 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. 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 sovrapposto: un intervallo di indirizzi IP è allocato 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.

5. 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 netmask del pool IPAM o se la risorsa non è nella stessa Regione AWS come il pool IPAM, sarà 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.
 - **Utilizzo IP:** per le risorse che sono VPC, questo valore rappresenta la percentuale di spazio degli indirizzi IP nel VPC occupata dai CIDR di sottorete. Per le risorse che sono sottoreti, se alla sottorete è stato assegnato un CIDR IPv4, si tratta della percentuale di spazio di indirizzi IPv4 nella sottorete in uso. Se alla sottorete è stato eseguito il provisioning di un CIDR IPv6, la percentuale di spazio di indirizzi IPv6 in uso non è rappresentata. Al momento non è possibile calcolare la percentuale di spazio degli indirizzi IPv6 in uso. Per risorse costituite da pool IPv4 pubblici, questa è la percentuale di spazio degli indirizzi IP nel pool che è stata allocata a indirizzi IP elastici (EIP).
 - **Regione:** La Regione AWS della risorsa.
 - **ID proprietario:** L'ID dell'account AWS 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 IPv4 pubblico.
 - **ID pool:** ID del pool IPAM in cui si trova la risorsa.
6. 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 di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. La documentazione fornisce descrizioni dettagliate delle opzioni che è possibile utilizzare quando si eseguono i comandi.

Utilizza i seguenti comandi della AWS CLI 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](#)

Monitoraggio IPAM con Amazon CloudWatch

IPAM archivia automaticamente i parametri relativi all'utilizzo degli indirizzi IP (come ad esempio lo spazio degli indirizzi IP disponibile nei pool IPAM e il numero di CIDR di risorse conformi alle regole di allocazione) e all'utilizzo delle risorse nello [spazio dei nomi Amazon CloudWatch](#) AWS/IPAM nella regione di origine dell'IPAM.

Indice

- [Pool e parametri ambito IPAM](#)
- [Parametri di utilizzo delle risorse](#)

Pool e parametri ambito IPAM

IPAM pubblica i dati relativi ai pool e agli ambiti IPAM 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 la configurazione di notifiche in Amazon CloudWatch non rientrano nell'ambito di questa sezione. Per ulteriori informazioni, consulta [Utilizzo dei parametri di Amazon CloudWatch](#) nella Guida per l'utente di Amazon CloudWatch.

Le dimensioni e i parametri che IPAM invia ad Amazon CloudWatch sono elencati di seguito.

Parametri del pool IPAM

Nome parametro	Descrizione
CompliantResourceCidrs	Il numero di CIDR delle risorse gestite conformi alle regole di allocazione del pool IPAM. Per ulteriori informazioni sulle regole di assegnazione, consulta Come creare un pool di livello superiore IPv4 .
NoncompliantResourceCidrs	Il numero di CIDR delle risorse gestite non conformi alle regole di allocazione del pool IPAM. Per ulteriori informazioni sulle regole di assegnazione, consulta Come creare un pool di livello superiore IPv4 .

Nome parametro	Descrizione
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

Nome parametro	Descrizione
CompliantResourceCidrs	Il numero di CIDR delle risorse conformi alle regole di allocazione per i pool IPAM nell'ambito.
ManagedResourceCidrs	Il numero di CIDR delle risorse per risorse gestibili (VPC o pool IPv4 pubblici) allocati da un pool IPAM nell'ambito.
NoncompliantResourceCidrs	Il numero di CIDR delle risorse conformi alle regole di allocazione per i pool IPAM nell'ambito.
OverlappingResourceCidrs	Il numero di CIDR delle risorse che si sovrappongono nell'ambito.
UnmanagedResourceCidrs	Il numero di CIDR delle risorse nell'ambito attualmente associati a risorse gestibili ma non gestite da IPAM.

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

Dimensione	Descrizione
AddressFamily	La famiglia di indirizzi IP per i CIDR delle risorse (IPv4 o IPv6).
Locale	La regione AWS in cui desideri che questo pool IPAM sia disponibile per le allocazioni.

Dimensione	Descrizione
PoolID	L'ID di un pool.
ScopeID	L'ID di un ambito.

Per informazioni sul monitoraggio dei VPC con Amazon CloudWatch, consulta [Metriche di CloudWatch per i VPC](#) nella Guida per l'utente di Amazon Virtual Private Cloud.

Parametri di utilizzo delle risorse

IPAM pubblica i parametri di utilizzo dell'IP per le risorse monitorate da IPAM in Amazon CloudWatch. Queste risorse includono:

- VPC (IPv4 e IPv6)
- Sottoreti (IPv4)
- Pool IPv4 pubblici

IPAM calcola e pubblica i parametri di utilizzo IP separatamente per famiglia di indirizzi IP (IPv4 o IPv6). L'utilizzo IP di una risorsa viene calcolato su tutti i suoi CIDR della stessa famiglia di indirizzi.

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 VPC contenenti un CIDR assegnato da un pool IPAM (con 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 pool IPv4 pubblici contenenti un CIDR assegnato 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. Puoi modificare questi limiti contattando il Centro di supporto AWS come descritto in [Service Quotas di AWS](#) nei Riferimenti generali di AWS.

Example Esempio

Supponiamo che IPAM monitori 2.500 VPC e 10.000 sottoreti, tutti con CIDR IPv4 e IPv6. IPAM pubblica i seguenti parametri di utilizzo IP:

- Fino a 150 parametri per l'utilizzo IP IPv4 del VPC, tra cui:
 - 50 VPC con utilizzo dell'IP IPv4 più elevato
 - 50 VPC con utilizzo di IPv4 più basso
 - Fino a 50 VPC contenenti un CIDR IPv4 assegnato da un pool IPAM
- Fino a 150 parametri per l'utilizzo IPv6 del VPC, tra cui:
 - 50 VPC con utilizzo dell'IP IPv6 più elevato
 - 50 VPC con utilizzo di IPv6 più basso
 - Fino a 50 VPC contenenti un CIDR IPv6 assegnato da un pool IPAM
- Fino a 150 parametri per l'utilizzo IPv4 della sottorete, tra cui:
 - 50 sottoreti con utilizzo dell'IP IPv4 più elevato
 - 50 sottoreti con utilizzo dell'IP IPv4 più basso
 - Fino a 50 sottoreti il cui VPC contiene un CIDR IPv4 assegnato da un pool IPAM

Parametri VPC

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

Nome parametro	Descrizione
VpcIPUsage	Il totale degli IP coperti dai CIDR nelle sottoreti del VPC diviso per il totale degli IP coperti dai CIDR nel VPC. Questo viene calcolato su tutti i CIDR VPC nello stesso ambito IPAM e separatamente per i CIDR IPv4 e IPv6.

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

Dimensione	Descrizione
AddressFamily	La famiglia di indirizzi IP per i CIDR delle risorse (IPv4 o IPv6).
OwnerID	L'ID del proprietario del VPC.
Regione	La regione AWS 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
SubnetIPUsage	Il numero di IP attivi diviso per gli IP totali nel CIDR IPv4 della sottorete.

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

Dimensione	Descrizione
AddressFamily	La famiglia di indirizzi IP per i CIDR delle risorse (solo IPv4).

Dimensione	Descrizione
OwnerID	L'ID del proprietario della sottorete.
Regione	La regione AWS 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.

Parametri del pool IPv4 pubblico

Il nome e la descrizione dei parametri del pool IPv4 pubblico sono elencati di seguito.

Nome parametro	Descrizione
PublicIPv4PoolIPUsage	Il numero di EIP del pool IPv4 pubblico diviso per il totale degli IP del pool.

Di seguito sono elencate le dimensioni che puoi utilizzare per filtrare i parametri del pool IPv4 pubblico.

Dimensione	Descrizione
OwnerID	L'ID del proprietario del pool IPv4 pubblico.
PublicIPv4PoolID	L'ID del pool IPv4 pubblico.
Regione	La regione AWS in cui si trova il pool IPv4 pubblico.
ScopeID	L'ID dell'ambito IPAM a cui appartiene il pool IPv4 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 Elastic di proprietà di Amazon di cui hai eseguito il provisioning o che hai assegnato alle risorse nel tuo account AWS.
AssociatedAmazonOwnedElasticIPs	Il numero di indirizzi IP Elastic di proprietà di Amazon che hai associato alle risorse nel tuo account AWS.
AssociatedBringYourOwnIPs	Il numero di indirizzi IPv4 pubblici che hai portato in AWS utilizzando Porta i tuoi indirizzi IP (BYOIP) e hai associato alle risorse nel tuo account AWS.
BringYourOwnIPs	Il numero di indirizzi IPv4 pubblici che hai portato in AWS utilizzando Porta i tuoi indirizzi IP (BYOIP).
EC2PublicIPs	Il numero di indirizzi IPv4 pubblici assegnati alle istanze EC2 quando le istanze sono state avviate in una sottorete predefinita o in una sottorete configurata per l'assegnazione automatica di un indirizzo IPv4 pubblico.
ServiceManagedBringYourOwnIPs	Il numero di indirizzi IPv4 pubblici che hai portato in AWS utilizzando Porta i tuoi indirizzi IP (BYOIP) di cui hai eseguito il provisioning e che hai gestito tramite un servizio AWS.
ServiceManagedIPs	Il numero di indirizzi IPv4 pubblici di cui hai eseguito il provisioning e che hai gestito tramite un servizio AWS.
UnassociatedAmazonOwnedElasticIPs	Il numero di indirizzi IP Elastic di proprietà di Amazon che non hai associato alle risorse nel tuo account AWS.
UnassociatedBringYourOwnIPs	Il numero di indirizzi IPv4 pubblici che hai portato in AWS utilizzando Porta i tuoi indirizzi IP (BYOIP) e che non hai associato alle risorse nel 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 regione AWS in cui è collocato l'indirizzo IP pubblico.

Suggerimento rapido per la creazione di allarmi

Per creare rapidamente un allarme Amazon CloudWatch per le risorse con un elevato utilizzo di indirizzi IP, apri la console CloudWatch, scegli Parametri, Tutti i parametri, scegli la scheda Query, quindi seleziona Namespace AWS/IPAM > VPC IP Usage Metrics, AWS/IPAM > Subnet IP Usage Metrics o AWS/IPAM > Public IPv4 Pool IP Usage Metrics, scegli il Nome parametro MAX(VpcIPUsage), MAX(SubnetIPUsage) o MAX(PublicIPv4PoolIPUsage) e infine Crea allarme. Per ulteriori informazioni, consulta [Creazione di allarmi nelle query di Approfondimenti sulle metriche](#) nella Guida per l'utente di Amazon CloudWatch.

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 cronologici IP per cercare la modifica dello stato degli indirizzi IP o dei CIDR per i seguenti tipi di risorse:

- VPC
- Sottoreti VPC
- Indirizzi IP elastici
- Istanze EC2
- Interfacce di rete EC2 collegate alle istanze

⚠ Important

Sebbene IPAM non monitori le istanze Amazon EC2 o le interfacce di rete EC2 che sono collegate alle istanze, puoi utilizzare la funzione Cerca nella cronologia IP per cercare i dati cronologici sui CIDR dell'istanza EC2 e dell'interfaccia di rete.

ℹ 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 [Spostamento dei CIDR del VPC tra 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 l'utente [Come integrare IPAM con account esterni alla tua organizzazione](#), il proprietario dell'IPAM, può visualizzare la cronologia degli indirizzi IP di tutte le risorse CIDR di 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 IP IPv4 o IPv6 o 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. Utilizza questa opzione se il CIDR viene visualizzato in più VPC.
7. Selezionare Search (Cerca).

Command line

I comandi di questa sezione rimandano alla documentazione di riferimento alla CLI di AWS. 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 qualche esempio delle modalità di utilizzo di AWS CLI per analizzare e controllare l'utilizzo degli indirizzi IP, consulta [Tutorial: visualizzazione della cronologia degli indirizzi IP mediante la AWS CLI](#).

I risultati della ricerca sono organizzati nelle seguenti colonne:

- Orario di fine campionato: Orario di fine campionato dell'associazione risorsa-CIDR nell'ambito IPAM. Le modifiche vengono rilevate in snapshot periodici, quindi l'orario di fine potrebbe essersi verificato prima di questo orario specifico.
- Orario di inizio campionato: Orario di inizio campionato dell'associazione risorsa-CIDR 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, viene creato un IPAM e pool IPAM con CIDR 10.0.0.0/8 e viene selezionata l'opzione di importazione automatica per consentire a IPAM di individuare e importare tutti i CIDR che rientrano nell'intervallo di indirizzi IP 10.0.0.0/8. Poiché IPAM rileva le modifiche ai CIDR in snapshot periodici, non rileverà 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 netmask del pool IPAM o se la risorsa non è nella stessa Regione AWS come il pool IPAM, sarà 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 Regione AWS della risorsa.
- ID proprietario: L'ID dell'account AWS della persona che ha creato questa risorsa (se applicabile).

Visualizzazione di informazioni dettagliate relative agli indirizzi IP pubblici

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

Note

AWS costi per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla [pagina dei prezzi di Amazon VPC](#).

Puoi visualizzare le informazioni dettagliate per i seguenti tipi di indirizzi IPv4 pubblici:

- Indirizzi IP elastici (EIP): indirizzi IPv4 statici e pubblici forniti da Amazon che puoi associare a un'istanza, un'interfaccia di rete elastica o una risorsa EC2. AWS
- Indirizzi IPv4 pubblici per EC2: indirizzi IPv4 pubblici assegnati a un'istanza EC2 da Amazon (se l'istanza EC2 viene avviata in una sottorete predefinita o in una sottorete configurata per assegnare automaticamente un indirizzo IPv4 pubblico).
- [Indirizzi BYOIPv4: indirizzi IPv4 pubblici nell'intervallo di indirizzi IPv4 che hai introdotto utilizzando Bring your own IP address \(BYOIP\). AWS](#)
- Indirizzi IPv4 gestiti dal servizio: indirizzi IPv4 pubblici assegnati automaticamente alle risorse e gestiti da un servizio. AWS Ad esempio, gli indirizzi IPv4 pubblici su Amazon ECS, Amazon RDS o Amazon Workspaces.

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

Informazioni sugli IP pubblici mostra tutti gli indirizzi IPv4 pubblici utilizzati dai servizi nelle regioni. Puoi utilizzare queste informazioni per identificare l'utilizzo degli indirizzi IPv4 pubblici e visualizzare i consigli per rilasciare gli indirizzi IP elastici inutilizzati.

- Tipi di IP pubblici: il numero di indirizzi IPv4 pubblici organizzati per tipo.
 - EIP di proprietà di Amazon: indirizzi IP elastici che hai fornito o assegnato alle risorse del tuo account. AWS
 - IP pubblici EC2: indirizzi IPv4 pubblici assegnati alle istanze EC2 quando le istanze sono state avviate in una sottorete predefinita o in una sottorete configurata per assegnare automaticamente un indirizzo IPv4 pubblico.
 - BYOIP: indirizzi IPv4 pubblici che hai AWS utilizzato con Bring your own IP address (BYOIP).
 - IP gestiti dal servizio: indirizzi IPv4 pubblici forniti e gestiti da un servizio. AWS
- Utilizzo EIP: numero di indirizzi IP elastici organizzati in base al loro utilizzo.
 - EIP associati di proprietà di Amazon: indirizzi IP elastici che hai fornito nel tuo AWS account e che hai associato a un'istanza, interfaccia di rete o risorsa EC2. AWS
 - BYOIP associato: indirizzi IPv4 pubblici che hai AWS utilizzato utilizzando BYOIP e che hai associato a un'interfaccia di rete.
 - EIP non associati di proprietà di Amazon: indirizzi IP elastici che hai fornito nel tuo AWS account ma che non hai associato a un'interfaccia di rete.
 - BYOIP non associato: indirizzi IPv4 pubblici che hai impostato AWS utilizzando BYOIP ma non associati a un'interfaccia di rete.
- Indirizzi IP pubblici: una tabella di indirizzi IPv4 pubblici e dei relativi attributi.
 - Indirizzo IP: l'indirizzo IPv4 pubblico.
 - Associato: se l'indirizzo è associato o meno a un'istanza, interfaccia di rete o risorsa EC2. AWS
 - Associato: l'indirizzo IPv4 pubblico è associato a un'istanza, interfaccia di rete o risorsa EC2. AWS

- Non associato: l'indirizzo IPv4 pubblico non è associato a nessuna risorsa ed è inattivo nell'account. AWS
- Tipo di indirizzo: il tipo di indirizzo IP.
 - EIP di proprietà di Amazon: l'indirizzo IPv4 pubblico è un indirizzo IP elastico.
 - BYOIP: l'indirizzo IPv4 pubblico è stato portato a utilizzare BYOIP. AWS
 - IP pubblico EC2: l'indirizzo IPv4 pubblico è stato assegnato automaticamente a un'istanza EC2.
 - Servizio gestito BYOIP: l'indirizzo IPv4 pubblico è stato impostato utilizzando Bring your own IP (BYOIP). AWS
 - IP gestito dal servizio: l'indirizzo IPv4 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 IP pubblici non vengono elencati. Per visualizzare questi IP pubblici, 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).
 - Sistema di bilanciamento del carico (EC2): un Application Load Balancer o un Network Load Balancer.
 - Gateway NAT (VPC): Un gateway NAT pubblico Amazon VPC.
 - VPN da sito a sito: un gateway privato virtuale. AWS Site-to-Site VPN
 - Altro: altro servizio attualmente non identificabile.
- Nome (ID EIP): se questo indirizzo IPv4 pubblico è un'allocazione degli indirizzi IP elastici, si tratta del nome e dell'ID dell'allocazione EIP.
- ID dell'interfaccia di rete: se questo indirizzo IPv4 pubblico è associato a un'interfaccia di rete, questo è l'ID dell'interfaccia di rete.
- ID dell'istanza: se questo indirizzo IPv4 pubblico è associato a un'istanza EC2, questo è l'ID dell'istanza.
- Gruppi di sicurezza: se questo indirizzo IPv4 pubblico è associato a un'istanza EC2, si tratta del nome e dell'ID del gruppo di sicurezza assegnato all'istanza.
- Pool IPv4 pubblico: se si tratta di un indirizzo IP elastico proveniente da un pool di indirizzi IP

da un intervallo di indirizzi IP che possiedi e che hai trasferito ad Amazon (utilizzando BYOIP), il valore è l'ID del pool IPv4 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.
- Resource discovery ID (ID rilevamento risorse): l'ID del rilevamento delle risorse che ha rilevato questo indirizzo IPv4 pubblico.
- 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 della presenza di EIP non associati nell'account e della necessità di rilasciarli.

Important

L'aggiornamento di Informazioni sugli IP pubblici è avvenuto recentemente. Se visualizzi un errore relativo alla mancanza delle autorizzazioni per la chiamata `GetIpamDiscoveredPublicAddresses`, devi aggiornare l'autorizzazione gestita associata a una scoperta 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 dei gruppi di sicurezza in entrata:** se questo indirizzo IP è associato a un'istanza EC2, queste sono le regole del gruppo di sicurezza che controllano il traffico in entrata verso l'istanza.
- **Regole dei gruppi di sicurezza in uscita:** se questo indirizzo IP è associato a un'istanza EC2, 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 AWS delle risorse.

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 processi comuni su IPAM utilizzando la CLI di AWS. Per ottenere la AWS CLI, consulta [Accedi a IPAM](#). Per ulteriori informazioni sui concetti IPAM menzionati in questi tutorial, consulta [Funzionamento di IPAM](#).

Indice

- [Tutorial: Creazione di IPAM e pool utilizzando la console](#)
- [Tutorial: Creazione di IPAM e pool utilizzando la AWS CLI](#)
- [Tutorial: visualizzazione della cronologia degli indirizzi IP utilizzando la AWS CLI](#)
- [Tutorial: Porta il tuo ASN in IPAM](#)
- [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#)
- [Tutorial: Trasferimento di un CIDR BYOIP IPv4 in IPAM](#)
- [Tutorial: Pianificare lo spazio degli indirizzi IP VPC per le allocazioni IP delle sottoreti](#)

Tutorial: Creazione di IPAM e pool utilizzando la console

In questo tutorial creerai un IPAM, eseguirai l'integrazione con AWS Organizations, creerai pool di indirizzi IP e creerai 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 utente singolo, 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](#)
- [In che modo AWS Organizations si 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, è necessario aver creato un account AWS Organizations con almeno un account membro. Per istruzioni, consulta [Creazione e configurazione di un'organizzazione](#) nella Guida per l'utente di AWS Organizations.

In che modo AWS Organizations si integra con IPAM

Questa sezione mostra un esempio degli account AWS Organizations 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-account nell'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 (denominato example-member-account-1 nell'immagine seguente) come account amministratore di 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 (denominato example-member-account-2 nell'immagine seguente) come account sviluppatore. Questo account crea un VPC con un CIDR assegnato da un pool IPAM.

The screenshot shows the AWS Organizations console. On the left is a navigation sidebar with 'AWS Organizations' and 'AWS accounts' selected. The main content area is titled 'AWS accounts' and includes a search bar with the placeholder 'Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.' and buttons for 'Hierarchy' and 'List'. Below this is a table showing the organizational structure:

Organizational structure	Account created/joined date
<ul style="list-style-type: none"> Root (r-fssg) <ul style="list-style-type: none"> Organizational-unit-1 (ou-fssg-ycy89843) <ul style="list-style-type: none"> Organizational-unit-1a (ou-fssg-q5brfv9c) <ul style="list-style-type: none"> example-member-account-1 (848560618819 example-member-account-1@amazon.com) - Joined 2022/12/28 example-member-account-2 (848560618819 example-member-account-2@amazon.com) - Joined 2022/12/28 example-management-account (855210303341 example-management-account@amazon.com) - Joined 2022/12/28 (management account) 	

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 dividerlo con questa unità organizzativa.

Note

Per ulteriori informazioni sui tipi di account AWS Organizations, come gli account di gestione e gli account dei membri, consulta la [terminologia e i concetti di AWS Organizations](#).

Fase 1: delega di un amministratore IPAM

In questo passaggio, delegherai come amministratore di IPAM l'account di un membro di AWS Organizations. Quando deleghi un amministratore di IPAM, viene creato automaticamente [un ruolo](#)

[collegato al servizio](#) in ciascuno dei tuoi account dei membri di AWS Organizations. IPAM monitora l'utilizzo dell'indirizzo IP in questi account assumendo il ruolo collegato al servizio in ciascun account membro. Quindi, può scoprire le risorse e i relativi CIDR indipendentemente dalla propria unità organizzativa.

Non puoi completare questo passaggio se non disponi delle autorizzazioni AWS Identity and Access Management (IAM) richieste. Per ulteriori informazioni, consulta [Integrare IPAM con gli account di un'organizzazione AWS](#).

Per delegare un account amministratore IPAM

1. Tramite l'account di gestione di AWS Organizations, apri la console IPAM all'indirizzo <https://console.aws.amazon.com/ipam/>.
2. Nella Console di gestione AWS, scegliere la Regione AWS in cui si desidera utilizzare 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 di AWS Organizations.
5. Immetti l'ID dell'account AWS per l'account membro dell'organizzazione. L'amministratore IPAM deve essere l'account di un membro di AWS Organizations, non l'account di gestione.

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

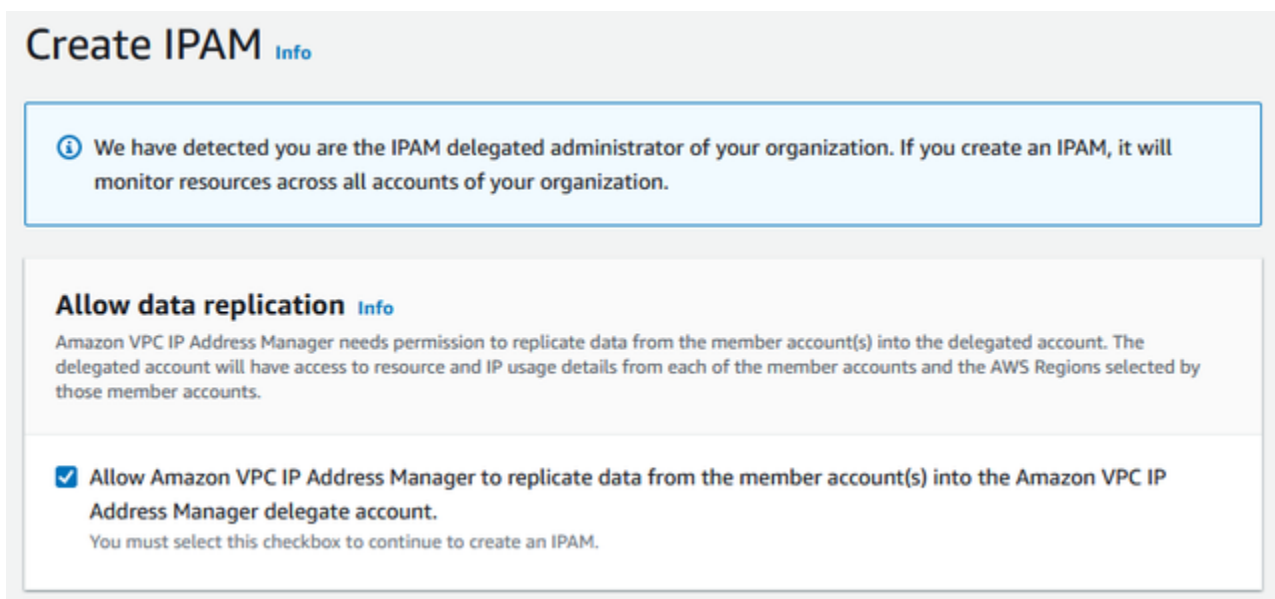
6. Seleziona Salva modifiche. Le informazioni sull'amministratore delegato sono compilate con i dettagli relativi all'account membro.

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 membro di AWS Organizations delegato come amministratore IPAM nel [passaggio precedente](#), apri la console IPAM all'indirizzo <https://console.aws.amazon.com/ipam/>.
2. Nella Console di gestione AWS, scegliere la Regione AWS in cui si desidera 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. Alla voce Regioni operative, scegli le Regioni AWS in cui questo IPAM è in grado di gestire e scovare le risorse. La Regione AWS in cui stai creando l'IPAM è selezionata automaticamente 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.

IPAM settings [Info](#)

Name tag - *optional*

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

Description - *optional*

Write a brief description for the IPAM.

Operating Regions

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



Default resources will be created

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

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

6. Scegli Create IPAM (Crea IPAM).

✔ Successfully created IPAM ipam-005f921c17ebd5107
✕

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

DemoIPAM (ipam-005f921c17ebd5107) Info

Edit Delete

IPAM details

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

Operating Regions | Associated discoveries | Tags

Operating Regions (3) Info

< 1 >

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

Passaggio 3: creazione di un pool IPAM di livello superiore

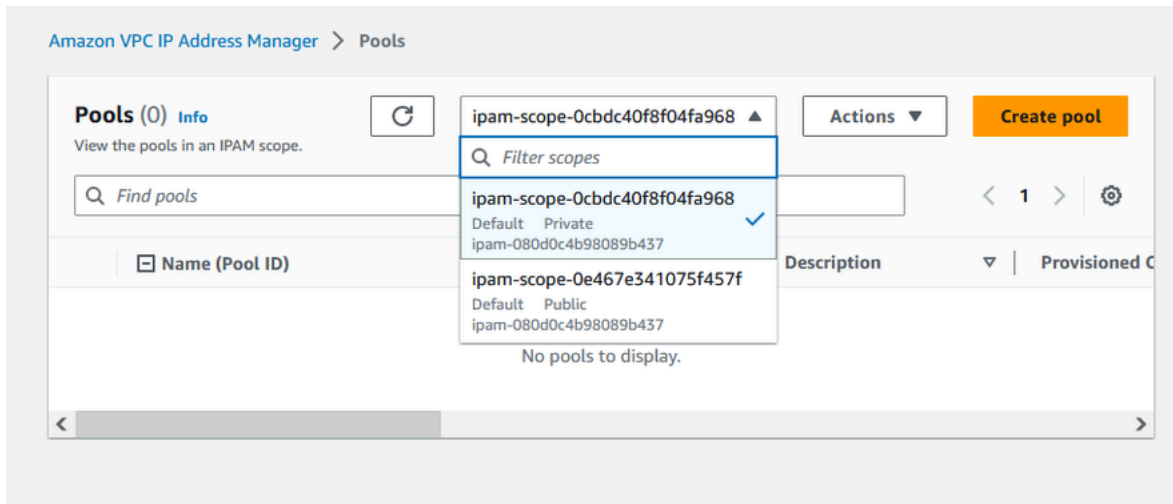
In questo tutorial, creerai una gerarchia di pool a partire dal pool IPAM di livello superiore. Nei passaggi successivi, creerai un paio di pool regionali e un pool di sviluppo di pre-produzione in uno dei pool regionali.

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. Tramite l'account di gestione 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 Address family (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 Regioni AWS 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.

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

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

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

Description - optional
Write a brief description for the pool.

Pool hierarchy [Info](#)

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

Address family
Select the address family for this pool.

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

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

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

CIDRs to provision [Info](#)

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

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/16	65K IPs	Remove
< > ^ v		

Add new CIDR

12. Lascia disattivate le impostazioni delle regole di allocazione di "Configura questo pool". Questo è il nostro pool di livello superiore e non assegnerai CIDR ai VPC direttamente da questo pool. Li allocherai, invece, da un sottogruppo creato da questo pool.

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



AWS best practice

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

Configure this pool's allocation rule settings

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

Sent request to provision 10.0.0.0/16

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

Global pool (ipam-pool-06fb4cace4bc1e551)

Pool summary

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

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

CIDRs (1) Info

Deprovision CIDRs | Provision CIDR

Filter CIDRs

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

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

✔ Sent request to provision 10.0.0.0/16 ✕

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

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

Pool summary

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

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

CIDRs (1) Info

Deprovision CIDRs | Provision CIDR

< 1 > ⚙️

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

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

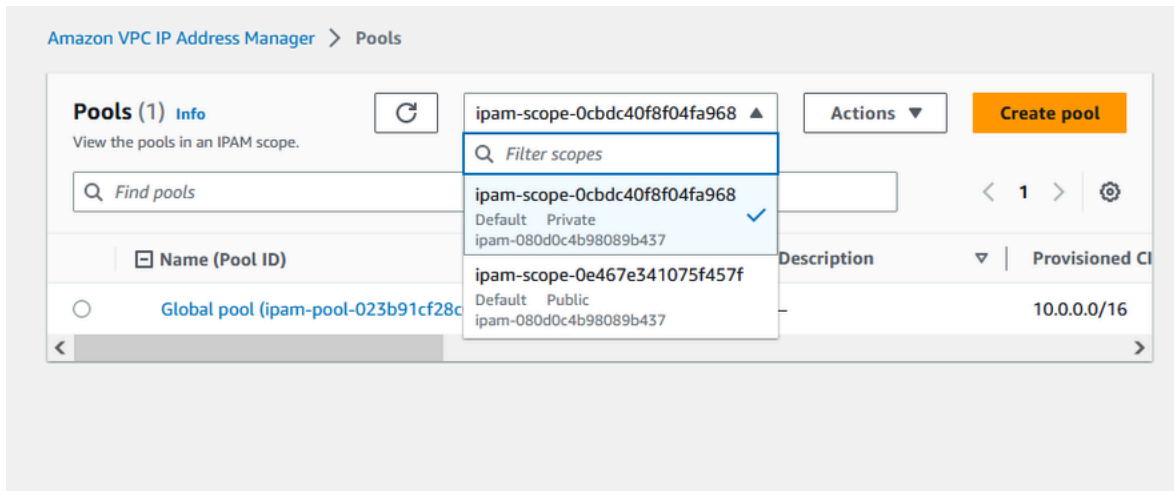
Fase 4: creazione di pool IPAM regionali

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 dei membri della tua organizzazione per allocare i CIDR ai loro VPC.

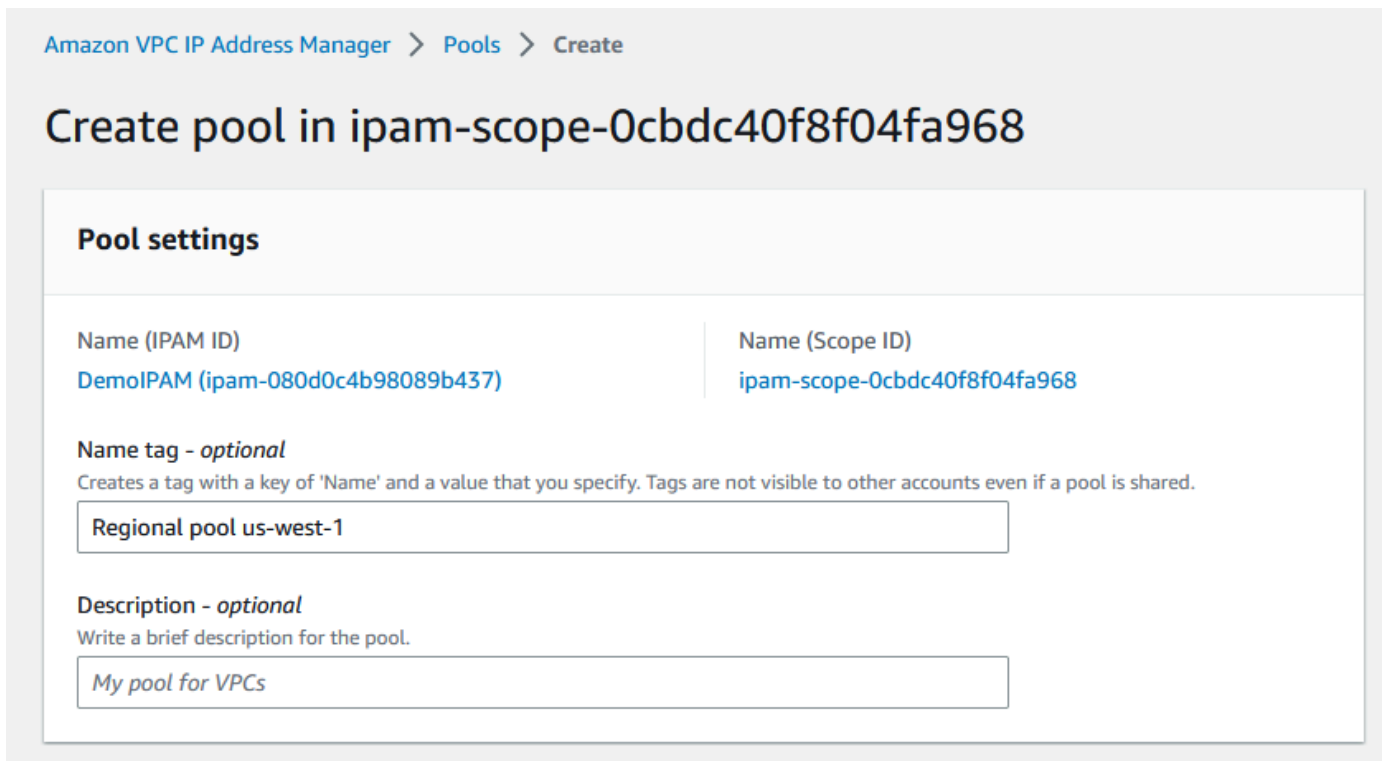
Per creare un pool regionale

1. Tramite l'account di gestione 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.



- 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.

Pool hierarchy [Info](#)

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

Global pool (ipam-pool-023b91cf28c61a0fb) ▼

▼ **Source pool summary**

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

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

IPv4
 IPv6

Pools in the private scope must have address family IPv4.

Locale
Select a locale for this pool to reside.

US West (N. California) - us-west-1 ▼

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

- 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](#).
- In CIDR per cui effettuare il provisioning, inserisci 10.0.0.0/18, che fornirà a questo pool circa 16.000 indirizzi IP disponibili.

CIDRs to provision [Info](#)

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

IP space visualization (source pool)

Zoom Overlapping New allocation Allocated Available

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



CIDR

Enter a CIDR to be provisioned.

16K IPs

< > ^ v

10. Lascia disattivate le impostazioni delle regole di allocazione di "Configura questo pool". Non allocherai CIDR ai VPC direttamente da questo pool. Li allocherai, invece, da un sottogruppo creato da questo pool.

Allocation rule settings - optional [Info](#)

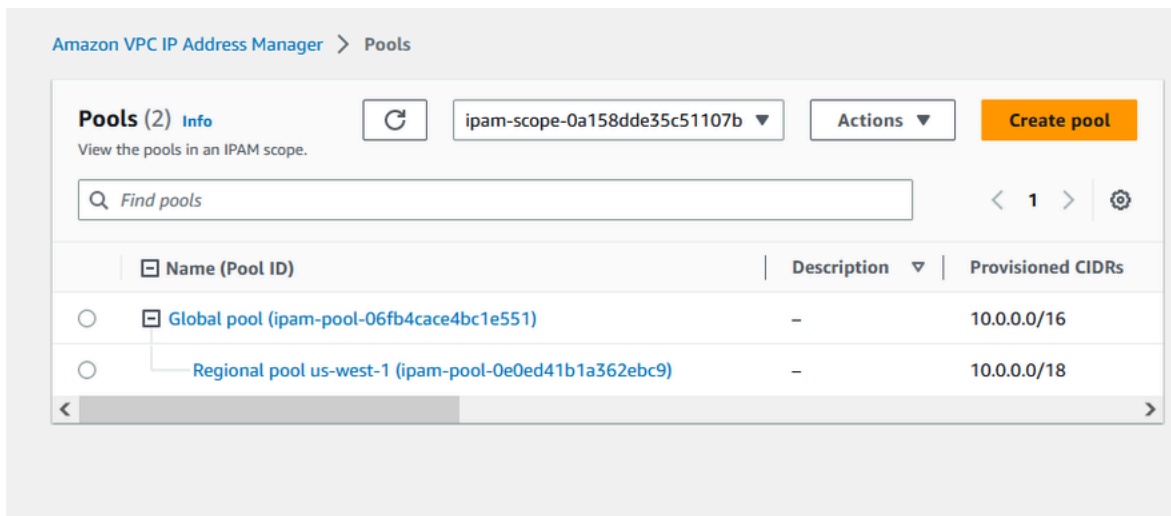


AWS best practice

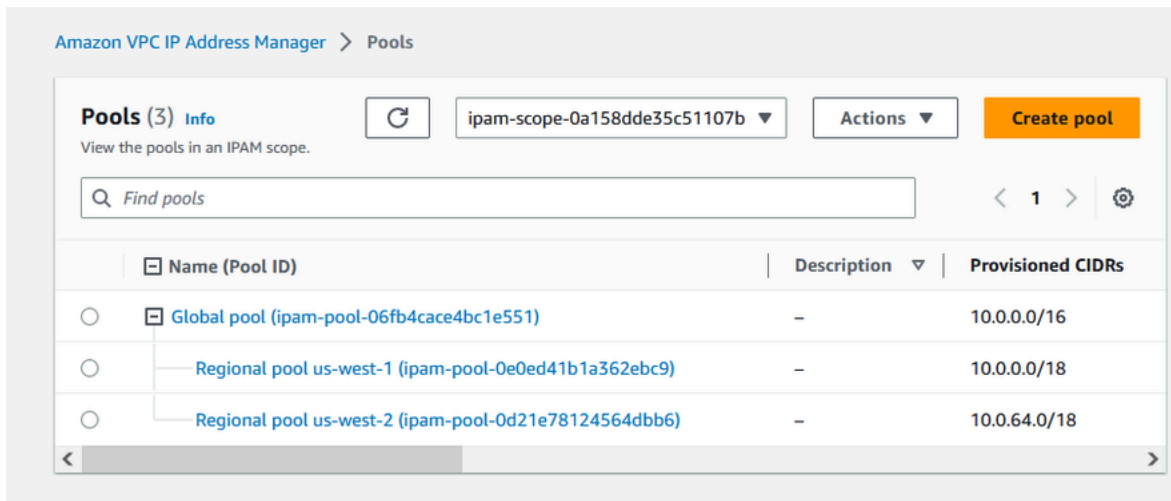
We recommend you create a top-level pool and then Regional pools under the top-level pool. Under the Regional pools, create development pools. From the development pools you can configure allocation rules to control which resources can use CIDRs from these pools. For more examples of how to organize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

Configure this pool's allocation rule settings

11. 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.

Amazon VPC IP Address Manager > Pools > Create

Create pool in ipam-scope-0cbdc40f8f04fa968

Pool settings

Name (IPAM ID)

DemoIPAM (ipam-080d0c4b98089b437)

Name (Scope ID)

ipam-scope-0cbdc40f8f04fa968

Name tag - *optional*

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

Description - *optional*

Write a brief description for the pool.

Pool hierarchy [Info](#)

Source pool

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

▼ Source pool summary

Name (Pool ID)

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

Description

-

Provisioned CIDRs

10.0.0.0/18

Locale

us-west-1

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

CIDRs to provision [Info](#)

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

IP space visualization (source pool)

Zoom Overlapping New allocation Allocated Available

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

CIDR

Enter a CIDR to be provisioned.

10.0.0.0/20 4K IPs Remove

< > ^ v

Add specific CIDR Add CIDR by size

3. 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 i CIDR delle risorse che rileva 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 [Come creare un pool di livello superiore 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 [Come creare un pool di livello superiore 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 consentire ai VPC di assegnare spazio dal pool. Dimosteremo in seguito come funziona.

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



AWS best practice

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

Configure this pool's allocation rule settings

CIDR management

Automatically import discovered resources

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

- Allow automatic import
- Don't allow

Netmask compliancy

Minimum netmask length

The minimum netmask length for allocating resources within the pool.

/24 (256 IPs)

Default netmask length

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

/24 (256 IPs)

Maximum netmask length

The maximum netmask length for allocating resources within the pool.

/24 (256 IPs)

Tag compliancy

Tagging requirements

Add tagging requirements for resources in this pool.

Key

environment



Value - *optional*

pre-prod



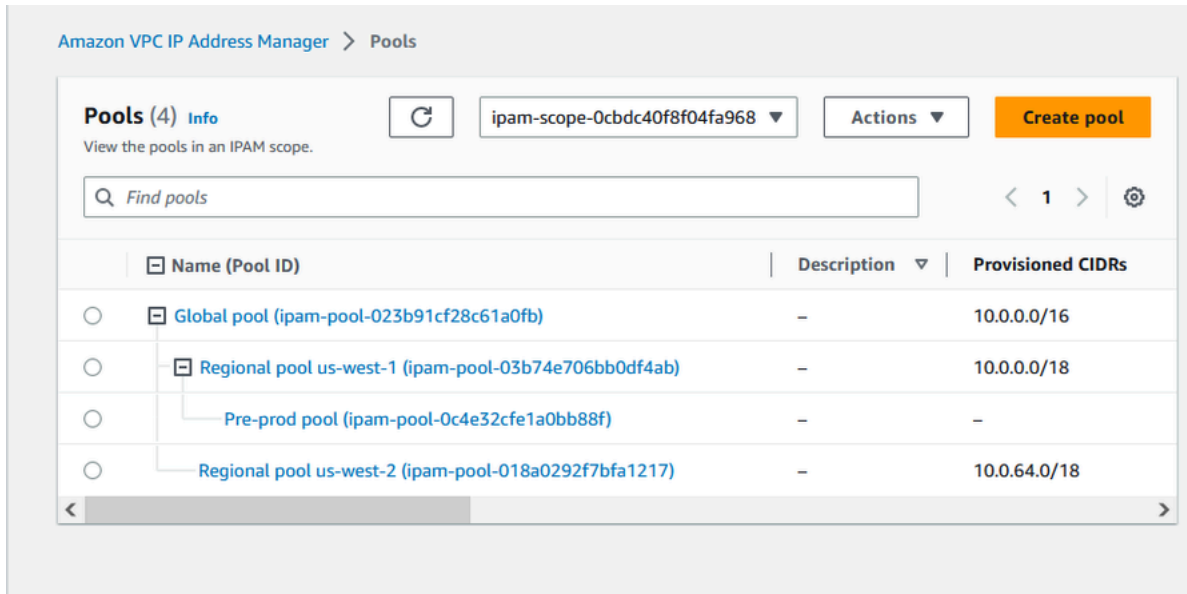
Remove

Add new required tag

You can add up to 49 more tags.

4. 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 la procedura descritta in questa sezione per condividere il pool IPAM di pre-produzione tramite AWS Resource Access Manager (RAM).

Questa sezione è composta da due sottosezioni:

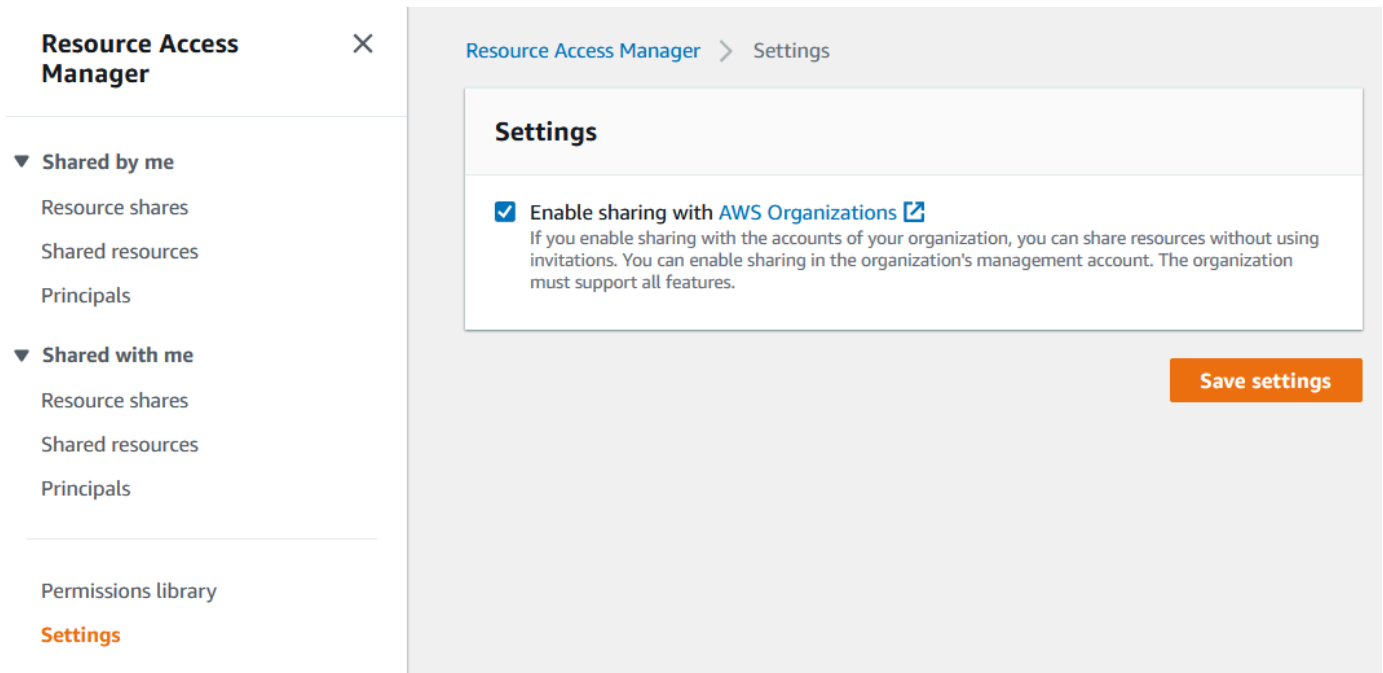
- [Fase 6.1. Abilitazione della condivisione delle risorse in AWS RAM](#): questo passaggio deve essere eseguito dall'account di gestione di AWS Organizations.
- [Fase 6.2. Condividi un pool IPAM utilizzando AWS RAM](#): questo passaggio deve essere eseguito dall'amministratore di IPAM.

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 la procedura descritta in questa sezione per abilitare la condivisione delle risorse con AWS RAM.

Per abilitare la condivisione delle risorse

1. Tramite l'account di gestione di AWS Organizations, apri la console AWS RAM all'indirizzo <https://console.aws.amazon.com/ram/>.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, poi Abilita condivisione con AWS Organizations e quindi 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 [Condividi un pool IPAM utilizzando AWS RAM](#).

Per condividere un pool IPAM utilizzando AWS RAM

1. Tramite l'account di gestione 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. Si apre la console AWS RAM. Condividerai il pool usando AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).

The screenshot shows the AWS IP Address Manager console for a pool named 'Pre-prod pool (ipam-pool-07bdd12d7c94e4693)'. The 'Resource sharing' tab is active, displaying a table with no resource shares. A 'Create resource share' button is highlighted with an orange box.

Pool summary

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

Resource sharing Info

Filter resource shares

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

Create resource share

Si apre la console AWS RAM.

6. Nella console AWS RAM, scegli nuovamente Creazione di 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.

Specify resource share details

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

Resource share name

Name

Provide a descriptive name for the resource share.

Resources - optional

Choose the resources to add to the resource share.

Select resource type

< 1 > ⚙

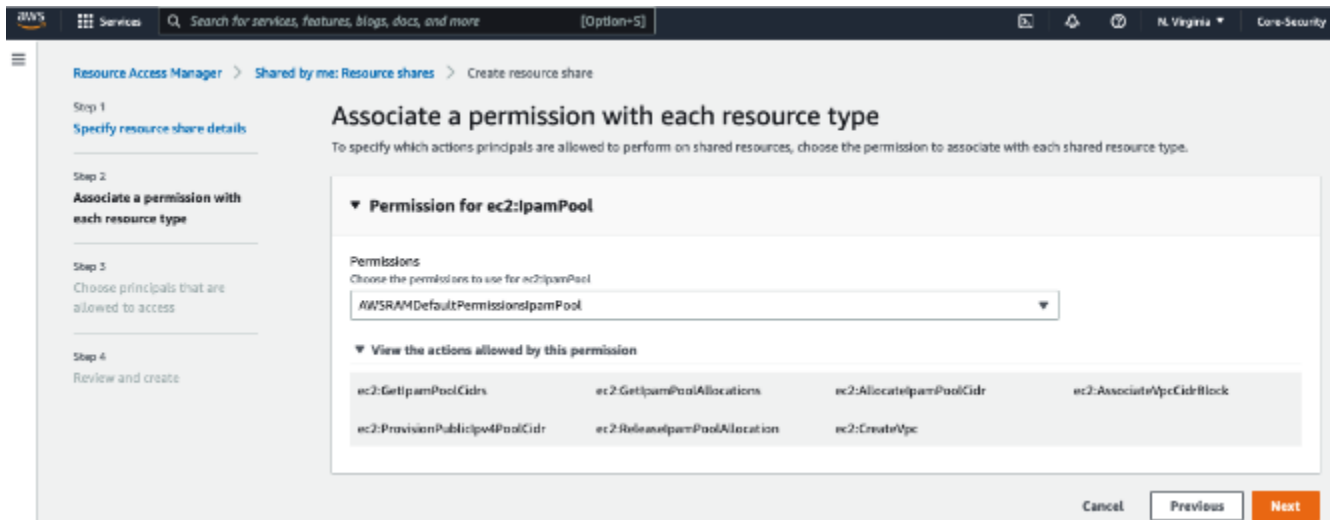
<input type="checkbox"/>	ARN	Locale
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-06fb4cace4bc1e551	None
<input checked="" type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-07bdd12d7c94e4693	us-west-1
<input type="checkbox"/>	arn:aws:ec2::320805250157:ipam-pool/ipam-pool-0b8123821c7ef5319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

Selected resources (1)

Deselect

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

- Seleziona Successivo.
- Lascia selezionata l'autorizzazione `AwsRamDefaultPermissionsIPamPool` predefinita. I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione [Condividi un pool IPAM utilizzando AWS RAM](#).



11. Seleziona Successivo.
12. In Principali, scegli Consenti la condivisione solo all'interno dell'organizzazione. Inserisci l'ID dell'unità organizzativa di AWS Organizations (come indicato in [In che modo AWS Organizations si integra con IPAM](#)), quindi scegli Aggiungi.

Grant access to principals

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

Principals - *optional*

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

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

Principals

You can add multiple principals of different types.

Organizational unit (OU) ▼

ou-fssg-q5brfv9c

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

Add

▼ Selected principals (0)

Deselect

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

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

No selected principals.

Cancel

Previous

Next

13. Seleziona 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 nell'unità

organizzativa con cui è stato condiviso il pool IPAM nella sezione precedente (denominato example-member-account-2 in [In che modo AWS Organizations si integra con IPAM](#)). Per ulteriori informazioni sulle autorizzazioni IAM necessarie per creare VPC, consulta gli [esempi delle policy di Amazon VPC](#) in Nozioni di base su Amazon VPC.

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

1. Per utilizzare l'account membro come account sviluppatore, apri la console VPC all'indirizzo <https://console.aws.amazon.com/vpc/> utilizzando le credenziali dell'account membro.
2. Seleziona Crea VPC.
3. Esegui questa operazione:
 1. Inserisci un nome, come VPC di esempio.
 2. Scegli il blocco CIDR IPv4 allocato dall'IPAM.
 3. Nel pool IPAM IPv4, scegli l'ID del pool di pre-produzione.
 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.

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

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

VPC settings

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

VPC only VPC and more

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

Example VPC

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

IPv4 IPAM pool

ipam-pool-0c4e32cfe1a0bb88f
us-west-1

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

Netmask

/24 (allowed maximum) 256 IPs

4. A scopo dimostrativo, in Tag, non aggiungere altri tag in questo momento. Quando hai creato il pool di pre-produzione (in [5. Creazione di un pool di sviluppo di pre-produzione](#)), hai aggiunto una regola di allocazione che richiede che tutti i VPC creati con i CIDR da questo pool dispongano di un tag ambiente/pre-prod. Per ora, lascia il tag ambiente/pre-prod disattivato in modo da poter vedere che viene visualizzato un errore che segnala che non è stato aggiunto un tag obbligatorio.
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 che tutti i VPC creati con CIDR da questo pool disponessero di un tag ambiente/pre-prod.

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

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

VPC > Your VPCs > Create VPC

Create VPC Info

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

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

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

Example VPC

IPv4 CIDR block Info

IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

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

Tags

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

Key	Value - optional	
<input style="width: 100%;" type="text" value="Name"/>	<input style="width: 100%;" type="text" value="Example VPC"/>	<input type="button" value="Remove"/>
<input style="width: 100%;" type="text" value="environment"/>	<input style="width: 100%;" type="text" value="pre-prod"/>	<input type="button" value="Remove"/>

You can add 48 more tags.

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




✔ You successfully created vpc-07701f4fcc6549b8d / Example VPC

VPC > Your VPCs > vpc-07701f4fcc6549b8d

vpc-07701f4fcc6549b8d / Example VPC

Actions ▼

Details [Info](#)

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

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.

- Utilizzando l'account amministratore IPAM, elimina la condivisione di risorse di esempio nella console AWS RAM. Per istruzioni dettagliate, consulta [Eliminazione di una condivisione di risorse in AWS RAM](#) nella Guida per l'utente di AWS Resource Access Manager.
- 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](#).
- Utilizzando l'account amministratore IPAM, elimina l'IPAM di esempio selezionando l'IPAM nella console IPAM e quindi scegliendo Azioni > Elimina. Per istruzioni dettagliate, consulta [Elimina un IPAM](#).
- 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.

Delete IPAM DemoIPAM (ipam-080d0c4b98089b437) ×

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

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

Cancel Delete

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

Tutorial: Creazione di IPAM e pool utilizzando la AWS CLI

Segui i passaggi descritti in questo tutorial per utilizzare la AWS CLI per creare un IPAM, creare pool di indirizzi IP e assegnare 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 operante nella Regione AWS 1 e nella Regione AWS 2
 - Ambito privato
 - Pool di livello superiore
 - Pool regionale nella Regione AWS 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](#)
- [Passaggio 3: creazione di un pool di indirizzi IPv4](#)
- [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. Pulizia](#)

Passaggio 1: abilitare IPAM nella tua organizzazione

Questa operazione è facoltativa. Completa questo passaggio per abilitare IPAM nell'organizzazione e configurare l'IPAM delegato utilizzando la CLI di AWS. Per ulteriori informazioni sul ruolo dell'account IPAM, consulta [Integrare IPAM con gli account di un'organizzazione AWS](#).

Questa richiesta deve essere fatta 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 111111111111
```

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 Regioni AWS è possibile utilizzare i pool IPAM. Per ulteriori informazioni sulle Regioni operative, consulta [Crea un IPAM](#).

Per creare un IPAM utilizzando la 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
    }
  ]
}
```

Passaggio 3: creazione di un pool di indirizzi IPv4

Per creare un pool di indirizzi IPv4, segui i passaggi descritti in questa sezione.

Important

Su questo pool di livello superiore non utilizzerai l'opzione `--local`. 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 la località `None`, non sarà disponibile per le risorse VPC in nessuna regione AWS.

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

Per creare un pool di indirizzi IPv4 per tutte le risorse AWS che utilizzano la AWS CLI

1. Esegui il comando seguente per creare un pool di indirizzi IPv4. 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 [Effettua il provisioning di CIDR a un pool](#).

Per effettuare il provisioning di un blocco CIDR al pool utilizzando la 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 crei un pool IPAM, il pool appartiene alla Regione AWS dell'IPAM per impostazione predefinita. Quando si crea un VPC, il pool dal quale il VPC si estrae deve trovarsi nella stessa Regione del VPC. Puoi utilizzare l'opzione `--local` 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 --local 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 la 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 operazione è facoltativa. È possibile completare questo passaggio solo se [Integrare IPAM con gli account di un'organizzazione AWS](#) è stato completato.

Quando crei una condivisione AWS RAM di un pool IPAM, essa abiliterà le assegnazioni IP tra gli account. La condivisione RAM è disponibile solo nella Regione AWS di origine. 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 [Condividi un pool IPAM utilizzando 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. Pulizia

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

1. Eliminare 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: visualizzazione della cronologia degli indirizzi IP utilizzando la 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 della AWS CLI, consulta la sezione [Utilizzo della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface.

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:

- VPC
- Sottoreti VPC
- Indirizzi IP elastici
- Istanze EC2 in esecuzione
- Interfacce di rete EC2 collegate alle istanze

Important

Sebbene IPAM non monitori istanze Amazon EC2 o interfacce di rete EC2 collegate alle istanze, puoi utilizzare la funzione Cerca nella cronologia IP per cercare i dati cronologici su CIDR dell'istanza EC2 e dell'interfaccia di rete.

Note

- I comandi di questo tutorial devono essere eseguiti utilizzando l'account proprietario dell'IPAM e la regione AWS che ospita l'IPAM.
- I registri delle modifiche ai CIDR vengono rilevati in snapshot periodici: ciò significa che può trascorrere del tempo prima che i registri vengano visualizzati o aggiornati. Inoltre, i valori di SampledStartTime e SampleEndTime possono differire da quelli effettivi in cui gli eventi 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
```

- Visualizza i risultati dell'analisi. Nell'esempio seguente, nel periodo di tempo il CIDR è stato allocato a un'interfaccia di rete e all'istanza EC2. L'assenza di un valore SampledEndTime indica che il registro 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 differisce dall'ID proprietario dell'interfaccia di rete (come nel caso dei gateway NAT, delle interfacce di rete Lambda nei VPC e di altri servizi AWS), il valore 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. L'assenza di un valore SampledEndTime indica che il registro 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-0864c82a42f5bffd",

```

```

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

```

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, nel periodo di tempo il CIDR è stato allocato a due diversi VPC in una regione diversa da quella di origine dell'IPAM. L'assenza di un valore `SampledEndTime` indica che il registro 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, nel periodo di tempo il CIDR è stato allocato a numerosi sottoreti e VPC. L'assenza di un valore SampledEndTime indica che il registro 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, nel periodo di tempo il CIDR è stato allocato a un'interfaccia di rete e all'istanza EC2. L'assenza di un valore SampledEndTime indica che il registro 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
```

- 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. L'assenza di un valore SampledEndTime indica che il registro 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-0864c82a42f5bffd",
      "ResourceCidr": "10.2.1.0/24",
      "VpcId": "vpc-0f5ee7e1ba908a378",
      "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
    },
    {
      "ResourceOwnerId": "123456789012",
      "ResourceRegion": "us-east-1",
      "ResourceType": "vpc",
      "ResourceId": "vpc-0f5ee7e1ba908a378",
      "ResourceCidr": "10.2.1.0/24",
      "ResourceComplianceStatus": "compliant",
      "ResourceOverlapStatus": "nonoverlapping",
      "VpcId": "vpc-0f5ee7e1ba908a378",
      "SampledStartTime": "2021-12-27T20:08:46.672000+00:00"
    }
  ]
}
```

Scenario 7: Quali risorse sono attualmente associate con **54.0.0.9/32**?

In questo esempio, **54.0.0.9/32** è assegnato a un indirizzo IP elastico che non fa parte dell'organizzazione AWS integrata con il tuo 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. Dato che 54.0.0.9/32 è assegnato a un indirizzo IP elastico che non fa parte dell'organizzazione AWS integrata con l'IPAM in questo esempio, non vengono restituiti record.

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

Tutorial: Porta il tuo ASN in IPAM

Se le tue applicazioni utilizzano indirizzi IP affidabili e numeri di sistema autonomi (ASN) che i tuoi partner o clienti hanno inserito in liste di accettazione nella loro rete, puoi eseguire queste applicazioni in AWS senza chiedere ai tuoi partner o clienti di modificare le loro liste di accettazione.

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 (ISP), ad esempio, utilizzano gli ASN per identificare l'origine del traffico di rete. Non tutte le organizzazioni acquistano i propri ASN, ma quelle che li acquistano possono portare il proprio ASN in AWS.

Porta il tuo Numero di sistema autonomo (BYOASN) ti consente di pubblicizzare gli indirizzi IP che porti in AWS con 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 da portare in IPAM e che tu abbia già portato un CIDR BYOIP in AWS e abbia eseguito il provisioning a un pool nel tuo ambito pubblico. Puoi portare un ASN in IPAM in qualunque momento, ma

per utilizzarlo devi associarlo a un CIDR che hai portato 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 del tuo ASN o di un ASN AWS immediatamente, ma sei limitato a passare da un ASN AWS 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 portato un intervallo di indirizzi IP in AWS con [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#), è necessario l'intervallo CIDR degli indirizzi IP assieme alla chiave privata che hai creato e utilizzato per firmare l'intervallo CIDR che hai portato in AWS.
- Quando porti un intervallo di indirizzi IP a AWS con [Tutorial: trasferisci i tuoi indirizzi IP su IPAM, crei un certificato X.509](#) e [carichi il certificato X.509 nel record RDAP nel 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.

Passaggi del tutorial

Completa i passaggi seguenti utilizzando la console AWS o la 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, scegli IPAM.
3. Scegli il tuo IPAM.
4. Scegli la scheda BYOASNs (BYOASN), quindi scegli Provision BYOASNs (Esegui il provisioning BYOASN).
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 account AWS, ASN è l'ASN che stai portando in 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 che hai creato in [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#). Devi utilizzare la stessa 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. Inserisci la firma.
9. (Facoltativo) Per fornire un altro ASN, scegli Fornisci un altro ASN. Puoi eseguire il provisioning di 5 ASN. Per aumentare questa quota, consulta [Quote per l'IPAM](#).
10. Scegli Provision (Esegui il provisioning).
11. Visualizza il processo di provisioning nella scheda BYOASNs (BYOASN). Attendi che lo Stato (Stato) passi da Provisioning in sospeso a Provisioned (Provisioning eseguito). I BYOASN in stato Failed-provision (Provisioning non riuscito) 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. Per il pool, Service (Servizio) deve essere impostato su EC2 e deve essere stata scelta una locale.
15. Scegli la scheda CIDRs (CIDR) e seleziona un CIDR BYOIP.
16. Scegli Actions (Azioni) > Manage BYOASN associations (Gestisci associazioni BYOASN).
17. In Associated BYOASNs (BYOASN associati), scegli l'ASN portato in AWS. Se disponi di più ASN, puoi associare più ASN al CIDR BYOIP. Puoi associare tutti gli ASN che puoi portare in IPAM. Tieni presente che per impostazione predefinita puoi trasferire fino a 5 ASN in 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 scheda CIDRs (CIDR) del pool.
21. Seleziona il CIDR BYOIP e scegli Actions (Operazioni) > Advertise (Pubblicizzazione). In tal modo, vengono visualizzate le tue opzioni ASN: l'ASN Amazon e tutti gli ASN portati in 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 l'annullamento del provisioning dell'ASN, nella scheda BYOASNs (BYOASN) scegli l'ASN, quindi scegli Deprovision ASN (Annulla provisioning ASN). In tal modo, il provisioning dell'ASN viene annullato. I BYOASN in stato Deprovisioned (Provisioning annullato) vengono rimossi automaticamente dopo 7 giorni.

La pulizia è completa.

Command line

1. Esegui il provisioning del tuo ASN includendo l'ASN e lo stesso messaggio di autorizzazione e la stessa firma che hai utilizzato quando hai portato il tuo CIDR in IPAM in [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#).

```
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 che l'opzione è ProvisionStatusimpostata 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 gli Amazon ASN 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 CIDR BYOIP a cui lo hai associato, puoi annullarne il provisioning.

```
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 ti spiegano come portare lo spazio di un indirizzo IP pubblico su AWS e come gestire tale 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 su AWS: È possibile utilizzare IPAM per incorporare uno spazio di indirizzo IP pubblico una volta e quindi distribuire gli IP pubblici tra le Regioni. Senza IPAM, sarà necessario integrare gli IP pubblici per ciascuna Regione AWS.

Important

Prima di iniziare questo tutorial, completa i passaggi riportati in [Prerequisiti di onboarding per il tuo intervallo di indirizzi BYOIP](#) nella Guida per l'utente di Amazon EC2 per istanze Linux. Quando si creano i ROA, per i CIDR IPv4 è necessario impostare la lunghezza massima di un prefisso di indirizzo IP su /24. Per i CIDR IPv6, se vengono aggiunti a un pool pubblicizzabile, la lunghezza massima di un prefisso dell'indirizzo IP deve essere /48. Ciò garantisce la piena flessibilità per dividere il tuo indirizzo IP pubblico tra Regioni AWS. 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 blocco IPv4 più piccolo e che /48 è il blocco IPv6 più piccolo che puoi pubblicizzare da una Regione a Internet.

Indice

- [Portare un CIDR IPv4 pubblico su IPAM utilizzando sia la Console di gestione AWS sia la AWS CLI](#)
- [Portare un CIDR IPv4 pubblico su IPAM usando solo la AWS CLI](#)

Portare un CIDR IPv4 pubblico su IPAM utilizzando sia la Console di gestione AWS sia la AWS CLI

Segui questi passaggi per portare un CIDR IPv4 o IPv6 su IPAM utilizzando sia la Console di gestione AWS sia la AWS CLI.

Important

Prima di iniziare questo tutorial, completa i passaggi riportati in [Prerequisiti di onboarding per il tuo intervallo di indirizzi BYOIP](#) nella Guida per l'utente di Amazon EC2 per istanze Linux. Quando si creano i ROA, per i CIDR IPv4 è necessario impostare la lunghezza massima di un prefisso di indirizzo IP su /24. Per i CIDR IPv6, se vengono aggiunti a un pool pubblicizzabile, la lunghezza massima di un prefisso dell'indirizzo IP deve essere /48. Ciò garantisce la piena flessibilità per dividere il tuo indirizzo IP pubblico tra Regioni AWS. 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 blocco IPv4 più piccolo e che /48 è il blocco IPv6 più piccolo che puoi pubblicizzare da una Regione a Internet.

Indice

- [Portare un CIDR IPv4 su IPAM utilizzando sia la Console di gestione AWS sia la AWS CLI](#)

- [Porta un CIDR IPv6 su IPAM utilizzando la Console di gestione AWS](#)

Portare un CIDR IPv4 su IPAM utilizzando sia la Console di gestione AWS sia la AWS CLI

Segui questi passaggi per portare un CIDR IPv4 su IPAM e allocare un indirizzo IP elastico (EIP) utilizzando sia la Console di gestione AWS sia la AWS CLI.

Important

- Al momento non è possibile fornire o pubblicizzare intervalli di indirizzi BYOIP nelle Zone Locali.
- 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](#).
- Ciascun passaggio di questo tutorial deve essere eseguito da uno dei tre account di 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 alloca i CIDR da un pool IPAM. In questo tutorial, tale account verrà chiamato account membro.

Indice

- [Fase 1: creazione di profili denominati della AWS CLI 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](#)
- [Fase 4. Condividi il pool regionale](#)
- [Passaggio 5: creazione di un pool IPv4 pubblico](#)
- [Passaggio 6: effettuare il provisioning del CIDR IPv4 pubblico al pool IPv4 pubblico](#)
- [Passaggio 7: creazione di un indirizzo IP elastico dal pool IPv4 pubblico](#)

- [Passaggio 8: associazione dell'indirizzo IP elastico a un'istanza EC2](#)
- [Passaggio 9: pubblicizzare il CIDR](#)
- [Passaggio 10: eliminazione](#)

Fase 1: creazione di profili denominati della AWS CLI e ruoli IAM

Per completare questo tutorial come singolo utente AWS, puoi utilizzare profili denominati AWS CLI 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 gli account AWS, consulta [Utilizzo di un ruolo IAM in AWS CLI](#) nella Guida per l'utente di AWS Identity and Access Management.

Crea un ruolo e un profilo denominato per ciascuno dei tre account AWS che utilizzerai in questo tutorial:

- Un profilo chiamato `management-account` per l'account di gestione di AWS Organizations.
- Un profilo chiamato `ipam-account` per l'account membro di AWS Organizations configurato come amministratore IPAM.
- Un profilo chiamato `member-account` per l'account membro di AWS Organizations che alloca i CIDR 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 potrai osservare che i comandi AWS CLI di esempio utilizzano l'opzione `--profile` con uno dei profili con nome 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 Address family (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).

La località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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.

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 pubblico, scegli una delle seguenti opzioni:
 - BYOIP: stai trasferendo l'intervallo di indirizzi IPv4 o IPv6 (BYOIP) a questo pool.
 - Di proprietà di Amazon: desideri che Amazon fornisca un intervallo di indirizzi IPv6 a questo pool.

11. Esegui una di queste operazioni:

- Se nel passaggio precedente hai scelto BYOIP, in CIDR di cui eseguire il provisioning scegli un CIDR di cui effettuare il provisioning per il pool. Tieni presente che quando effettui il provisioning di un CIDR IPv4 a un pool all'interno del pool di livello superiore, il CIDR IPv4 minimo di cui è possibile effettuare il provisioning è /24; non sono consentiti CIDR più specifici (come ad esempio /25). È necessario includere il CIDR e il messaggio BYOIP e la firma del certificato nella richiesta in modo da poter verificare il possesso dello spazio pubblico. Per un elenco dei prerequisiti BYOIP, incluso come ottenere questo messaggio BYOIP e la firma del certificato, consulta [Portare un CIDR IPv4 pubblico su IPAM utilizzando sia la Console di gestione AWS sia la AWS CLI](#).

Important

Il provisioning del CIDR BYOIP può richiedere fino a una settimana.

- Se hai scelto Di proprietà di Amazon, in Lunghezza della maschera di rete scegli una lunghezza della maschera di rete compresa tra /40 e /52. Il valore predefinito è /52.
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 scheda CIDRs (CIDR) nella pagina dei dettagli del pool. Tieni presente che il provisioning del CIDR BYOIP può richiedere fino a una settimana.

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 Località 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 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.

La località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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 Service (Servizio), scegli EC2 (EIP/VPC). Il servizio selezionato determina il servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione possibile è EC2 (EIP/VPC), il che significa che i CIDR allocati da questo pool saranno pubblicizzabili per il servizio Amazon EC2 (per gli indirizzi IP elastici) e per il servizio Amazon VPC (per i CIDR associati ai VPC).
10. In CIDR to provision (CIDR di cui effettuare il provisioning), scegli un CIDR di cui effettuare il provisioning per il pool. Tieni presente che quando effettui il provisioning di un CIDR a un pool all'interno del pool di livello superiore, il CIDR IPv4 minimo di cui è possibile effettuare il provisioning è /24; non sono consentiti CIDR più specifici (come ad esempio /25).
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 [Come creare un pool di livello superiore 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 scheda CIDRs (CIDR) nella pagina dei dettagli del pool.

Fase 4. Condividi il pool regionale

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

4.1. 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 la procedura descritta in questa sezione per abilitare la condivisione delle risorse con AWS RAM. Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile management-account`.

Per abilitare la condivisione delle risorse

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

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

4.2. 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 [Condividi un pool IPAM utilizzando AWS RAM](#). Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile ipam-account`.

Per condividere un pool IPAM utilizzando AWS RAM

1. Tramite l'account di gestione 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 e scegli Azioni > Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. Si apre la console AWS RAM. Il pool è condiviso tramite AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).
6. Nella console AWS RAM, scegli nuovamente Creazione di una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona tipo di risorsa, scegli pool IPAM, quindi scegli l'ARN del pool che desideri condividere.
9. Seleziona Avanti.
10. Scegli l'autorizzazione. `AWSRAMPermissionIpamPoolByoipCidrImport` I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione [Condividi un pool IPAM utilizzando AWS RAM](#).
11. Seleziona Avanti.
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. Seleziona Avanti.
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 allocare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool1`, quindi 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 `AWSRAMDefaultPermissionsIpamPool1`.

Passaggio 5: creazione di un pool IPv4 pubblico

La creazione di un pool IPv4 pubblico è un passaggio necessario per portare un indirizzo IPv4 pubblico ad AWS da gestire con IPAM. Questo passaggio dovrebbe essere eseguito dall'account membro che effettuerà il provisioning di un indirizzo IP elastico.

Questo passaggio deve essere eseguito dall'account membro utilizzando la AWS CLI.

Important

I pool IPv4 pubblici e i pool IPAM sono gestiti da risorse distinte in AWS. I pool IPv4 pubblici sono risorse per account singolo che consentono di convertire i CIDR di proprietà pubblica in indirizzi IP elastici. I pool IPAM possono essere utilizzati per assegnare lo spazio pubblico ai pool IPv4 pubblici.

Per creare un pool IPv4 pubblico tramite la 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 `Local` 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, potrai visualizzare l'ID del pool IPv4 pubblico. Sarà necessario questo ID nel passaggio successivo.

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

Passaggio 6: effettuare il provisioning del CIDR IPv4 pubblico al pool IPv4 pubblico

Effettua il provisioning del CIDR IPv4 pubblico al pool IPv4 pubblico. Il valore per `--region` deve corrispondere al valore `Local` 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. Il prefisso IPv4 meno specifico che puoi utilizzare è `/24`.

Note

Se stai trasferendo un intervallo di CIDR /24 su IPAM per dividerlo 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 pool IPv4 pubblico tramite la 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 su cui è stato effettuato il provisioning nel pool IPv4 pubblico.

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

Una volta creato il pool IPv4 pubblico, per visualizzare il pool IPv4 pubblico allocato nel pool regionale IPAM, apri la console IPAM e visualizza l'allocazione nel pool regionale sotto Allocations (Allocazioni) o Resources (Risorse).

Passaggio 7: creazione di un indirizzo IP elastico dal pool IPv4 pubblico

Completa i passaggi descritti nella sezione [Allocazione di un indirizzo IP elastico](#) della Guida per l'utente di Amazon EC2 per le istanze Linux per creare un indirizzo IP elastico (EIP) dal pool IPv4 pubblico. Quando apri EC2 nella Console di gestione AWS, la regione AWS in cui allochi l'EIP deve corrispondere all'opzione `Local` scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP.

Questo passaggio deve essere eseguito dall'account membro. Se usi la AWS CLI, utilizza l'opzione `--profile member-account`.

Passaggio 8: associazione dell'indirizzo IP elastico a un'istanza EC2

Completa i passaggi descritti nella sezione [Associazione di un indirizzo IP elastico a un'istanza o un'interfaccia di rete](#) della Guida per l'utente di Amazon EC2 per le istanze Linux per associare l'EIP a

un'istanza EC2. Quando apri EC2 nella Console di gestione AWS, la regione AWS alla quale associ l'EIP deve corrispondere all'opzione Local e 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 dall'account membro. Se usi la AWS CLI, utilizza l'opzione `--profile member-account`.

Passaggio 9: pubblicizzare il CIDR

I passaggi in questa sezione devono essere eseguiti dall'account IPAM. Una volta associato l'indirizzo IP elastico (EIP) a un'istanza o a Elastic Load Balancer, puoi iniziare a pubblicizzare il CIDR portato in AWS presente nel pool con il valore Service EC2 (EIP/VPC) (Servizio EC2 (EIP/VPC)) configurato. 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. Scegli la scheda CIDR.
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 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.

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. Scegli la scheda CIDR.
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 usi la AWS CLI, utilizza l'opzione `--profile member-account`.

- Completa i passaggi descritti nella sezione [Annullamento dell'associazione di un indirizzo IP elastico](#) della Guida per l'utente di Amazon EC2 per le istanze Linux per annullare l'associazione dell'EIP. Quando apri EC2 nella Console di gestione AWS, la regione AWS dalla quale annulli l'associazione dell'EIP deve corrispondere all'opzione Local e 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 usi la AWS CLI, utilizza l'opzione `--profile member-account`.

- Completa i passaggi descritti nella sezione [Rilascio di un indirizzo IP elastico](#) della Guida per l'utente di Amazon EC2 per le istanze Linux per rilasciare un indirizzo IP elastico (EIP) dal pool IPv4 pubblico. Quando apri EC2 nella Console di gestione AWS, la regione AWS in cui allochi

l'EIP deve corrispondere all'opzione `Local` scelta al momento della creazione del pool che verrà utilizzato per il CIDR BYOIP.

Passaggio 4: revoca del provisioning del CIDR IPv4 dal pool IPv4 pubblico

Questo passaggio deve essere eseguito dall'account membro utilizzando la AWS CLI.

1. Visualizza i CIDR BYOIP.

```
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 seguente comando per rilasciare l'ultimo indirizzo IP nel CIDR dal pool IPv4 pubblico. Inserisci l'indirizzo IP con una netmask di /32.

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

Nell'output, sarà visualizzato il CIDR su cui è stato revocato il provisioning.

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

Important

È necessario eseguire di nuovo questo comando per ogni indirizzo IP nell'intervallo CIDR. Se il CIDR è un /24, dovrai eseguire questo comando per revocare il provisioning di ciascuno dei 256 indirizzi IP nel CIDR /24.

3. Visualizza di nuovo i CIDR BYOIP e assicurati che non ci siano più indirizzi con provisioning. 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 conteggio degli indirizzi IP nel pool IPv4 pubblico.

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

Note

Può trascorrere un po' di tempo prima che IPAM scopra che le allocazioni pubbliche del pool IPv4 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.

Passaggio 5: eliminazione del pool IPv4 pubblico

Questo passaggio deve essere eseguito dall'account membro.

- Esegui il comando seguente per eliminare il pool IPv4 pubblico dal CIDR. Quando esegui il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `Local` 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 usando 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).

Passaggio 6: 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 usi la AWS CLI per eliminare le condivisioni RAM e disabilitare l'integrazione di RAM, utilizza le opzioni `--profile ipam-account` e `--profile management-account`.

- Completa i passaggi descritti nella sezione [Eliminazione di una condivisione di risorse in AWS RAM](#) e [Disattivazione della condivisione delle risorse con AWS Organizations](#) della Guida

per l'utente di AWS RAM, in questo ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione RAM con AWS Organizations.

Passaggio 7: revoca del provisioning dei CIDR dal pool regionale e dal pool di livello superiore

Questo passaggio deve essere eseguito dall'account IPAM. Se usi la AWS CLI per condividere il pool, utilizza l'opzione `--profile ipam-account`.

- Completa i passaggi descritti in [Revoca del provisioning di CIDR da un pool](#) per revocare il provisioning dei CIDR dal pool regionale e quindi dal pool di livello superiore, in questo ordine.

Passaggio 8: eliminazione del pool regionale e del pool di livello superiore

Questo passaggio deve essere eseguito dall'account IPAM. Se usi la AWS CLI per condividere il pool, utilizza l'opzione `--profile ipam-account`.

- Completa i passaggi descritti in [Elimina un pool](#) per eliminare il pool regionale e quindi il pool di livello superiore, in questo ordine.

Porta un CIDR IPv6 su IPAM utilizzando la Console di gestione AWS

Completa i passaggi di questo tutorial per portare un CIDR IPv6 su IPAM e allocare un VPC con il CIDR utilizzando in entrambi i casi la Console di gestione AWS e la AWS CLI.

Important

- Al momento non è possibile fornire o pubblicizzare intervalli di indirizzi BYOIP nelle Zone Locali.
- 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](#).
- Ciascun passaggio di questo tutorial deve essere eseguito da uno dei tre account di 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 alloca i CIDR 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 (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. 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 Address family (Famiglia di indirizzi), scegli IPv6.

Quando scegli IPv6, viene visualizzata un'opzione di attivazione/disattivazione che consente di controllare se AWS è può divulgare pubblicamente i CIDR in questo pool. Lascia abilitata questa opzione.

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. Verifica che sia selezionata l'opzione Allow CIDRs in this pool to be publicly advertisable (Consenti ai CIDR in questo pool di essere pubblicizzabili pubblicamente).
10. In Locale (Località), scegli None (Nessuna). Imposterai la località sul pool Regionale.

La località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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.

11. In Origine IP pubblico, BYOIP è selezionato per impostazione predefinita.
12. In CIDR to provision (CIDR di cui effettuare il provisioning), scegli un CIDR di cui effettuare il provisioning per il pool. Si noti che quando si esegue il provisioning di un CIDR IPv6 in un pool all'interno del pool di primo livello, l'intervallo di indirizzi IPv6 più specifico che è possibile inserire è /48 per i CIDR pubblicizzabili pubblicamente e /60 per i CIDR che non lo sono. È necessario includere il CIDR e il messaggio BYOIP e la firma del certificato nella richiesta in modo da poter verificare il possesso dello spazio pubblico. Per un elenco dei prerequisiti BYOIP, incluso come ottenere questo messaggio BYOIP e la firma del certificato, consulta [Portare un CIDR IPv4 pubblico su IPAM utilizzando sia la Console di gestione AWS sia la AWS CLI](#).

⚠ Important

Il provisioning del CIDR BYOIP può richiedere fino a una settimana.

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. È possibile visualizzare lo stato del provisioning nella scheda CIDRs (CIDR) nella pagina dei dettagli del pool. Tieni presente che il provisioning del CIDR BYOIP può richiedere fino a una settimana.

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 località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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 Service (Servizio), scegli EC2 (EIP/VPC). Il servizio selezionato determina il servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione possibile è EC2 (EIP/VPC), il che significa che i CIDR allocati da questo pool saranno pubblicizzabili per il servizio Amazon EC2 (per gli indirizzi IP elastici) e per il servizio Amazon VPC (per i CIDR associati ai VPC).
10. In CIDR to provision (CIDR di cui effettuare il provisioning), scegli un CIDR di cui effettuare il provisioning per il pool. Si noti che quando si esegue il provisioning di un CIDR IPv6 in un pool all'interno del pool di primo livello, l'intervallo di indirizzi IPv6 più specifico che è possibile inserire è /48 per i CIDR pubblicizzabili pubblicamente e /60 per i CIDR che non lo sono.
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 rilevante: 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:
 - I CIDR che saranno assegnati per queste risorse non devono già essere assegnati 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 rileva più CIDR che si sovrappongono, IPAM importerà solo il CIDR più grande.
 - Se IPAM rileva più CIDR con CIDR corrispondenti, 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. L'intervallo delle lunghezze della netmask

possibili per gli indirizzi IPv4 è 0 - 32. L'intervallo delle lunghezze della netmask possibili per gli indirizzi IPv6 è 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.
- Località: la località necessaria alle risorse che utilizzano i CIDR di 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 scheda CIDRs (CIDR) nella pagina dei dettagli del pool.

Fase 3. Condividi il pool regionale

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

4.1. 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 la procedura descritta in questa sezione per abilitare la condivisione delle risorse con AWS RAM. Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile management-account`.

Per abilitare la condivisione delle risorse

1. Tramite l'account di gestione di AWS Organizations, apri la console AWS RAM all'indirizzo <https://console.aws.amazon.com/ram/>.

2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, poi Abilita condivisione con AWS Organizations e quindi Salva impostazioni.

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

4.2. 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 [Condividi un pool IPAM utilizzando AWS RAM](#). Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile ipam-account`.

Per condividere un pool IPAM utilizzando AWS RAM

1. Tramite l'account di gestione 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 e scegli Azioni > Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. Si apre la console AWS RAM. Il pool è condiviso tramite AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).
6. Nella console AWS RAM, scegli nuovamente Creazione di una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona tipo di risorsa, scegli pool IPAM, quindi scegli l'ARN del pool che desideri condividere.
9. Seleziona Avanti.
10. Scegli l'autorizzazione. `AWSRAMPermissionIpamPoolByoipCidrImport` I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione [Condividi un pool IPAM utilizzando AWS RAM](#).
11. Seleziona Avanti.
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. Seleziona Avanti.
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 allocare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool`, quindi 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`.

Passaggio 4: creazione di un VPC

Completa i passaggi descritti nella sezione [Creazione di un VPC](#) della Guida per l'utente di Amazon VPC.

Questo passaggio deve essere eseguito dall'account membro.

Note

- Quando apri il VPC nella Console di gestione AWS, la regione AWS in cui crei il VPC deve corrispondere all'opzione `Local` 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 crei 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 portato in AWS presente nel pool con il Service EC2 (EIP/VPC) (Servizio EC2 (EIP/VPC)) configurato. 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. Scegli la scheda CIDR.
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. Scegli la scheda CIDR.
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 descritti nella sezione [Eliminazione di un VPC](#) della Guida per l'utente di Amazon VPC per eliminare il VPC. Quando apri il VPC nella Console di gestione AWS, la regione AWS da cui elimini il VPC deve corrispondere all'opzione Local e 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: 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.

- Completa i passaggi descritti nella sezione [Eliminazione di una condivisione di risorse in AWS RAM](#) e [Disattivazione della condivisione delle risorse con AWS Organizations](#) della Guida per l'utente di AWS RAM, in questo ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione RAM con AWS Organizations.

Passaggio 4: revoca del provisioning dei CIDR dal pool regionale e dal pool di livello superiore

Questo passaggio deve essere eseguito dall'account IPAM.

- Completa i passaggi descritti in [Revoca del provisioning di CIDR da un pool](#) per revocare il provisioning dei CIDR dal pool regionale e quindi dal pool di livello superiore, in questo 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.

Portare un CIDR IPv4 pubblico su IPAM usando solo la AWS CLI

Segui questi passaggi per portare un CIDR IPv4 o IPv6 su IPAM utilizzando soltanto la AWS CLI.

Important

Prima di iniziare questo tutorial, completa i passaggi riportati in [Prerequisiti di onboarding per il tuo intervallo di indirizzi BYOIP](#) nella Guida per l'utente di Amazon EC2 per istanze Linux. Quando si creano i ROA, per i CIDR IPv4 è necessario impostare la lunghezza massima di un prefisso di indirizzo IP su /24. Per i CIDR IPv6, se vengono aggiunti a un pool pubblicizzabile, la lunghezza massima di un prefisso dell'indirizzo IP deve essere /48. Ciò garantisce la piena flessibilità per dividere il tuo indirizzo IP pubblico tra Regioni AWS. 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 blocco IPv4 più piccolo e che /48 è il blocco IPv6 più piccolo che puoi pubblicizzare da una Regione a Internet.

Indice

- [Portare un CIDR IPv4 pubblico su IPAM usando solo la AWS CLI](#)
- [Portare un CIDR IPv6 su IPAM usando solo la AWS CLI](#)

Portare un CIDR IPv4 pubblico su IPAM usando solo la AWS CLI

Segui questi passaggi per portare un CIDR IPv4 su IPAM e allocare un indirizzo IP elastico (EIP) utilizzando soltanto la AWS CLI.

Important

- Al momento non è possibile fornire o pubblicizzare intervalli di indirizzi BYOIP nelle Zone Locali.
- 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.](#)
- Ciascun passaggio di questo tutorial deve essere eseguito da uno dei tre account di 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 alloca i CIDR da un pool IPAM. In questo tutorial, tale account verrà chiamato account membro.

Indice

- [Fase 1: creazione di profili denominati della AWS CLI 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. Condividi il pool regionale](#)
- [Passaggio 8: creazione di un pool IPv4 pubblico](#)
- [Passaggio 9: effettuare il provisioning del CIDR IPv4 pubblico al pool IPv4 pubblico](#)
- [Passaggio 10: creazione di un indirizzo IP elastico dal pool IPv4 pubblico](#)
- [Passaggio 11: pubblicizzazione del CIDR](#)
- [Passaggio 12: pulizia](#)

Fase 1: creazione di profili denominati della AWS CLI e ruoli IAM

Per completare questo tutorial come singolo utente AWS, puoi utilizzare profili denominati AWS CLI 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 gli account AWS, consulta [Utilizzo di un ruolo IAM in AWS CLI](#) nella Guida per l'utente di AWS Identity and Access Management.

Crea un ruolo e un profilo denominato per ciascuno dei tre account AWS che utilizzerai in questo tutorial:

- Un profilo chiamato `management-account` per l'account di gestione di AWS Organizations.
- Un profilo chiamato `ipam-account` per l'account membro di AWS Organizations configurato come amministratore IPAM.
- Un profilo chiamato `member-account` per l'account membro di AWS Organizations che alloca i CIDR 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 potrai osservare che i comandi AWS CLI di esempio utilizzano l'opzione `--profile` con uno dei profili con nome per indicare quale account deve eseguire il comando.

Passaggio 2: creazione di un IPAM

Questo passaggio è facoltativo. 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 nel passaggio successivo. Stai utilizzando l'ambito pubblico perché i CIDR BYOIP sono indirizzi IP pubblici, che è ciò 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 indirizzi IPv4 per tutte le risorse AWS che utilizzano la 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 effettui il provisioning di un CIDR IPv4 a un pool all'interno del pool di livello superiore, il CIDR IPv4 minimo di cui è possibile effettuare il provisioning è /24; non sono consentiti CIDR più specifici (come ad esempio /25). È necessario includere il CIDR e il messaggio BYOIP e la firma del certificato nella richiesta in modo da poter verificare il possesso dello spazio pubblico. Per un elenco dei prerequisiti BYOIP, incluso come ottenere questo messaggio BYOIP e la firma del certificato, consulta [Portare un CIDR IPv4 pubblico su IPAM usando solo la AWS CLI](#).

Questo passaggio deve essere eseguito dall'account IPAM.

Important

Bisogna solo aggiungere `--cidr-authorization-context` 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 `--cidr-authorization-context`. 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 effettuare il provisioning di un blocco CIDR al pool utilizzando la 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-0a03d430ca3f5c035 --cidr 130.137.245.0/24 --cidr-authorization-
context Message="1|aws|470889052444|130.137.245.0/24|20250101|SHA256|
RSAPSS",Signature="W3gdQ9PZHLjPmrxnGM~cvGx~KCIsmAU0P7EN07VRnfSuf9NuJU5RUveQzus~QmF~Nx42j3z7d
hApR89Kt6GxRY0dRaNx8yt-uoZWzxcT2yIhWngy-
du9pnEHB0X6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXE1T5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZ1afBbrFxrjFWRCTJhc7Cg3ASbR0-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --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

Il provisioning del CIDR BYOIP 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. Il codice `--local` è obbligatorio nel pool e deve essere una delle Regioni operative configurate al momento della creazione dell'IPAM. La località è la Regione AWS in cui si desidera che questo pool IPAM sia disponibile per le assegnazioni. 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.

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 servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione possibile è `ec2`, il che significa che i CIDR allocati da questo pool saranno pubblicizzabili per il servizio Amazon EC2 (per gli indirizzi IP elastici) e per il servizio Amazon VPC (per i CIDR associati ai VPC).

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. Tieni presente che quando effettui il provisioning di un CIDR a un pool all'interno del pool di livello superiore, il CIDR IPv4 minimo di cui è possibile effettuare il provisioning è /24; non sono consentiti CIDR più specifici (come ad esempio /25).

Questo passaggio deve essere eseguito dall'account IPAM.

Per assegnare un blocco CIDR al pool Regionale utilizzando la 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. Condividi il pool regionale

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

4.1. 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 la procedura descritta in questa sezione per abilitare la condivisione delle risorse con AWS RAM. Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile management-account`.

Per abilitare la condivisione delle risorse

1. Tramite l'account di gestione di AWS Organizations, apri la console AWS RAM all'indirizzo <https://console.aws.amazon.com/ram/>.

2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, poi Abilita condivisione con AWS Organizations e quindi Salva impostazioni.

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

4.2. 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 [Condividi un pool IPAM utilizzando AWS RAM](#). Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile ipam-account`.

Per condividere un pool IPAM utilizzando AWS RAM

1. Tramite l'account di gestione 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 e scegli Azioni > Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. Si apre la console AWS RAM. Il pool è condiviso tramite AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).
6. Nella console AWS RAM, scegli nuovamente Creazione di una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona tipo di risorsa, scegli pool IPAM, quindi scegli l'ARN del pool che desideri condividere.
9. Seleziona Avanti.
10. Scegli l'autorizzazione. `AWSRAMPermissionIpamPoolByoipCidrImport` I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione [Condividi un pool IPAM utilizzando AWS RAM](#).
11. Seleziona Avanti.
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. Seleziona Avanti.
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 allocare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool`, quindi 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`.

Passaggio 8: creazione di un pool IPv4 pubblico

La creazione di un pool IPv4 pubblico è un passaggio necessario per portare un indirizzo IPv4 pubblico ad AWS da gestire con IPAM. Questo passaggio in genere viene eseguito da un altro account AWS che desidera effettuare il provisioning di un indirizzo IP elastico.

Questo passaggio deve essere eseguito dall'account membro.

Important

I pool IPv4 pubblici e i pool IPAM sono gestiti da risorse distinte in AWS. I pool IPv4 pubblici sono risorse per account singolo che consentono di convertire i CIDR di proprietà pubblica in indirizzi IP elastici. I pool IPAM possono essere utilizzati per assegnare lo spazio pubblico ai pool IPv4 pubblici.

Per creare un pool IPv4 pubblico tramite la 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, potrai visualizzare l'ID del pool IPv4 pubblico. Sarà necessario questo ID nel passaggio successivo.

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

Passaggio 9: effettuare il provisioning del CIDR IPv4 pubblico al pool IPv4 pubblico

Effettua il provisioning del CIDR IPv4 pubblico al pool IPv4 pubblico. Il valore per `--region` deve corrispondere al valore `--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 pool IPv4 pubblico tramite la 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 su cui è stato effettuato il provisioning nel pool IPv4 pubblico.

```
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 10: creazione di un indirizzo IP elastico dal pool IPv4 pubblico

Crea un indirizzo IP elastico (EIP) dal pool IPv4 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 pool IPv4 pubblico utilizzando la 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"
    }
  ]
}
```

Passaggio 11: pubblicizzazione del CIDR

I passaggi in questa sezione devono essere eseguiti dall'account IPAM. Una volta associato l'indirizzo IP elastico (EIP) a un'istanza o a Elastic Load Balancer, puoi iniziare a pubblicizzare il CIDR che hai portato su AWS presente nel pool con il codice `--aws-service ec2` definito. 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.

Inizia a pubblicizzare il CIDR utilizzando la 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 12: 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 il comando in questa sezione, il valore per `--region` deve corrispondere all'opzione `--local` che hai inserito quando hai creato il pool che verrà utilizzato per il CIDR BYOIP.

Eliminazione tramite la 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. Arresta la pubblicizzazione del CIDR IPv4.

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. Visualizza i CIDR BYOIP.

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": []
    }
]
}

```

5. Rilascia l'ultimo indirizzo IP nel CIDR dal pool IPv4 pubblico. Inserisci l'indirizzo IP con una netmask di /32. È necessario eseguire di nuovo questo comando per ogni indirizzo IP nell'intervallo CIDR. Se il CIDR è un /24, dovrai eseguire questo comando per revocare il provisioning di ciascuno dei 256 indirizzi IP nel CIDR /24. 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 130.137.245.255/32 --profile member-account
```

Nell'output, sarà visualizzato il CIDR su cui è stato revocato il provisioning.

```

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

```

6. Visualizza di nuovo i CIDR BYOIP e assicurati che non ci siano più indirizzi con provisioning. 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 conteggio degli indirizzi IP nel pool IPv4 pubblico.

```
{
```

```

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

```

7. 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 corrispondere all'opzione `--località` 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": []
}

```

8. 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"
  }
}
```

9. Elimina le condivisioni RAM e disabilita l'integrazione di RAM con AWS Organizations. Completa i passaggi descritti nella sezione [Eliminazione di una condivisione di risorse in AWS RAM](#) e [Disattivazione della condivisione delle risorse con AWS Organizations](#) della Guida per l'utente di AWS RAM, in questo ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione RAM con AWS Organizations.

Questo passaggio deve essere eseguito rispettivamente dall'account IPAM e dall'account di gestione. Se usi la AWS CLI per eliminare le condivisioni RAM e disabilitare l'integrazione

di RAM, utilizza le opzioni `--profile ipam-account` e `--profile management-account`.

10. 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"
  }
}
```

11. 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"
  }
}
```

12. 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"
  }
}
```

13. 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"  
  }  
],  
}
```

Portare un CIDR IPv6 su IPAM usando solo la AWS CLI

Segui questi passaggi per portare un CIDR IPv6 su IPAM e assegnare un VPC utilizzando soltanto la AWS CLI.

Important

- Al momento non è possibile fornire o pubblicizzare intervalli di indirizzi BYOIP nelle Zone Locali.
- 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](#).
- Ciascun passaggio di questo tutorial deve essere eseguito da uno dei tre account di 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 alloca i CIDR da un pool IPAM. In questo tutorial, tale account verrà chiamato account membro.

Indice

- [Fase 1: creazione di profili denominati della AWS CLI 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](#)
- [Passaggio 8: creazione di un VPC utilizzando il CIDR IPv6](#)
- [Passaggio 9: pubblicizzare il CIDR](#)
- [Passaggio 10: eliminazione](#)

Fase 1: creazione di profili denominati della AWS CLI e ruoli IAM

Per completare questo tutorial come singolo utente AWS, puoi utilizzare profili denominati AWS CLI 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 gli account AWS, consulta [Utilizzo di un ruolo IAM in AWS CLI](#) nella Guida per l'utente di AWS Identity and Access Management.

Crea un ruolo e un profilo denominato per ciascuno dei tre account AWS che utilizzerai in questo tutorial:

- Un profilo chiamato `management-account` per l'account di gestione di AWS Organizations.
- Un profilo chiamato `ipam-account` per l'account membro di AWS Organizations configurato come amministratore IPAM.
- Un profilo chiamato `member-account` per l'account membro di AWS Organizations che alloca i CIDR 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 potrai osservare che i comandi AWS CLI di esempio utilizzano

l'opzione `--profile` con uno dei profili con nome per indicare quale account deve eseguire il comando.

Passaggio 2: creazione di un IPAM

Questo passaggio è facoltativo. 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 desideri che questo CIDR del pool IPAM sia pubblicizzabile da 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 indirizzi IPv6 per tutte le risorse AWS che utilizzano la 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. Si noti che quando si esegue il provisioning di un CIDR IPv6 in un pool all'interno del pool di primo livello, l'intervallo di indirizzi IPv6 più specifico che è possibile inserire è /48 per i CIDR pubblicizzabili pubblicamente e /60 per i CIDR che non lo sono. È necessario includere il CIDR e il messaggio BYOIP e la firma del certificato nella richiesta in modo da poter verificare il possesso dello spazio pubblico. Per un elenco dei prerequisiti BYOIP, incluso come ottenere questo messaggio BYOIP e la firma del certificato, consulta [Portare un CIDR IPv4 pubblico su IPAM usando solo la AWS CLI](#).

Bisogna solo aggiungere `--cidr-authorization-context` 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 `--cidr-authorization-context`.

Questo passaggio deve essere eseguito dall'account IPAM.

Per effettuare il provisioning di un blocco CIDR al pool utilizzando la 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-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --cidr-authorization-
context Message="1|aws|470889052444|2605:9cc0:409::/48|20250101|
SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9R1pBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxFnp7RAJDvF1mBwxmSgH~C
Vp6LON3y00Xmp4JENB9uM7sMlu6oeoutGyyhXFeYPz1GSRdcdfKNKaimvPCqVsxGN5AwSi1KQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

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

Il provisioning del CIDR BYOIP 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 servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione possibile è `ec2`, il che significa che i CIDR allocati da questo pool saranno pubblicizzabili per il servizio Amazon EC2 (per gli indirizzi IP elastici) e per il servizio Amazon VPC (per i CIDR associati ai VPC).

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. Si noti che quando si esegue il provisioning del CIDR in un pool all'interno del pool di livello superiore, l'intervallo di indirizzi IPv6 più specifico che è possibile inserire è /48 per i CIDR pubblicizzabili pubblicamente e /60 per i CIDR che non lo sono.

Questo passaggio deve essere eseguito dall'account IPAM.

Per assegnare un blocco CIDR al pool Regionale utilizzando la 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 descritti in questa sezione per condividere il pool IPAM utilizzando (RAM). AWS Resource Access Manager

4.1. 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 la procedura descritta in questa sezione per abilitare la condivisione delle risorse con AWS RAM. Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile management-account`.

Per abilitare la condivisione delle risorse

1. Tramite l'account di gestione di AWS Organizations, apri la console AWS RAM all'indirizzo <https://console.aws.amazon.com/ram/>.

2. Nel riquadro di navigazione a sinistra, scegli Impostazioni, poi Abilita condivisione con AWS Organizations e quindi Salva impostazioni.

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

4.2. 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 [Condividi un pool IPAM utilizzando AWS RAM](#). Se usi la AWS CLI per abilitare la condivisione delle risorse, utilizza l'opzione `--profile ipam-account`.

Per condividere un pool IPAM utilizzando AWS RAM

1. Tramite l'account di gestione 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 e scegli Azioni > Visualizza dettagli.
4. Alla voce Condivisione risorse, scegli Crea condivisione di risorse. Si apre la console AWS RAM. Il pool è condiviso tramite AWS RAM.
5. Selezionare Create a resource share (Crea una condivisione di risorse).
6. Nella console AWS RAM, scegli nuovamente Creazione di una condivisione di risorse.
7. Aggiungi un Nome per il pool condiviso.
8. In Seleziona tipo di risorsa, scegli pool IPAM, quindi scegli l'ARN del pool che desideri condividere.
9. Seleziona Avanti.
10. Scegli l'autorizzazione. `AWSRAMPermissionIpamPoolByoipCidrImport` I dettagli delle opzioni di autorizzazione non rientrano nell'ambito di questo tutorial, ma puoi trovare ulteriori informazioni su queste opzioni alla sezione [Condividi un pool IPAM utilizzando AWS RAM](#).
11. Seleziona Avanti.
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. Seleziona Avanti.
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 allocare l'indirizzo IP CIDRS dal pool IPAM, crea una seconda condivisione di risorse con `AWSRAMDefaultPermissionsIpamPool`, quindi 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`.

Passaggio 8: creazione di un VPC utilizzando il CIDR IPv6

Crea un VPC utilizzando l>ID del pool IPAM. È inoltre necessario associare un blocco CIDR IPv4 al VPC tramite l'opzione `--cidr-block` o la richiesta fallirà. 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 CIDR IPv6 utilizzando la 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

Una volta creato il VPC con CIDR assegnato in IPAM, puoi iniziare a pubblicizzare il CIDR che hai portato su AWS presente nel pool con il codice `--aws-service ec2` definito. 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 utilizzando la 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.

Eliminazione tramite la 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 `--local` 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 descritti nella sezione [Eliminazione di una condivisione di risorse in AWS RAM](#) e [Disattivazione della condivisione delle risorse con AWS Organizations](#) della Guida per l'utente di AWS RAM, in questo ordine, per eliminare le condivisioni RAM e disabilitare l'integrazione RAM con AWS Organizations.

Questo passaggio deve essere eseguito rispettivamente dall'account IPAM e dall'account di gestione. Se usi la AWS CLI per eliminare le condivisioni RAM e disabilitare l'integrazione di RAM, utilizza le opzioni `--profile ipam-account` e `--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 CIDR BYOIP IPv4 in IPAM

Segui questi passaggi per trasferire un CIDR IPv4 esistente su IPAM. Se si dispone già di un CIDR IPv4 BYOIP con AWS, è possibile spostare il CIDR a IPAM da un pool IPv4 pubblico. Non è possibile spostare un CIDR IPv6 a IPAM.

Questo tutorial presuppone che tu abbia già portato un intervallo di indirizzi IP su AWS utilizzando il processo descritto in [Utilizzare i propri indirizzi IP \(BYOIP\) in Amazon EC2](#) e ora desideri trasferire quell'intervallo di indirizzi IP su IPAM. Se si sta portando per la prima volta un nuovo indirizzo IP a AWS, completare i passaggi in [Tutorial: trasferisci i tuoi indirizzi IP su IPAM](#).

Se trasferisci un pool IPv4 pubblico su IPAM, non si avrà alcun impatto sulle allocazioni esistenti. Dopo aver trasferito un pool IPv4 pubblico su 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](#).

Important

- Questo tutorial presuppone che tu abbia già completato i passaggi nella sezione [Crea un IPAM](#).
- Ciascun passaggio di questo tutorial deve essere eseguito da uno dei due account di AWS Organizations:
 - 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: creazione di profili denominati della AWS CLI e ruoli IAM](#)
- [Passaggio 2: ottenimento dell'ID di ambito pubblico dell'IPAM](#)
- [Passaggio 3: creazione di un pool IPAM](#)
- [Passaggio 4: condivisione del pool IPAM utilizzando la AWS RAM](#)
- [Passaggio 5: trasferimento di un CIDR BYOIP IPv4 esistente su IPAM](#)
- [Passaggio 6: visualizzazione del CIDR in IPAM](#)
- [Passaggio 7: pulizia](#)

Fase 1: creazione di profili denominati della AWS CLI e ruoli IAM

Per completare questo tutorial come singolo utente AWS, puoi utilizzare profili denominati AWS CLI 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 gli account AWS, consulta [Utilizzo di un ruolo IAM in AWS CLI](#) nella Guida per l'utente di AWS Identity and Access Management.

Crea un ruolo e un profilo denominato per ciascuno dei tre account AWS che utilizzerai in questo tutorial:

- Un profilo chiamato `ipam-account` per l'account AWS che è l'amministratore IPAM.
- Un profilo chiamato `byoip-owner-account` per l'account AWS nell'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 potrai osservare che i comandi AWS CLI di esempio utilizzano l'opzione `--profile` con uno dei profili con nome 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 `--local` 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 servizio AWS in cui il CIDR sarà pubblicizzabile. Attualmente, l'unica opzione possibile è `ec2`, il che significa che i CIDR allocati da questo pool saranno pubblicizzabili per il servizio Amazon EC2 (per gli indirizzi IP elastici) e per il servizio Amazon VPC (per i CIDR associati ai VPC).

Per creare un pool di indirizzi IPv4 per il CIDR BYOIP trasferito utilizzando la 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. Il valore `OwnerId` sarà necessario nel 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: condivisione del pool IPAM utilizzando la AWS RAM

Segui i passaggi in questa sezione per condividere un pool IPAM utilizzando la AWS RAM in modo che un altro account AWS possa trasferire un CIDR BYOIP IPV4 esistente al pool IPAM e utilizzare il pool IPAM. Questo passaggio deve essere eseguito dall'account **ipam-account**.

Per condividere un pool di indirizzi IPv4 utilizzando la AWS CLI

1. Visualizza le autorizzazioni di AWS RAM disponibili per i pool IPAM. Per completare i passaggi riportati in questa sezione, sono necessari entrambi gli ARN.

```
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'account **byoip-owner-account** di importare i CIDR BYOIP 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'account **byoip-owner-account** di allocare l'indirizzo IP CIDRS dal pool IPAM ai pool IPv4 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"
  }
}
```

Grazie alla creazione della condivisione di risorse in RAM, l'account proprietario dell'IPAM può ora assegnare CIDR all'IPAM.

Passaggio 5: trasferimento di un CIDR BYOIP IPv4 esistente su IPAM

Segui i passaggi in questa sezione per trasferire un CIDR BYOIP IPV4 esistente su IPAM. Questo passaggio deve essere eseguito dall'account **byoip-owner-account**.

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

Puoi usare la AWS Management Console o la 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 account **byoip-owner-account**.
2. Nel pannello di navigazione, seleziona Pool.
3. Scegli 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 comandi AWS CLI per trasferire un CIDR BYOIP al pool IPAM utilizzando il comando AWS CLI:

1. Esegui il comando seguente per trasferire il CIDR. Assicurarsi che il valore `--region` sia la Regione AWS 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 un CIDR BYOIP trasferito nel pool IPAM utilizzando la AWS CLI

- Esegui il comando seguente per visualizzare l'assegnazione gestita in IPAM. Assicurarsi che il valore `--region` sia la Regione AWS 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 eliminare le risorse create in questo tutorial utilizzando la 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: condivisione del pool IPAM utilizzando la 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. Assicurarsi che il valore `--region` corrisponda alla Regione AWS 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 l'ultimo indirizzo IP nel CIDR dal pool IPv4 pubblico. Inserisci l'indirizzo IP con una netmask di /32. È necessario eseguire di nuovo questo comando per ogni indirizzo IP nell'intervallo CIDR. Se il CIDR è un /24, dovrai eseguire questo comando per revocare il

provisioning di ciascuno dei 256 indirizzi IP nel CIDR /24. 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 130.137.249.255/32
```

Nell'output, sarà visualizzato il CIDR su cui è stato revocato il provisioning.

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

6. Visualizza di nuovo i CIDR BYOIP e assicurati che non ci siano più indirizzi con provisioning. 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 pool IPv4 pubblico.

```
{
  "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 indirizzi IPv4 privato in un ambito IPAM privato a VPC e sottoreti. Puoi completare questo tutorial anche utilizzando l'ambito pubblico e un intervallo CIDR IPv6 creando il VPC con l'opzione di blocco CIDR IPv6 fornita da Amazon nella 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 allocare i CIDR alle sottoreti oppure può essere utilizzato come pool di origini in cui puoi creare altri pool. In questo

tutorial, utilizziamo il pool di pianificazione delle risorse come pool di origini per i pool di sottoreti.

- Puoi creare più pool di pianificazione delle risorse utilizzando lo stesso VPC se al VPC è stato eseguito il provisioning di più di un CIDR; se a un VPC sono assegnati due CIDR, ad esempio, puoi 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 creare VPC, consulta gli [esempi delle policy di Amazon VPC](#) in Nozioni di base su Amazon VPC.

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. Tramite l'account di gestione 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 IPv4 CIDR manual input (Input manuale CIDR IPv4) e inserisci un blocco CIDR IPv4. In questo tutorial, utilizziamo 10.0.0.0/20.
5. Ignora l'opzione per l'aggiunta di un blocco CIDR IPv6.
6. Seleziona Crea VPC.
7. Tramite l'account di gestione 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. Tramite l'account di gestione 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 Name tag (Tag nome), 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 eseguire il provisioning di CIDR al pool di pianificazione delle risorse.
9. In CIDR to provision (CIDR di cui eseguire il provisioning), scegli un CIDR VPC di cui eseguire 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 sospenso) 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. Tramite l'account di gestione 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 Name tag (Tag nome), 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. In CIDR to provision (CIDR di cui eseguire il provisioning), scegli un CIDR di cui eseguire il provisioning al 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 denominata "prod-subnet-pool".

A questo punto, se desideri rendere disponibile questo pool di sottoreti ad altri account AWS, puoi condividere il pool di sottoreti. Per istruzioni su come eseguire questa operazione, consulta [Condividi un pool IPAM utilizzando 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. Tramite l'account di gestione 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 IPv4 CIDR block (Blocco CIDR IPv4), scegli IPAM-allocated IPV4 CIDR block (Blocco CIDR IPv4 allocato tramite IPAM), quindi scegli il pool di sottoreti di sviluppo e una maschera di rete /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. Puoi creare pool di sottoreti aggiuntivi in base alle esigenze oppure avviare un'istanza EC2 in una delle sottoreti.

IPAM pubblica le metriche relative all'utilizzo degli indirizzi IP nelle sottoreti. Puoi impostare allarmi CloudWatch sulla metrica SubnetIPUsage, in modo da poter intervenire quando vengono superate le soglie di utilizzo degli IP. Ad esempio, avendo un CIDR /24 (256 indirizzi IP) assegnato a una sottorete, se desideri ricevere una notifica quando è stato utilizzato l'80% degli IP puoi impostare un allarme CloudWatch che ti avvisi quando viene raggiunta tale soglia. 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. Tramite l'account di gestione 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 con i CIDR di cui è stato eseguito il provisioning, anche se i CIDR non proverranno più da un pool IPAM.
6. Scegliere Delete (Elimina).
7. [Elimina le sottoreti](#).
8. [Elimina il VPC](#).

La pulizia è completa.

Identity and Access Management in IPAM

AWS utilizza le credenziali di sicurezza per identificarti e per concederti l'accesso alle risorse AWS. Puoi utilizzare le caratteristiche di AWS Identity and Access Management (IAM) per consentire ad altri utenti, servizi e applicazioni di utilizzare le risorse AWS completamente o in modo limitato, senza condividere le credenziali di sicurezza.

Questa sezione descrive i ruoli collegati al servizio AWS creati specificamente per IPAM e per le policy gestite allegate ai ruoli collegati al servizio 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 su identity and access management di VPC, consulta [Identity and Access Management di Amazon VPC](#) nella Guida per l'utente di Amazon VPC.

Indice

- [Ruoli collegati al servizio per IPAM](#)
- [Policy gestite da AWS per IPAM](#)
- [Policy di esempio](#)

Ruoli collegati al servizio per IPAM

I ruoli collegati al servizio in AWS Identity and Access Management (IAM) abilitano i servizi AWS a chiamare altri servizi AWS per tuo conto. Per ulteriori informazioni sui ruoli collegati al servizio, consulta [Utilizzo dei ruoli collegati al servizio](#) nella Guida per l'utente IAM.

Attualmente esiste un solo ruolo collegato al servizio per IPAM: AWSServiceRoleForIPAM.

Autorizzazioni concesse al ruolo collegato al servizio

IPAM utilizza il ruolo collegato al servizio AWSServiceRoleForIPAM per chiamare le azioni nella policy gestita AWSIPAMServiceRolePolicy. Per ulteriori informazioni sulle operazioni consentite in tale policy, consulta [Policy gestite da AWS per IPAM](#).

Questo ruolo collegato al servizio dispone inoltre di una [policy di attendibilità IAM](#) che autorizza il servizio `ipam.amazonaws.com` ad assumere il ruolo collegato al 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 i relativi CIDR e integrando le risorse con IPAM.

Il ruolo collegato al servizio viene creato in due modi:

- Quando si integra con AWS Organizations

Se si [Integrare IPAM con gli account di un'organizzazione AWS](#) utilizzano la console IPAM o il comando AWS CLI `enable-ipam-organization-admin-account`, il ruolo collegato al servizio `AWSServiceRoleForIPAM` viene creato automaticamente in ciascuno dei propri account membri di AWS Organizations. 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:

- L'Account di gestione di Organizations AWS che consente l'integrazione IPAM con Organizations AWS deve disporre di una policy IAM che consenta di svolgere 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 si [Utilizza IPAM con un singolo account](#), il ruolo collegato al servizio `AWSServiceRoleForIPAM` viene creato automaticamente quando si crea un IPAM come tale account.

Important

Se si utilizza IPAM con un singolo account AWS, prima di creare un IPAM, è necessario assicurarsi che l'account AWS utilizzato abbia una policy IAM collegata che consenta l'operazione `iam:CreateServiceLinkedRole`. Quando si crea l'IPAM, si crea

automaticamente il ruolo collegato di servizio `AWSServiceRoleForIPAM`. Per maggiori informazioni sulla gestione di una policy IAM, consultare [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Modifica del ruolo collegato ai servizi

Non è possibile modificare il ruolo collegato al servizio `AWSServiceRoleForIPAM`.

Eliminazione del ruolo collegato ai servizi

Se non occorre più utilizzare IPAM, è consigliabile eliminare il ruolo collegato al servizio `AWSServiceRoleForIPAM`.

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.

Attenersi alla seguente procedura per eliminare il ruolo collegato al servizio tramite al CLI di AWS:

1. Elimina le risorse IPAM utilizzando [deprovision-ipam-pool-cidr](#) e [delete-ipam](#). Per ulteriori informazioni, consulta [Revoca del provisioning di CIDR da un pool](#) e [Elimina un IPAM](#).
2. Disabilita l'account IPAM con [disable-ipam-organization-admin-account](#).
3. Disabilita il servizio IPAM con [disable-aws-service-access](#) utilizzando 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.

Policy gestite da AWS per IPAM

Se utilizzi IPAM con un singolo account AWS e crei un IPAM, la policy gestita `AWSIPAMServiceRolePolicy` viene creata automaticamente nel tuo account IAM e collegata al [ruolo collegato al servizio](#) `AWSServiceRoleForIPAM`.

Se si abilita l'integrazione IPAM con AWS Organizations, la policy gestita `AWSIPAMServiceRolePolicy` viene creata automaticamente nel proprio account IAM e in ognuno degli account membri di AWS Organizations, e la policy gestita è allegata al ruolo collegato al servizio `AWSServiceRoleForIPAM`.

Questa policy gestita consente a IPAM di eseguire le operazioni seguenti:

- Monitorare i CIDR associati alle risorse di rete EC2 in tutti i membri della tua organizzazione AWS.
- Archiviare i parametri relativi a IPAM in Amazon CloudWatch, come ad esempio lo spazio indirizzi IP disponibile nei pool IPAM e il numero di CIDR di risorse conformi alle regole di assegnazione.

L'esempio che segue mostra i dettagli relativi alle policy gestite create.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAMDiscoveryDescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*"
    }
  ]
}
```



```

    },
    {
      "Sid": "CloudWatchMetricsPublishActions",
      "Effect": "Allow",
      "Action": "cloudwatch:PutMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/IPAM"
        }
      }
    }
  ]
}

```

La prima istruzione nell'esempio precedente consente a IPAM di monitorare i CIDR utilizzati dai singoli account AWS o dai membri della propria AWS Organization.

La seconda istruzione nell'esempio precedente utilizza la chiave di condizione `cloudwatch:PutMetricData` per consentire a IPAM di memorizzare i parametri IPAM nel tuo AWS/IPAM [Spazio dei nomi Amazon CloudWatch](#). Questi parametri sono utilizzati dalla Console di gestione AWS per visualizzare i dati sulle assegnazione nei pool e negli ambiti IPAM. Per ulteriori informazioni, consulta [Monitora l'utilizzo del CIDR con il pannello di controllo IPAM](#).

Aggiornamenti sulla policy gestita da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per IPAM a partire da quando questo servizio ha iniziato a tenere traccia delle modifiche.

Modifica	Descrizione	Data
AWSIPAMServiceRolePolicy	È stata aggiunta un'azione alla policy gestita AWSIPAMServiceRolePolicy (<code>ec2:GetIpamDiscoveredPublicAddresses</code>) per consentire a IPAM l'acquisizione di indirizzi IP pubblici durante il rilevamento delle risorse.	13 novembre 2023

Modifica	Descrizione	Data
AWSIPAMServiceRolePolicy	Sono state aggiunte azioni alla policy gestita AWSIPAMServiceRolePolicy (ec2:DescribeAccountAttributes , ec2:DescribeNetworkInterfaces , ec2:DescribeSecurityGroups , ec2:DescribeSecurityGroupRules , ec2:DescribeVpnConnections , globalaccelerator:ListAccelerators e globalaccelerator:ListByoipCidrs) per consentire a IPAM l'acquisizione di indirizzi IP pubblici durante il rilevamento delle risorse.	1 novembre 2023
AWSIPAMServiceRolePolicy	Sono state aggiunte due azioni alla policy gestita AWSIPAMServiceRolePolicy (ec2:GetIpamDiscoveredAccounts e ec2:GetIpamDiscoveredResourceCidrs) per consentire a IPAM di acquisire gli account AWS e le risorse CIDR in fase di monitoraggio durante il rilevamento delle risorse.	25 gennaio 2023

Modifica	Descrizione	Data
IPAM ha iniziato a monitorare le modifiche	IPAM ha iniziato a monitorare le modifiche per le sue policy gestite da AWS.	2 dicembre 2021

Policy di esempio

La policy presa ad esempio in questa sezione contiene tutte le operazioni AWS Identity and Access Management (IAM) relative all'utilizzo completo di IPAM. In base all'utilizzo di IPAM, potrebbe non essere necessario effettuare tutte le operazioni IAM. Per un'esperienza completa di utilizzo della console IPAM, potrebbe essere necessario aggiungere ulteriori operazioni IAM per servizi quali AWS Organizations, AWS Resource Access Manager (RAM) e Amazon CloudWatch.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIpamByoasn",
        "ec2:DeprovisionIpamByoasn",
        "ec2:DescribeIpamByoasn",
        "ec2:DisassociateIpamByoasn",
        "ec2:ProvisionIpamByoasn",
        "ec2:CreateIpam",
        "ec2:DescribeIpams",
        "ec2:ModifyIpam",
        "ec2>DeleteIpam",
        "ec2:CreateIpamScope",
        "ec2:DescribeIpamScopes",
        "ec2:ModifyIpamScope",
        "ec2>DeleteIpamScope",
        "ec2:CreateIpamPool",
        "ec2:DescribeIpamPools",
        "ec2:ModifyIpamPool",
        "ec2>DeleteIpamPool",
        "ec2:ProvisionIpamPoolCidr",
        "ec2:GetIpamPoolCidrs",
        "ec2:DeprovisionIpamPoolCidr",
```

```

        "ec2:AllocateIpamPoolCidr",
        "ec2:GetIpamPoolAllocations",
        "ec2:ReleaseIpamPoolAllocation",
        "ec2:CreateIpamResourceDiscovery",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:ModifyIpamResourceDiscovery",
        "ec2>DeleteIpamResourceDiscovery",
        "ec2:AssociateIpamResourceDiscovery",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DisassociateIpamResourceDiscovery",
        "ec2:GetIpamResourceCidrs",
        "ec2:ModifyIpamResourceCidr",
        "ec2:GetIpamAddressHistory",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "ipam.amazonaws.com"
        }
    }
}
]
}
}

```

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	Default	Adattabile
Lunghezza della maschera di rete dei blocchi CIDR IPv6 forniti da Amazon	/52	Sì. Contatta il Centro di supporto AWS come descritto in Service Quotas di AWS nei Riferimenti generali di AWS.
Blocchi CIDR IPv6 forniti da Amazon per ogni pool regionale	1	Sì. Contatta il Centro di supporto AWS come descritto in Service Quotas di AWS nei Riferimenti generali di AWS.
Numeri di sistema autonomi (ASN) che puoi portare in IPAM	5	Sì. Contatta il Centro di supporto AWS come descritto in Service Quotas di AWS nei Riferimenti generali di AWS.
CIDR per pool	50	Sì
Amministratori IPAM per organizzazione	1	No
IPAM per Regione	1	No

Nome	Default	Adattabile
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
Parametri di utilizzo delle risorse	50	Sì. Contatta il Centro di supporto AWS come descritto in Service Quotas di AWS nei 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

Questa sezione spiega come visualizzare le informazioni relative ai prezzi e i costi attuali dell'IPAM.

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 correnti 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 console AWS Cost Management all'indirizzo <https://console.aws.amazon.com/cost-management/home>.
2. Avvia Cost Explorer.
3. Filtra per utilizzo IPAM selezionando Tipo di utilizzo e inserendo **IPAddressManager**.
4. Seleziona una o più caselle di controllo. Ciascuna di esse rappresenta una regione AWS diversa.
5. Fare clic su Apply (Applica).

Se, ad esempio, selezioni USE1-IPAddressManager-IP-Hours(Hrs), vedrai il numero di ore IP attive fatturate da IPAM nella regione us-east-1 e il costo. Se, ad esempio, l'utilizzo in ore è 18, potresti avere 1 indirizzo IP attivo per 18 ore, 3 indirizzi IP attivi ciascuno per 6 ore o qualsiasi combinazione di questi per un totale di 18 ore.

Per ulteriori informazioni su AWS Cost Explorer, consulta [Analisi dei costi con AWS Cost Explorer](#) nella Guida per l'utente di AWS Cost Management.

Informazioni correlate

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

- [Best practice di Amazon VPC IP Address Manager](#): un blog AWS 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](#): un blog AWS che introduce 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 blog AWS che spiega come condividere un pool IPAM con gli account di un'unità organizzativa di AWS Organizations.

Cronologia dei documenti per IPAM

La tabella seguente illustra le versioni di IPAM.

Caratteristica	Descrizione	Data di rilascio
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 informazioni sugli IP pubblici in una singola regione. Ora puoi visualizzare Informazioni sugli IP pubblici in tutte le regioni. Inoltre, ora puoi visualizzare 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 monitorare e le metriche correlate agli indirizzi IP a livello di sottorete e VPC.	17 novembre 2023
Bring your own ASN (BYOASN)	Ora puoi portare il tuo Numero di sistema autonomo (ASN) in AWS.	17 novembre 2023
Aggiornamenti delle policy gestite da AWS: aggiornamento a una policy esistente	AWSIPAMServiceRolePolicy attuale aggiornata.	17 novembre 2023
Aggiornamenti delle policy gestite da AWS: aggiornamento a una policy esistente	AWSIPAMServiceRolePolicy attuale aggiornata.	1 novembre 2023
Parametri di utilizzo delle risorse	IPAM ora pubblica i parametri di utilizzo IP per le risorse monitorate da IPAM su Amazon CloudWatch.	2 agosto 2023

Caratteristica	Descrizione	Data di rilascio
Public IP insights	Public IP Insights mostra tutti gli indirizzi IPv4 pubblici utilizzati dai servizi in questa regione all'interno dell'account. Puoi utilizzare queste informazioni per identificare l'utilizzo degli indirizzi IPv4 pubblici e visualizzare i consigli per rilasciare gli indirizzi IP elastici inutilizzati.	28 luglio 2023
Aggiornamenti delle policy gestite da AWS: aggiornamento a una policy esistente	AWSIPAMServiceRolePolicy attuale aggiornata.	25 gennaio 2023
Come integrare IPAM con account esterni alla tua organizzazione	Ora puoi gestire indirizzi IP esterni alla tua organizzazione da un singolo account IPAM e condividere i pool IPAM con gli account di altre organizzazioni AWS.	25 gennaio 2023
Blocco CIDR contiguo IPv6 fornito da Amazon per pool IPAM	Quando crei un pool IPAM nell'ambito pubblico, ora puoi eseguire il provisioning di un blocco CIDR contiguo IPv6 fornito da Amazon nel pool. Per ulteriori informazioni, consulta Come creare pool IPv6 .	25 gennaio 2023
Versione 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.