Administrador de direcciones IP

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: Administrador de direcciones IP

Table of Contents

¿Qué es IPAM?

Amazon VPC IP Address Manager (IPAM) es una característica de VPC que facilita la planificación, el seguimiento y el monitoreo de las direcciones IP de las cargas de trabajo de AWS. Puede utilizar los flujos de trabajo automatizados de IPAM para administrar las direcciones IP de una forma más eficiente.

Puede utilizar IPAM para realizar lo siguiente:

- Organizar el espacio de direcciones IP en dominios de enrutamiento y seguridad
- Monitorear el espacio de direcciones IP en uso así como los recursos que utilizan el espacio en función de las reglas empresariales
- Ver el historial de asignaciones de direcciones IP en su organización
- Asignar los CIDR a las VPC de forma automática mediante reglas empresariales específicas
- Solucionar problemas de conectividad de red
- Habilitar el uso compartido entre regiones y cuentas de sus direcciones de Traer sus propias direcciones IP (BYOIP)
- Aprovisione bloques de CIDR de IPv6 contiguos proporcionados por Amazon en grupos para crear VPC

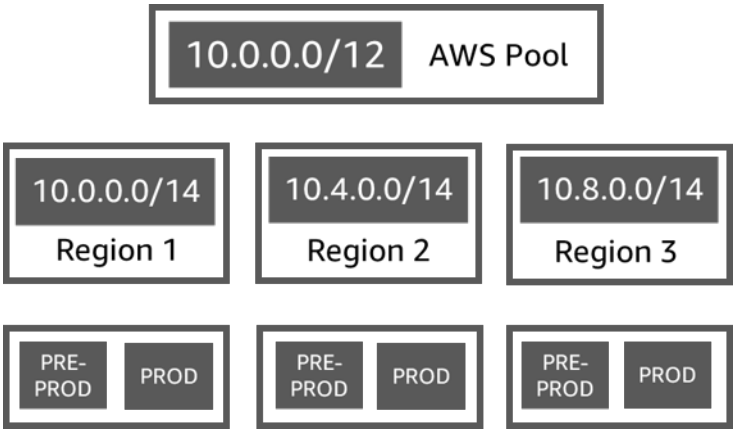
Esta guía contiene las siguientes secciones:

- Cómo funciona IPAM: conceptos y terminología de IPAM.
- Introducción a IPAM: pasos para habilitar la administración de direcciones IP en toda la empresa con AWS Organizations, crear un IPAM y planificar el uso de direcciones IP.
- Administración del espacio de direcciones IP en IPAM: pasos para administrar su IPAM, alcances, grupos y asignaciones.
- Seguimiento del uso de direcciones IP en IPAM: pasos para monitorear y realizar un seguimiento del uso de direcciones IP con IPAM.
- Tutoriales para IP Address Manager de Amazon VPC: Tutoriales detallados paso a paso para crear un IPAM y grupos, asignar CIDR de VPC y traer sus propios CIDR de direcciones IP públicas a IPAM.

Cómo funciona IPAM

En este tema, se explican algunos de los conceptos clave para ayudarlo a comenzar a utilizar IPAM.

En el siguiente diagrama, se muestra una jerarquía de grupos de IPAM para varias regiones de AWS dentro de un grupo de nivel superior de IPAM. Cada grupo regional de AWS incluye dos grupos de desarrollo de IPAM, un grupo para recursos de preproducción y otro para recursos de producción. Para obtener más información acerca de los conceptos de IPAM, consulte las descripciones de debajo del diagrama.



Para utilizar el Administrador de direcciones IP de Amazon VPC (IPAM), primero cree un IPAM.

Cuando crea el IPAM, elija en qué región de AWS se creará. Al crear un IPAM, IPAM de AWS VPC crea automáticamente dos alcances para IPAM. Los alcances, junto con los grupos y las asignaciones, son componentes clave de su IPAM.

- Un alcance es el contenedor de más alto nivel dentro de IPAM. Al crear un IPAM, se crea automáticamente un alcance público predeterminado y otro privado predeterminado para usted. Cada alcance representa el espacio IP de una única red. El alcance privado está destinado a todas las direcciones IP que no se pueden anunciar en la Internet. Por lo general, el alcance público está destinado a todas las direcciones IP que se pueden anunciar en la Internet desde AWS. Tenga en cuenta que al aprovisionar direcciones BYOIPv6 a un grupo de IPAM, puede configurar las direcciones para que no se anuncien públicamente aunque estén en el alcance público. Los alcances le permiten reutilizar las direcciones IP en varias redes no conectadas sin causar superposición o conflicto de direcciones IP. Dentro de un alcance, se crean grupos de IPAM.
- Un grupo es un conjunto de rangos continuos de direcciones IP (o CIDR). Los grupos de IPAM le permiten organizar las direcciones IP según sus necesidades de enrutamiento y seguridad. Puede

tener varios grupos dentro de un grupo de nivel superior. Por ejemplo, si tiene necesidades de enrutamiento y seguridad independientes para las aplicaciones de desarrollo y producción, puede crear un grupo para cada una. Dentro de los grupos de IPAM, se asignan CIDR a los recursos de AWS.

- Una asignación es una asignación de CIDR desde un grupo de IPAM a otro recurso o grupo de IPAM. Cuando crea una VPC y elige un grupo de IPAM para el CIDR de la VPC, el CIDR se asigna desde el CIDR aprovisionado al grupo de IPAM. Puede monitorear y administrar la asignación con IPAM.

IPAM puede administrar y monitorear el espacio IPv6 público y privado. Para más información sobre el direccionamiento IPv6 privado y público, consulte Direcciones IPv6 en la Guía del usuario de Amazon VPC.

Para empezar y crear un IPAM, consulte Introducción a IPAM.

Introducción a IPAM

Siga los pasos en esta sección para comenzar a utilizar IPAM. El objetivo de esta sección es ayudarlo a empezar rápidamente con el IPAM, pero es posible que descubra que lo que puede conseguir con los pasos de esta sección no se ajusta a sus necesidades. Para obtener información sobre las distintas formas de utilizar el IPAM, consulte Planificar el aprovisionamiento de direcciones IP y Tutoriales para IP Address Manager de Amazon VPC.

En esta sección, comenzará por acceder al IPAM y decidir si desea delegar una cuenta del IPAM. Al final de esta sección, habrá creado un IPAM, creado varios grupos de direcciones IP y asignado un CIDR en un grupo a una VPC.

Tareas

- Acceso a IPAM
- Configuración de las opciones de integración para el IPAM
- Creación de un IPAM
- Planificar el aprovisionamiento de direcciones IP
- Asignación de CIDR desde un grupo del IPAM

Acceso a IPAM

Al igual que otros servicios de AWS, puede crear, acceder y administrar su IPAM con los siguientes métodos:

- AWS Management Console: proporciona una interfaz web que se puede utilizar para crear y administrar IPAM. Consulte https://console.aws.amazon.com/ipam/.
- AWS Command Line Interface (AWS CLI): proporciona comandos para un amplio conjunto de servicios de AWS, incluido Amazon VPC. La AWS CLI es compatible con Windows, macOS y Linux. Para obtener AWS CLI, consulte AWS Command Line Interface.
- SDK de AWS: proporcionan API específicas del lenguaje. Los SDK de AWS se ocupan de muchos de los detalles de conexión, como el cálculo de firmas, la gestión de intentos de solicitud y la gestión de errores. Para obtener más información, consulte SDK de AWS.
- API de consulta: proporciona acciones de API de nivel inferior a las que se llama mediante solicitudes HTTPS. Utilizar la API de consulta es la forma más directa de obtener acceso a IPAM. Sin embargo, requiere que la aplicación gestione detalles de nivel inferior, como, por ejemplo, la

generación del hash para firmar la solicitud y la gestión de errores. Para obtener más información, consulte las acciones de Amazon IPAM en la Referencia de la API de Amazon EC2.

Esta guía se centra principalmente en utilizar la AWS Management Console para crear, acceder y administrar su IPAM. En cada descripción de cómo completar un proceso en la consola, incluimos enlaces a la Referencia de comandos de la AWS CLI para que pueda llevar a cabo las mismas tareas con la AWS CLI.

Si es la primera vez que utiliza IPAM, revise Cómo funciona IPAM para obtener información sobre el rol de IPAM en Amazon VPC y luego continúe con las instrucciones de Configuración de las opciones de integración para el IPAM.

Configuración de las opciones de integración para el IPAM

En esta sección, se describen las opciones para integrar el IPAM con AWS Organizations y otras cuentas de AWS o usarlo con una sola cuenta de AWS.

Antes de empezar a utilizar IPAM, debe elegir una de las opciones de esta sección para permitir que IPAM monitoree los CIDR asociados con los recursos de red de EC2 y las métricas de almacenamiento:

- Para permitir que IPAM se integre con AWS Organizations y habilitar el servicio IPAM de Amazon VPC a fin de administrar y monitorear los recursos de red creados por todas las cuentas de miembros de AWS Organizations, consulte Integración de IPAM con cuentas en una organización de AWS.
- Después de realizar la integración con AWS Organizations, para integrar IPAM con cuentas ajenas a su organización, consulte Integración de IPAM con cuentas ajenas a su organización.
- Para utilizar una cuenta única de AWS con IPAM y habilitar el servicio IPAM de Amazon VPC a fin de administrar y monitorear los recursos de red que crea con la cuenta única, consulte Utilizar IPAM con una sola cuenta.

Si no elige una de estas opciones, puede seguir creando recursos de IPAM, como grupos, pero no verá métricas en el panel y no podrá monitorear el estado de los recursos.

Contenido

- Utilizar IPAM con una sola cuenta

Integración de IPAM con cuentas en una organización de AWS

Opcionalmente, puede seguir los pasos de esta sección para integrar IPAM con AWS Organizations y delegar una cuenta de miembro como la cuenta de IPAM.

La cuenta de IPAM es responsable de crear un IPAM y utilizarlo para administrar y monitorear el uso de direcciones IP.

La integración de IPAM con AWS Organizations y la delegación de un administrador de IPAM presentan los siguientes beneficios:

- Comparta los grupos de IPAM con su organización: cuando delega una cuenta de IPAM, IPAM habilita otras cuentas de miembro de AWS Organizations en la organización para asignar CIDR de grupos de IPAM que se comparten mediante el uso de AWS Resource Access Manager (RAM). Para obtener más información acerca de la configuración de una organización, consulte ¿Qué es AWS Organizations? en la Guía del usuario de AWS Organizations.
- Monitoree el uso de direcciones IP en su organización: cuando delega una cuenta de IPAM, concede permiso a IPAM para monitorear el uso de IP en todas sus cuentas. Como resultado, IPAM importa automáticamente los CIDR que utilizan las VPC existentes en otras cuentas de miembro de AWS Organizations en IPAM.

Si no delega una cuenta de miembro de AWS Organizations como cuenta de IPAM, IPAM monitoreará los recursos solo en la cuenta de AWS que utiliza para crear el IPAM.

> **Note**
>
> Al integrarse con AWS Organizations:
>
> - Debe habilitar la integración con AWS Organizations mediante el uso de IPAM en la consola de administración de AWS o mediante el comando de la AWS CLI enable-ipam-organization-admin-account. Esto garantiza que se cree el rol `AWSServiceRoleForIPAM` vinculado al servicio. Si habilita el acceso de confianza con AWS Organizations mediante la consola de AWS Organizations o mediante el comando de la AWS CLI register-delegated-administrator, el rol `AWSServiceRoleForIPAM` vinculado al servicio no se crea y no puede administrar ni supervisar recursos dentro de su organización.

- La cuenta del IPAM debe ser una cuenta de miembro de AWS Organizations. No puede usar la cuenta de administración de AWS Organizations como cuenta de IPAM. Para comprobar si su IPAM ya está integrado con AWS Organizations, siga los pasos que se indican a continuación y consulte los detalles de la integración en Configuración de la organización.
- IPAM le cobra por cada dirección IP activa que monitorea en las cuentas de miembro de su organización. Para obtener más información acerca de los precios, consulte Precios de IPAM.
- Debe tener una cuenta en AWS Organizations y una cuenta de administración configurada con una o varias cuentas de miembro. Para obtener más información sobre los tipos de cuenta, consulte Conceptos y terminología en la Guía del usuario de AWS Organizations. Para obtener más información sobre la configuración de una organización, consulte Introducción a AWS Organizations.
- La cuenta de IPAM debe utilizar un rol de IAM que tenga asociada una política de IAM que permita la acción `iam:CreateServiceLinkedRole`. Al crear la IPAM, se crea automáticamente el rol vinculado a servicios AWSServiceRoleForIPAM.
- El usuario asociado a la cuenta de administración de AWS Organizations debe utilizar un rol de IAM que tenga asociadas las siguientes acciones de política de IAM:
  - `ec2:EnableIpamOrganizationAdminAccount`
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator`
  - `iam:CreateServiceLinkedRole`

  Para obtener más información acerca de la creación de roles de IAM, consulte Creación de un rol para delegar permisos a un usuario de IAM en la Guía del usuario de IAM.
- El usuario asociado a la cuenta de administración de Organizations AWS debe utilizar un rol de IAM que tenga asociadas las siguientes acciones de política de IAM adjuntas para enumerar tus actuales administradores delegados de AWS Orgs: `organizations:ListDelegatedAdministrators`

AWS Management Console

Para seleccionar una cuenta de IPAM

1. Utilizando la cuenta de administración de AWS Organizations, abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En la AWS Management Console, elija la región de AWS en la que desea trabajar con IPAM.
3. En el panel de navegación, elija Configuración de la organización.
4. La opción Delegar solo está disponible si ha iniciado sesión en la consola como la cuenta de administración de AWS Organizations. Elija Delegar.
5. Ingrese el ID de cuenta de AWS para una cuenta de IPAM. El administrador de IPAM debe ser una cuenta de miembro de AWS Organizations.
6. Seleccione Save changes (Guardar cambios).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

- Para delegar una cuenta de administrador de IPAM mediante la AWS CLI, utilice el siguiente comando: enable-ipam-organization-admin-account.

Cuando delega una cuenta de miembro de Organizations como una cuenta de IPAM, IPAM crea automáticamente un rol de IAM vinculado al servicio en todas las cuentas de miembro de su organización. IPAM monitorea el uso de direcciones IP en estas cuentas asumiendo el rol de IAM vinculado al servicio en cada cuenta de miembro, descubre los recursos y sus CIDR, y los integra con IPAM. IPAM podrá detectar los recursos de todas las cuentas de miembro, independientemente de su unidad organizativa. Si hay cuentas de miembro que han creado una VPC, por ejemplo, verá la VPC y su CIDR en la sección Resources (Recursos) de la consola de IPAM.

> **Important**
>
> El rol de la cuenta de administración de AWS Organizations que delegó el administrador de IPAM ya está completo. Para seguir utilizando IPAM, la cuenta de administrador de IPAM debe iniciar sesión en Amazon VPC IPAM y crear un IPAM.

Integración de IPAM con cuentas ajenas a su organización

En esta sección, se describe cómo integrar su IPAM con cuentas de AWS ajenas a su organización. Para completar los pasos en esta sección, debe haber completado los pasos de Integración de IPAM con cuentas en una organización de AWS y haber delegado una cuenta de IPAM.

La integración de IPAM con cuentas de AWS ajenas a su organización le permite hacer lo siguiente:

- Administrar direcciones IP ajenas a su organización desde una única cuenta de IPAM.
- Compartir grupos de IPAM con servicios de terceros alojados en otras cuentas de AWS en otras AWS Organizations.

Tras integrar IPAM con cuentas de AWS ajenas a su organización, puede compartir un grupo de IPAM directamente con las cuentas que desee de otras organizaciones.

Contenido

Condiciones y limitaciones

Esta sección contiene consideraciones y limitaciones para integrar IPAM con cuentas ajenas a su organización:

- Cuando comparte una detección de recursos con otra cuenta, los únicos datos que se intercambian son los datos de monitoreo de la dirección IP y el estado de la cuenta. Puede ver estos datos antes de compartirlos mediante los comandos de la CLI get-ipam-discovered-resource-cidrs y get-ipam-discovered-accounts o las API GetIpamDiscoveredResourceCidrs y GetIpamDiscoveredAccounts. En el caso de las detecciones de recursos que monitorean los recursos de una organización, no se comparte ningún dato de la organización (como los nombres de las unidades organizativas de la organización).
- Al crear una detección de recursos, la detección de recursos monitorea todos los recursos visibles de la cuenta del propietario. Si la cuenta del propietario es una cuenta de AWS de servicio de terceros que crea recursos para varios de sus propios clientes, la detección de recursos detectará esos recursos. Si la cuenta de AWS de servicio de terceros comparte la detección de recursos con una cuenta de AWS de usuario final, el usuario final tendrá visibilidad de los recursos de los demás clientes del servicio de AWS de terceros. Por ese motivo, el servicio de AWS de terceros

debe tener cuidado al crear y compartir detecciones de recursos o utilizar una cuenta de AWS independiente para cada cliente.

Información general del proceso

En esta sección, se explica cómo integrar su IPAM con cuentas de AWS ajenas a su organización. Se hace referencia a temas que se tratan en otras secciones de esta guía. Mantenga esta página visible y abra los temas enlazados a continuación en una ventana nueva para regresar a esta página y obtener orientación.

Al integrar IPAM con cuentas de AWS ajenas a su organización, hay cuatro cuentas de AWS involucradas en el proceso:

- Propietario de la organización principal: la cuenta de administración de AWS Organizations para la organización 1.
- Cuenta de IPAM de la organización principal: la cuenta de administrador delegada de IPAM para la organización 1.
- Propietario de la organización secundaria: la cuenta de administración de AWS Organizations para la organización 2.
- Cuenta de administrador de la organización secundaria: la cuenta de administrador delegada de IPAM para la organización 2.

Pasos

1. El propietario de la organización principal delega a un miembro de su organización como cuenta de IPAM de la organización principal (consulte Integración de IPAM con cuentas en una organización de AWS).
2. La cuenta de IPAM de la organización principal crea un IPAM (consulte Creación de un IPAM).
3. El propietario de la organización secundaria delega a un miembro de su organización como cuenta de administrador de la organización secundaria (consulte Integración de IPAM con cuentas en una organización de AWS).
4. La cuenta de administrador de la organización secundaria crea una detección de recursos y la comparte con la cuenta de IPAM de la organización principal mediante AWS RAM (consulte Creación de una detección de recursos para integrarla con otro IPAM y Uso compartido de una detección de recursos con otra cuenta de AWS). La detección de recursos debe crearse en la misma región de origen que el IPAM de la organización principal.

5. La cuenta de IPAM de la organización principal acepta la invitación a compartir recursos mediante AWS RAM (consulte Aceptar y rechazar invitaciones para compartir recursos en la Guía del usuario de AWS RAM).
6. La cuenta de IPAM de la organización principal asocia la detección de recursos a su IPAM (consulte Asociación de una detección de recursos a un IPAM).
7. La cuenta de IPAM de la organización principal ahora puede monitorear o administrar los recursos de IPAM creados por las cuentas de la organización secundaria.
8. (Opcional) La cuenta de IPAM de la organización principal comparte los grupos de IPAM con las cuentas de los miembros de la organización secundaria (consulte Compartir un grupo de IPAM mediante AWS RAM).
9. (Opcional) Si la cuenta de IPAM de la organización principal quiere dejar de detectar recursos en la organización secundaria, puede desasociar la detección de recursos del IPAM (consulte Desasociación de una detección de recursos).
10. (Opcional) Si la cuenta de administrador de la organización secundaria quiere dejar de participar en el IPAM de la organización principal, puede dejar de compartir la detección de recursos compartidos (consulte Actualizar un recurso compartido en AWS RAM en la Guía del usuario de AWS RAM) o eliminar la detección de recursos (consulte Eliminación de una detección de recursos).

Utilizar IPAM con una sola cuenta

Si elige no Integración de IPAM con cuentas en una organización de AWS, puede utilizar IPAM con una sola cuenta de AWS.

Cuando crea un IPAM en la siguiente sección, se crea automáticamente un rol vinculado a servicios del IPAM de Amazon VPC en AWS Identity and Access Management (IAM).

Los roles vinculados a servicios son un tipo de rol de IAM que permite que los servicios de AWS accedan a otros servicios de AWS en su nombre. Simplifican el proceso de administración de permisos al crear y administrar automáticamente los permisos necesarios para que los servicios de AWS específicos lleven a cabo las acciones necesarias, lo que agiliza la configuración y la administración de estos servicios.

IPAM utiliza el rol vinculado a servicios para supervisar y almacenar métricas de los CIDR asociados a los recursos de las redes de EC2. Para obtener más información sobre el rol vinculado a servicios y cómo lo utiliza IPAM, consulte Roles vinculados a servicios para IPAM.

> **Important**
>
> Si utiliza IPAM con una sola cuenta de AWS, debe asegurarse de que la cuenta de AWS que utilice para crear el IPAM emplee un rol de IAM con una política asociada a él que permita la acción `iam:CreateServiceLinkedRole`. Al crear el IPAM, se crea automáticamente el rol vinculado a servicios AWSServiceRoleForIPAM. Para obtener más información sobre la administración de las políticas de IAM, consulte Edición de políticas de IAM en la Guía del usuario de IAM.

Una vez que una sola cuenta de AWS tiene permiso de crear el rol vinculado a servicios de IPAM, vaya a Creación de un IPAM.

Creación de un IPAM

Siga los pasos de esta sección para crear un IPAM. Si ha delegado un administrador de IPAM, se deben completar estos pasos para la cuenta de IPAM.

> **Important**
>
> Al crear un IPAM, se le pedirá que permita a IPAM replicar datos de cuentas de origen en una cuenta delegada de IPAM. Para integrar IPAM con AWS Organizations, IPAM necesita su permiso para replicar detalles del uso de recursos e IP en todas las cuentas (desde cuentas de miembro hasta la cuenta delegada de miembro de IPAM) y en las regiones de AWS (desde regiones operativas hasta la región de origen de su IPAM). Para los usuarios de IPAM de cuenta única, IPAM necesita su permiso para replicar los detalles del uso de recursos e IP en las regiones operativas a la región de origen de su IPAM.

Cuando crea el IPAM, elige las regiones de AWS en las que el IPAM puede administrar los CIDR de direcciones IP. Estas regiones de AWS se denominan regiones operativas. IPAM descubre y monitorea los recursos solo en las regiones de AWS que selecciona como regiones operativas. IPAM no almacena ningún dato fuera de las regiones operativas seleccionadas.

El siguiente ejemplo de jerarquía muestra cómo las regiones de AWS que asigna al crear el IPAM afectarán a las regiones que estarán disponibles para los grupos que cree más adelante.

- IPAM que opera en la región 1 de AWS y la región 2 de AWS

- Alcance privado
  - Grupo de IPAM de nivel superior
    - Grupo regional de IPAM en la región 2 de AWS
      - Grupo de desarrollo
        - Asignación de una VPC en la región 2 de AWS

Solo puede crear un IPAM. Para obtener más información sobre el aumento de las cuotas relacionadas con el IPAM, consulte Cuotas de IPAM.

AWS Management Console

Para crear un IPAM

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En la AWS Management Console, elija la región de AWS en la que desea crear el IPAM. Cree el IPAM en su región principal de operaciones.
3. En la página de inicio del servicio, elija Create IPAM (Crear IPAM).
4. Seleccione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir al Administrador de direcciones IP de Amazon VPC replicar los datos de las cuentas de origen en la cuenta delegada de IPAM). Si no selecciona esta opción, no puede crear un IPAM.
5. Elija un Nivel de IPAM. Para obtener más información sobre las características disponibles en cada nivel y los costos asociados a los niveles, consulte la pestaña de IPAM en la Página de precios de Amazon VPC.
6. En Operating regions (Regiones operativas), seleccione las regiones de AWS en las que este IPAM puede administrar y descubrir recursos. La región de AWS en la que va a crear su IPAM se selecciona como una de las regiones operativas de forma predeterminada. Por ejemplo, si va a crear este IPAM en la región `us-east-1` de AWS, pero desea crear grupos de IPAM regionales más adelante que proporcionen CIDR a las VPC en `us-west-2`, seleccione `us-west-2` aquí. Si olvida una región operativa, puede volver más adelante y editar la configuración del IPAM.

> **Note**
>
> Si crea un IPAM en el nivel gratuito, puede seleccionar varias regiones operativas para su IPAM, pero la única característica de IPAM que se encontrará disponible en todas las regiones operativas es Información sobre IP públicas. No puede utilizar otras características del nivel gratuito, como BYOIP, en todas las regiones operativas del IPAM. Solo puede utilizarlas en la región de origen del IPAM. Para utilizar todas las características del IPAM en todas las regiones operativas, cree un IPAM en el nivel avanzado.

7. Elija si desea habilitar los CIDR GUA de IPv6 privados. Para obtener más información acerca de esta opción, consulta Habilitar el aprovisionamiento de CIDR GUA IPv6 privados.
8. Elija si desea activar el modo de medición. Para obtener más información acerca de esta opción, consulta Habilitar distribución de costos.
9. Elija Create IPAM (Crear IPAM).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear, modificar y ver los detalles relacionados con su IPAM:

1. Para crear el IPAM: create-ipam.
2. Para ver el IPAM que ha creado: describe-ipams.
3. Para ver los alcances que se crean automáticamente: describe-ipam-scopes.
4. Para modificar un IPAM existente: modify-ipam.

Cuando haya completado estos pasos, el IPAM habrá hecho lo siguiente:

- Ha creado su IPAM. Puede ver el IPAM y las regiones operativas seleccionadas actualmente al elegir los IPAM en el panel de navegación izquierdo de la consola.

- Se creó un alcance privado y otro público. Puede ver los alcances al seleccionar Scopes (Alcances) en el panel de navegación. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.

Planificar el aprovisionamiento de direcciones IP

Siga los pasos de esta sección para planificar el aprovisionamiento de direcciones IP mediante grupos de IPAM. Si ha configurado una cuenta de IPAM, dicha cuenta debe completar estos pasos. El proceso de creación de grupos varía de acuerdo al ámbito público o privado de los grupos. En esta sección se detallan los pasos para crear un grupo regional en el ámbito privado. Para ver tutoriales sobre BYOIP y BYOASN, consulte Tutoriales.

> **Important**
>
> Para utilizar los grupos de IPAM en todas las cuentas de AWS, debe integrar IPAM con AWS Organizations o, de lo contrario, es posible que algunas características no funcionen correctamente. Para obtener más información, consulte Integración de IPAM con cuentas en una organización de AWS.

En IPAM, un grupo es un conjunto de rangos de direcciones IP contiguos (o CIDR). Los grupos le permiten organizar las direcciones IP según sus necesidades de enrutamiento y seguridad. Puede crear grupos para regiones de AWS fuera de la región de IPAM. Por ejemplo, si tiene necesidades de enrutamiento y seguridad independientes para las aplicaciones de desarrollo y producción, puede crear un grupo para cada una.

En el primer paso de esta sección, creará un grupo de nivel superior. A continuación, creará un grupo regional dentro del grupo de nivel superior. Dentro del grupo regional, puede crear grupos adicionales según sea necesario, como grupos de entornos de producción y desarrollo. De forma predeterminada, puede crear grupos de hasta diez unidades. Para obtener información sobre las cuotas de IPAM, consulte Cuotas de IPAM.

> **Note**
>
> A lo largo de esta guía del usuario y en la consola de IPAM se utilizan los términos aprovisionar y asignar. Aprovisionar se utiliza cuando se agrega un CIDR a un grupo de IPAM. Asignar se utiliza cuando asocia un CIDR desde un grupo de IPAM a un recurso.

A continuación, se muestra un ejemplo de jerarquía de la estructura de grupos que creará al completar los pasos de esta sección:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Alcance privado
    - Grupo de nivel superior
      - Grupo regional en la región 1 de AWS
        - Grupo de desarrollo
          - Asignación para una VPC

Esta estructura sirve como ejemplo de cómo podría querer utilizar IPAM, pero puede hacerlo de modo que se adapte a las necesidades de su organización. Para obtener más información sobre las prácticas recomendadas, consulte las Prácticas recomendadas del administrador de direcciones IP de Amazon VPC.

Si va a crear un único grupo de IPAM, complete los pasos de Creación de un grupo IPv4 de nivel superior y, a continuación, vaya a Asignación de CIDR desde un grupo del IPAM.

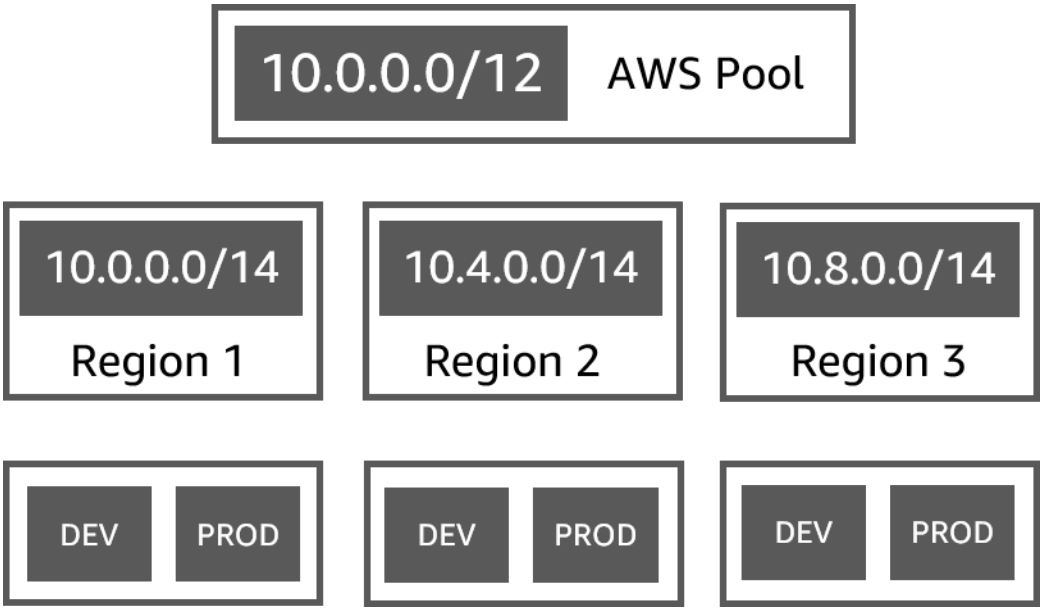
Contenido

Ejemplos de planes de grupos de IPAM

Puede utilizar IPAM de modo que se adapte a las necesidades de su organización. En esta sección, se proporcionan ejemplos de cómo organizar las direcciones IP.

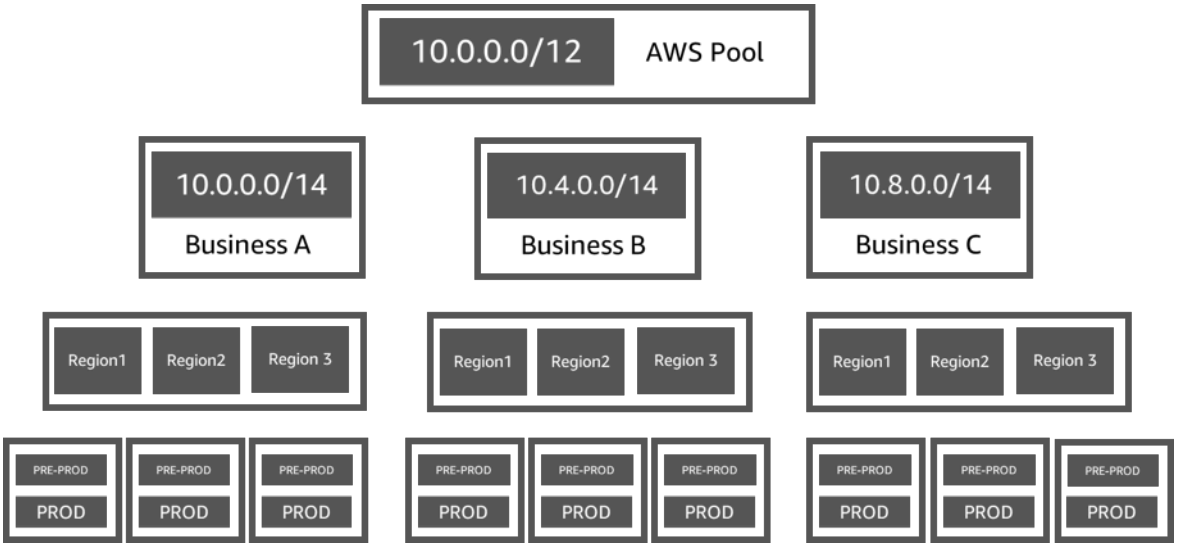
Grupos IPv4 en varias regiones de AWS

En el siguiente ejemplo, se muestra una jerarquía de grupos de IPAM para varias regiones de AWS dentro de un grupo de nivel superior. Cada grupo regional de AWS incluye dos grupos de desarrollo de IPAM, un grupo para recursos de desarrollo y otro para recursos de producción.



Grupos IPv4 para varias líneas de negocio

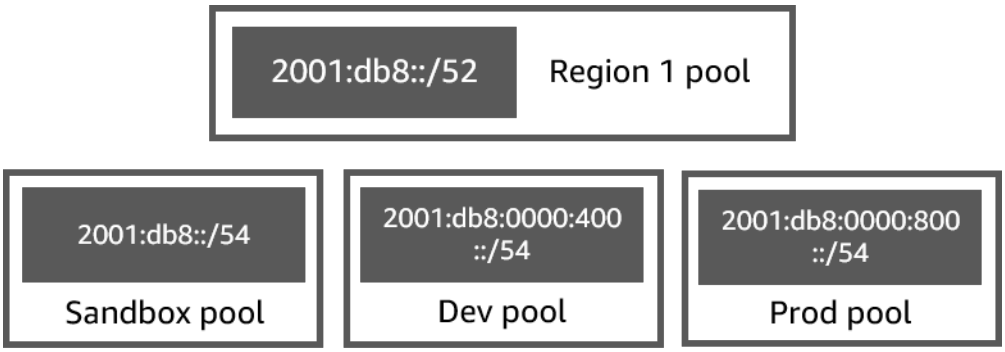
En el siguiente ejemplo, se muestra una jerarquía de grupos de IPAM para varias líneas de negocio dentro de un grupo de nivel superior. Cada grupo de cada línea de negocio contiene tres grupos regionales de AWS. Cada grupo regional incluye dos grupos de desarrollo de IPAM, un grupo para recursos de preproducción y otro para recursos de producción.



Grupos IPv6 en una región de AWS

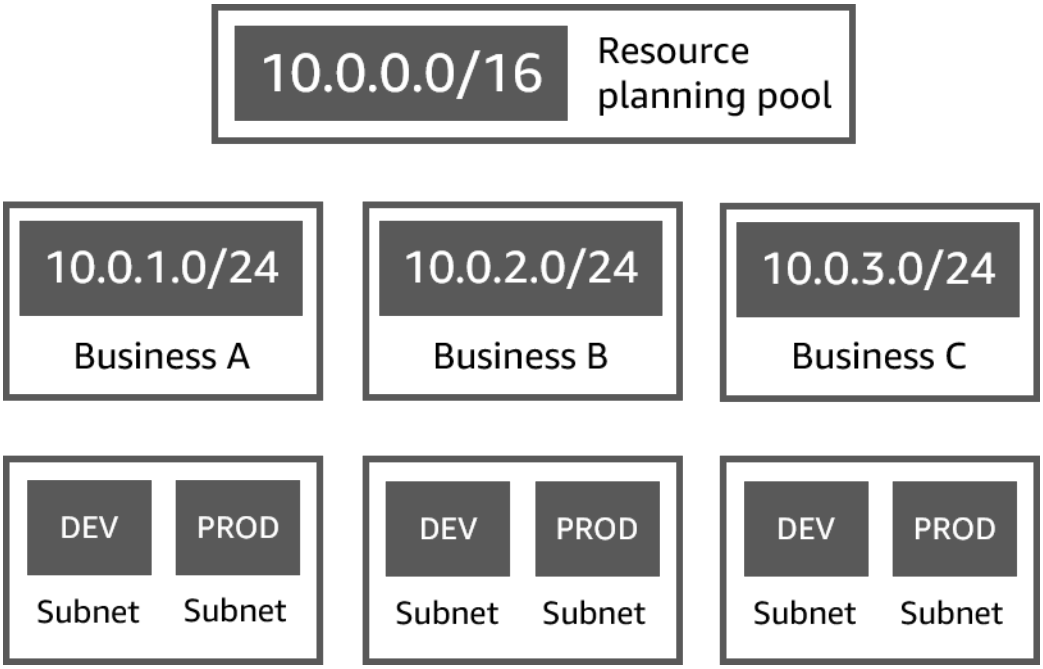
En el siguiente ejemplo, se muestra una jerarquía de grupos de IPAM de IPv6 para varias líneas de negocio dentro de un grupo regional. Cada grupo regional incluye tres grupos de IPAM, un grupo

para recursos de entorno aislado, un grupo para recursos de desarrollo y otro para recursos de producción.



Grupos de subredes para varias líneas de negocio

En el siguiente ejemplo, se muestra una jerarquía de grupos de planificación de recursos para varias líneas de negocio y grupos de subredes de desarrollo y producción. Para obtener más información sobre la planificación del espacio de direcciones IP de subred mediante el IPAM, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.



Creación de grupos IPv4

Siga los pasos de esta sección para crear una jerarquía de grupos de IPAM de IPv4.

El siguiente ejemplo muestra la jerarquía de la estructura de grupos que puede crear al seguir las instrucciones de esta guía. En esta sección, creará una jerarquía de grupos de IPAM de IPv4:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Alcance privado
    - Grupo de nivel superior (10.0.0.0/8)
      - Grupo regional en: región 2 de AWS (10.0.0.0/16)
        - Grupo de desarrollo (10.0.0.0/24)
          - Asignación para una VPC (10.0.0.0/25)

En el caso anterior, los CIDR utilizados son solo ejemplos. Ilustran que cada grupo dentro del grupo de nivel superior se aprovisiona con una parte del CIDR de nivel superior.

Contenido

Creación de un grupo IPv4 de nivel superior

Siga los pasos de esta sección para crear un grupo de IPAM de IPv4 de nivel superior. Al crear el grupo, aprovisiona un CIDR para que el grupo lo utilice. A continuación, asigne ese espacio a una asignación. Una asignación es una asignación de CIDR desde un grupo de IPAM a otro recurso o grupo de IPAM.

El siguiente ejemplo muestra la jerarquía de la estructura de grupos que puede crear al seguir las instrucciones de esta guía. En este paso, va a crear un grupo de IPAM de nivel superior:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Alcance privado
    - Grupo de nivel superior (10.0.0.0/8)
      - Grupo regional en: región 1 de AWS (10.0.0.0/16)
        - Grupo de desarrollo para las VPC que no son de producción (10.0.0.0/24)
          - Asignación para una VPC (10.0.0.0/25)

En el caso anterior, los CIDR utilizados son solo ejemplos. Ilustran que cada grupo dentro del grupo de nivel superior se aprovisiona con una parte del CIDR de nivel superior.

Al crear un grupo de IPAM, puede configurar reglas para las asignaciones que se realizan dentro del grupo de IPAM.

Las reglas de asignación permiten configurar lo siguiente:

- Si IPAM debe importar automáticamente CIDR en el grupo de IPAM si los encuentra dentro del rango de CIDR de este grupo
- La longitud de máscara de red necesaria para las asignaciones dentro del grupo
- Las etiquetas necesarias para los recursos del grupo
- La configuración regional necesaria para los recursos del grupo. La configuración regional es la región de AWS en la que el grupo de IPAM está disponible para asignaciones.

Las reglas de asignación determinan si los recursos son conformes o no. Para obtener más información sobre la conformidad, consulte Monitorear el uso de CIDR por recurso.

> **Important**
>
> Hay una regla implícita adicional que no se muestra en las reglas de asignación. Si el recurso se encuentra en un grupo de IPAM que es un recurso compartido en el AWS Resource Access Manager (RAM), el propietario del recurso debe configurarse como maestro en AWS RAM. Para obtener más información acerca de compartir grupos con RAM, consulte Compartir un grupo de IPAM mediante AWS RAM.

El siguiente ejemplo muestra cómo puede utilizar reglas de asignación para controlar el acceso a un grupo de IPAM:

Example

Cuando crea los grupos en función de las necesidades de enrutamiento y seguridad, es posible que desee permitir que solo ciertos recursos utilicen un grupo. En tales casos, puede establecer una regla de asignación en la que se indique que cualquier recurso que desee un CIDR de este grupo debe tener una etiqueta que coincida con los requisitos de etiqueta de la regla de asignación. Por ejemplo, puede establecer una regla de asignación que indique que solo las VPC con la etiqueta prod pueden obtener CIDR desde un grupo de IPAM. También podría establecer una regla que indique que los CIDR asignados desde este grupo no pueden ser superiores a /24. En este caso, crear un recurso con un CIDR más grande que /24 de este grupo viola una regla de asignación en

el grupo y la creación falla. Los recursos existentes con un CIDR superior a /24 se marcan como no conformes.

> **Important**
>
> En este tema, se explica cómo crear un grupo IPv4 de nivel superior con un rango de direcciones IP proporcionado por AWS. Si desea usar su propio rango de direcciones IPv4 en AWS (BYOIP), existen requisitos previos. Para obtener más información, consulte Tutorial: incorpore sus direcciones IP a IPAM.

AWS Management Console

Para crear un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Elija Create pool (Crear grupo).
4. En Alcance de IPAM, elija el alcance privado que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.

   De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Los grupos del alcance privado deben ser grupos IPv4. Los grupos del alcance público pueden ser grupos IPv4 o IPv6. El alcance público está destinado a todo el espacio público.
5. (Opcional) Agregue una etiqueta de nombre y una descripción para el grupo.
6. En Origen, elija Alcance del IPAM.
7. En Address family (Familia de direcciones), elija IPv4.
8. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
9. Para Locale (Configuración regional), elija None (Ninguna). Establecerá la configuración regional en el grupo regional.

   La configuración regional es la región de AWS en la que desea que este grupo de IPAM esté disponible para asignaciones. Por ejemplo, solo puede asignar un CIDR para una VPC

desde un grupo de IPAM que comparte una configuración regional con la región de la VPC. Tenga en cuenta que, una vez elegida la configuración regional para un grupo, no puede modificarla. Si la región de origen de IPAM no está disponible debido a una interrupción y el grupo tiene una configuración regional diferente a la región de origen de IPAM, el grupo aún se puede usar para asignar direcciones IP.

10. (Opcional) Puede crear un grupo sin un CIDR, pero no podrá utilizar el grupo para asignaciones hasta que le haya aprovisionado un CIDR. Para aprovisionar un CIDR, elija Agregar CIDR nuevo. Ingrese un CIDR de IPv4 para aprovisionar en el grupo. Si desea usar su propio rango de direcciones IP IPv4 o IPv6 en AWS, existen requisitos previos. Para obtener más información, consulte Tutorial: incorpore sus direcciones IP a IPAM.
11. Elija reglas de asignación opcionales para este grupo:

    - Automatically import discovered resources (Importar automáticamente recursos detectados): esta opción no está disponible si Locale (Configuración regional) tiene el valor None (Ninguna). Si se selecciona, IPAM buscará continuamente recursos dentro del rango de CIDR de este grupo y los importará automáticamente como asignaciones al IPAM. Tenga en cuenta lo siguiente:
      - Los CIDR que se asignarán a estos recursos no se deben haber asignado previamente a otros recursos para que la importación se realice correctamente.
      - IPAM importará un CIDR independientemente de si cumple o no con las reglas de asignación del grupo, de modo que un recurso podría importarse y marcarse posteriormente como no conforme.
      - Si IPAM detecta varios CIDR que se superponen, importará únicamente el CIDR más grande.
      - Si IPAM detecta varios CIDR con CIDR que coinciden, IPAM importará solo uno de ellos aleatoriamente.

      ⚠ Warning
      - Después de crear un IPAM, cuando cree una VPC, elija la opción de bloque de CIDR asignado por IPAM. Si no lo hace, es posible que el CIDR que elija para su VPC se superponga con una asignación de CIDR de IPAM.
      - Si ya se asignó una VPC en un grupo de IPAM, no se podrá importar de manera automática una VPC con un CIDR que se superponga. Por ejemplo, si hay una VPC con un CIDR 10.0.0.0/26 asignado en un grupo de IPAM, no se podrá importar una VPC con un CIDR 10.0.0.0/23 (que cubriría el CIDR 10.0.0.0/26).

- Las asignaciones de CIDR de VPC existentes tardan un tiempo en importarse de manera automática a IPAM.

- Minimum netmask length (Longitud mínima de la máscara de red): la longitud mínima de la máscara de red requerida para que las asignaciones de CIDR en este grupo de IPAM sean conformes y para el bloque de CIDR de mayor tamaño que se puede asignar desde el grupo. La longitud mínima de la máscara de red debe ser inferior a su longitud máxima. Las longitudes de máscara de red posibles para las direcciones IPv4 van de 0 a 32. Las longitudes de máscara de red posibles para las direcciones IPv6 van de 0 a 128.
- Default netmask length (Longitud predeterminada de la máscara de red): longitud predeterminada de la máscara de red para las asignaciones agregadas a este grupo. Por ejemplo, si el CIDR que se aprovisiona para este grupo es **`10.0.0.0/8`** e ingresa **`16`** aquí, cualquier asignación nueva en este grupo tendrá por defecto una longitud de máscara de red de /16.
- Maximum netmask length (Longitud máxima de la máscara de red): longitud máxima de la máscara de red que se requerirá para las asignaciones de CIDR en este grupo. Este valor determina el bloque de CIDR de menor tamaño que se puede asignar desde el grupo.
- Tagging requirements (Requisitos de etiquetado): las etiquetas necesarias para que los recursos asignen espacio del grupo. Si los recursos cambian sus etiquetas después de haber asignado espacio o si se modifican las reglas de etiquetado de asignación en el grupo, el recurso puede marcarse como no conforme.
- Locale (Configuración regional): la configuración regional que se requerirá para los recursos que utilizan CIDR de este grupo. Los recursos importados automáticamente que no tengan esta configuración regional se marcarán como no conformes. Los recursos que no se importan automáticamente al grupo no podrán asignar espacio desde el grupo a menos que se encuentren en esta configuración regional.

> **Note**
>
> Las reglas de asignación se aplican solo a los recursos administrados dentro de ese grupo. Las reglas no se aplican a los recursos de los grupos dentro de un grupo.

12. (Opcional) Elija Tags (Etiquetas) para el grupo.
13. Elija Create pool (Crear grupo).
14. Consulte Creación de un grupo regional de IPv4.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear o editar un grupo de nivel superior en su IPAM:

1. Para crear un grupo: create-ipam-pool.
2. Para editar el grupo después de crearlo a fin de modificar las reglas de asignación: modify-ipam-pool.

Creación de un grupo regional de IPv4

Siga los pasos de esta sección para crear un grupo regional dentro de su grupo de nivel superior. Si solo necesita un grupo de nivel superior, y no necesita grupos de desarrollo o regionales adicionales, diríjase a Asignación de CIDR desde un grupo del IPAM.

> **Note**
>
> El proceso de creación de grupos varía de acuerdo al ámbito público o privado de los grupos. En esta sección se detallan los pasos para crear un grupo regional en el ámbito privado. Para ver tutoriales sobre BYOIP y BYOASN, consulte Tutoriales.

El siguiente ejemplo muestra la jerarquía de la estructura de grupos que crea al seguir las instrucciones de esta guía. En este paso, va a crear un grupo de IPAM regional:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Alcance privado
    - Grupo de nivel superior (10.0.0.0/8)
      - Grupo regional en la región 1 de AWS (10.0.0.0/16)
        - Grupo de desarrollo para las VPC que no son de producción (10.0.0.0/24)
          - Asignación para una VPC (10.0.0.0/25)

En el caso anterior, los CIDR utilizados son solo ejemplos. Ilustran que cada grupo dentro del grupo de nivel superior se aprovisiona con una parte del CIDR de nivel superior.

AWS Management Console

Para crear un grupo regional dentro de un grupo de nivel superior

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Elija Create pool (Crear grupo).
4. En Alcance de IPAM, elija el mismo alcance que utilizó cuando creó el grupo de nivel superior. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
5. (Opcional) Agregue una etiqueta de nombre y una descripción para el grupo.
6. En Origen, elija Grupo de IPAM. A continuación, elija el grupo de nivel superior que ha creado en la sección anterior.
7. Si va a crear este grupo en el alcance público, verá la opción Familia de direcciones. Elija IPv4.
8. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
9. Elija la configuración regional del grupo. La elección de una configuración regional garantiza que no haya dependencias entre regiones entre su grupo y los recursos que se asignan desde él. Las opciones disponibles proceden de las regiones operativas que eligió al crear su IPAM.

   La configuración regional es la región de AWS en la que desea que este grupo de IPAM esté disponible para asignaciones. Por ejemplo, solo puede asignar un CIDR para una VPC desde un grupo de IPAM que comparte una configuración regional con la región de la VPC. Tenga en cuenta que, una vez elegida la configuración regional para un grupo, no puede modificarla. Si la región de origen de IPAM no está disponible debido a una interrupción y el grupo tiene una configuración regional diferente a la región de origen de IPAM, el grupo aún se puede usar para asignar direcciones IP.

> **Note**
>
> Si crea un grupo en el nivel gratuito, solo puede elegir la configuración regional que coincida con la región de origen de su IPAM. Para utilizar todas las características del IPAM en todas las configuraciones regionales, actualice al nivel avanzado.

10. Si va a crear este grupo en el alcance público, verá la opción Servicio. Seleccione EC2 (EIP/VPC). El servicio que seleccione determina el servicio AWS en el que el CIDR será anunciado. Actualmente, la única opción es EC2 (EIP/VPC), lo que significa que los CIDR asignados desde este grupo podrán ser anunciados por el servicio Amazon EC2 (para direcciones IP elásticas) y el servicio Amazon VPC (para CIDR asociados a VPC).
11. (Opcional) Elija un CIDR para aprovisionar al grupo. Puede crear un grupo sin un CIDR, pero no podrá utilizar el grupo para asignaciones hasta que le haya aprovisionado un CIDR. Puede agregar CIDR a un grupo en cualquier momento al editar el grupo.
12. Aquí tiene las mismas opciones de reglas de asignación que cuando creó el grupo de nivel superior. Consulte Creación de un grupo IPv4 de nivel superior para obtener una explicación de las opciones disponibles al crear grupos. Las reglas de asignación del grupo regional no se heredan del grupo de nivel superior. Si no aplica ninguna regla aquí, no se establecerán reglas de asignación para el grupo.
13. (Opcional) Elija Tags (Etiquetas) para el grupo.
14. Cuando haya terminado de configurar el grupo, elija Create pool (Crear grupo).
15. Consulte Creación de un grupo IPv4 de desarrollo.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear un grupo regional en su IPAM:

1. Para obtener el ID del alcance en el que desea crear el grupo: describe-ipam-scopes.
2. Para obtener el ID del grupo en el que desea crear el grupo: describe-ipam-pools.
3. Para crear el grupo: create-ipam-pool.
4. Para visualizar el grupo nuevo: describe-ipam-pools.

Repita estos pasos para crear grupos adicionales dentro del grupo de nivel superior, según sea necesario.

Creación de un grupo IPv4 de desarrollo

Siga los pasos de esta sección para crear un grupo de desarrollo dentro de su grupo regional. Si solo necesita un grupo regional y de nivel superior, y no necesita grupos de desarrollo, diríjase a Asignación de CIDR desde un grupo del IPAM.

El siguiente ejemplo muestra la jerarquía de la estructura de grupos que puede crear al seguir las instrucciones de esta guía. En este paso, va a crear un grupo de IPAM de desarrollo:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Alcance privado
    - Grupo de nivel superior (10.0.0.0/8)
      - Grupo regional en: región 1 de AWS (10.0.0.0/16)
        - Grupo de desarrollo para las VPC que no son de producción (10.0.0.0/24)
          - Asignación para una VPC (10.0.1.0/25)

En el caso anterior, los CIDR utilizados son solo ejemplos. Ilustran que cada grupo dentro del grupo de nivel superior se aprovisiona con una parte del CIDR de nivel superior.

AWS Management Console

Para crear un grupo de desarrollo dentro de un grupo regional

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Elija Create pool (Crear grupo).
4. En Alcance de IPAM, elija el mismo alcance que utilizó cuando creó el grupo de nivel superior y el grupo regional. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
5. (Opcional) Agregue una etiqueta de nombre y una descripción para el grupo.
6. En Origen, elija Grupo de IPAM. A continuación, elija el grupo regional.
7. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP

de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.

8. (Opcional) Elija un CIDR para aprovisionar al grupo. Solo puede aprovisionar un CIDR que se aprovisionó en el grupo de nivel superior. Puede crear un grupo sin un CIDR, pero no podrá utilizar el grupo para asignaciones hasta que le haya aprovisionado un CIDR. Puede agregar CIDR a un grupo en cualquier momento al editar el grupo.
9. Aquí tiene las mismas opciones de reglas de asignación que cuando creó el grupo regional y de nivel superior. Consulte Creación de un grupo IPv4 de nivel superior para obtener una explicación de las opciones disponibles al crear grupos. Las reglas de asignación del grupo no se heredan del grupo que está encima de él en la jerarquía. Si no aplica ninguna regla aquí, no se establecerán reglas de asignación para el grupo.
10. (Opcional) Elija Tags (Etiquetas) para el grupo.
11. Cuando haya terminado de configurar el grupo, elija Create pool (Crear grupo).
12. Consulte Asignación de CIDR desde un grupo del IPAM.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear un grupo regional en su IPAM:

1. Para obtener el ID del alcance en el que desea crear el grupo: describe-ipam-scopes.
2. Para obtener el ID del grupo en el que desea crear el grupo: describe-ipam-pools.
3. Para crear el grupo: create-ipam-pool.
4. Para visualizar el grupo nuevo: describe-ipam-pools.

Repita estos pasos para crear grupos de desarrollo adicionales dentro del grupo regional, según sea necesario.

Creación de grupos de direcciones IPv6 en su IPAM

AWS ofrece conectividad IPv6 en muchos de sus servicios, incluidos EC2, VPC y S3, lo que le permite utilizar el mayor espacio de direcciones y las características de seguridad mejoradas de IPv6. IPv6 se diseñó para resolver esta limitación fundamental de IPv4. Al pasar a un espacio de

direcciones de 128 bits, IPv6 ofrece un gran número de direcciones IP únicas. Esta expansión masiva de direcciones permite la proliferación continua de tecnologías conectadas, desde teléfonos inteligentes y dispositivos de IoT hasta infraestructura en la nube.

Además, puede usar IPAM para asegurarse de que utiliza CIDR IPv6 contiguos para la creación de VPC. Los CIDR asignados de forma contigua son CIDR asignados secuencialmente. Permiten simplificar las reglas de seguridad y redes; los CIDR IPv6 pueden agruparse en una sola entrada en estructuras de red y seguridad, como listas de control de acceso, tablas de enrutamiento, grupos de seguridad y firewalls.

Siga los pasos de esta sección para crear una jerarquía de grupos de IPAM de IPv6. Al crear el grupo, puede aprovisionar un CIDR para que el grupo lo utilice. El grupo asigna espacio dentro de ese CIDR a las asignaciones del grupo. Una asignación es una asignación de CIDR desde un grupo de IPAM a otro recurso o grupo de IPAM.

> **Note**
>
> Tanto el direccionamiento IPv6 público como el privado están disponibles en AWS. AWS considera las direcciones IP públicas desde AWS las que se anuncian en Internet, mientras que las direcciones IP privadas no lo son ni pueden anunciarse en Internet desde AWS. Si desea que sus redes privadas admitan IPv6 y no tiene intención de enrutar el tráfico de estas direcciones a Internet, cree su pool de IPv6 en un ámbito privado. Para más información sobre el direccionamiento IPv6 privado y público, consulte Direcciones IPv6 en la Guía del usuario de Amazon VPC.

El siguiente ejemplo muestra la jerarquía de la estructura de grupos que puede crear al seguir las instrucciones de esta guía. En esta sección, creará una jerarquía de grupos de IPAM de IPv6:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Alcance
    - Grupo regional en la región 1 de AWS (2001:db8::/52)
      - Grupo de desarrollo (2001:db8::/54)
        - Asignación para una VPC (2001:db8::/56)

En el caso anterior, los CIDR utilizados son solo ejemplos. Ilustran que el grupo de desarrollo dentro del grupo regional se aprovisiona con una parte del CIDR del grupo regional.

Contenido

Creación de un grupo regional de direcciones IPv6 en su IPAM

Siga los pasos de esta sección para crear un grupo de IPAM regional de IPv6. Al aprovisionar un bloque de CIDR de IPv6 proporcionado por Amazon en un grupo, debe aprovisionarse en un grupo con una configuración regional (región de AWS) seleccionada. Al crear el grupo, puede aprovisionar un CIDR para que el grupo lo utilice o agregarlo más tarde. A continuación, asigne ese espacio a una asignación. Una asignación es una asignación de CIDR desde un grupo de IPAM a otro recurso o grupo de IPAM.

El siguiente ejemplo muestra la jerarquía de la estructura de grupos que puede crear al seguir las instrucciones de esta guía. En este paso, va a crear un grupo de IPAM regional de IPv6:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Ámbito
    - Grupo regional en la región 1 de AWS (2001:db8::/52)
      - Grupo de desarrollo (2001:db8::/54)
        - Asignación para una VPC (2001:db8::/56)

En el caso anterior, los CIDR utilizados son solo ejemplos. Ilustran que cada grupo dentro del grupo regional de IPv6 se aprovisiona con una parte del CIDR regional de IPv6.

Al crear un grupo de IPAM, puede configurar reglas para las asignaciones que se realizan dentro del grupo de IPAM.

Las reglas de asignación permiten configurar lo siguiente:

- La longitud de máscara de red necesaria para las asignaciones dentro del grupo
- Las etiquetas necesarias para los recursos del grupo
- La configuración regional necesaria para los recursos del grupo. La configuración regional es la región de AWS en la que el grupo de IPAM está disponible para asignaciones.

Las reglas de asignación determinan si los recursos son conformes o no. Para obtener más información sobre la conformidad, consulte Monitorear el uso de CIDR por recurso.

> **Note**
>
> Hay una regla implícita adicional que no se muestra en las reglas de asignación. Si el recurso se encuentra en un grupo de IPAM que es un recurso compartido en el AWS Resource Access Manager (RAM), el propietario del recurso debe configurarse como maestro en AWS RAM. Para obtener más información acerca de compartir grupos con RAM, consulte Compartir un grupo de IPAM mediante AWS RAM.

El siguiente ejemplo muestra cómo puede utilizar reglas de asignación para controlar el acceso a un grupo de IPAM:

Example

Cuando crea los grupos en función de las necesidades de enrutamiento y seguridad, es posible que desee permitir que solo ciertos recursos utilicen un grupo. En tales casos, puede establecer una regla de asignación en la que se indique que cualquier recurso que desee un CIDR de este grupo debe tener una etiqueta que coincida con los requisitos de etiqueta de la regla de asignación. Por ejemplo, puede establecer una regla de asignación que indique que solo las VPC con la etiqueta prod pueden obtener CIDR desde un grupo de IPAM.

> **Note**
>
> - En este tema, se explica cómo crear un grupo regional de IPv6 con un rango de direcciones IPv6 proporcionado por AWS o con un rango IPv6 privado. Si desea usar sus propios rangos de direcciones IPv4 o IPv6 públicos en AWS (BYOIP), existen requisitos previos. Para obtener más información, consulte Tutorial: incorpore sus direcciones IP a IPAM.
> - Si va a crear un grupo de IPv6 en un ámbito privado, puede utilizar un rango GUA o ULA de IPv6 privado. Para usar un rango GUA privado, primero debe haber activado la opción en su IPAM (consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados).

AWS Management Console

Para crear un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Elija Create pool (Crear grupo).
4. En Alcance de IPAM, seleccione alcance público o privado. Si desea que sus redes privadas admitan IPv6 y no tiene intención de enrutar el tráfico de estas direcciones a Internet, elija un alcance privado. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.

   De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado.
5. (Opcional) Agregue una etiqueta de nombre y una descripción para el grupo.
6. En Origen, elija Alcance del IPAM.
7. En Familia de direcciones, seleccione IPv6. Si crea este grupo en el ámbito público, todos los CIDR de este grupo se anunciarán públicamente.
8. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
9. Elija la Configuración regional del grupo. Si quiere aprovisionar un bloque de CIDR de IPv6 proporcionado por Amazon en un grupo, debe aprovisionarse en un grupo con una configuración regional (región de AWS) seleccionada. Elegir una configuración regional garantiza que no haya dependencias entre regiones entre su grupo y los recursos que se asignan desde él. Las opciones disponibles proceden de las regiones operativas que eligió para el IPAM al crearlo. Puede agregar regiones operativas adicionales en cualquier momento.

   La configuración regional es la Región AWS en la que desea que este grupo de IPAM esté disponible para asignaciones. Por ejemplo, solo puede asignar un CIDR para una VPC desde un grupo de IPAM que comparte una configuración regional con la región de la VPC. Tenga en cuenta que, una vez elegida la configuración regional para un grupo, no puede modificarla. Si la región de origen de IPAM no está disponible debido a una interrupción y el

grupo tiene una configuración regional diferente a la región de origen de IPAM, el grupo aún se puede usar para asignar direcciones IP.

> **Note**
>
> Si crea un grupo en el nivel gratuito, solo puede elegir la configuración regional que coincida con la región de origen de su IPAM. Para utilizar todas las características del IPAM en todas las configuraciones regionales, actualice al nivel avanzado.

10. (Opcional) Si va a crear un grupo de IPv6 en el ámbito público, en Servicio, elija EC2 (EIP/VPC). El servicio que seleccione determina el servicio AWS en el que el CIDR será anunciado. Actualmente, la única opción es EC2 (EIP/VPC), lo que significa que los CIDR asignados desde este grupo podrán ser anunciados por el servicio Amazon EC2 (para direcciones IP elásticas) y el servicio Amazon VPC (para CIDR asociados a VPC).
11. (Opcional) Si va a crear un grupo de IPv6 en el ámbito público, en la opción Origen de IP pública, elija Propiedad de Amazon para que AWS proporcione un rango de direcciones IPv6 para este grupo. Como se indica en la parte superior de esta página, en este tema se explica cómo crear un grupo regional de IPv6 con un rango de direcciones IP proporcionado por AWS. Si desea usar su propio rango de direcciones IPv4 o IPv6 en AWS (BYOIP), existen requisitos previos. Para obtener más información, consulte Tutorial: incorpore sus direcciones IP a IPAM.
12. (Opcional) Puede crear un grupo sin un CIDR, pero no podrá utilizar el grupo para asignaciones hasta que le haya aprovisionado un CIDR. Para aprovisionar un CIDR, realice una de las siguientes acciones:

    - Si va a crear un grupo de IPv6 en el ámbito público con un origen de IP pública propiedad de Amazon, para aprovisionar un CIDR, en CIDR para aprovisionar, elija Agregar CIDR propiedad de Amazon y elija el tamaño de máscara de red entre /40 y /52 para el CIDR. Al elegir una longitud de máscara de red en el menú desplegable, verá la longitud de la máscara de red y la cantidad de CIDR /56 que representa la máscara de red. De manera predeterminada, puede agregar un bloque de CIDR de IPv6 proporcionado por Amazon al grupo regional. Para obtener información sobre cómo aumentar el límite predeterminado, consulte Cuotas de IPAM.
    - Si va a crear un grupo de IPv6 en un ámbito privado, puede utilizar un rango GUA o ULA de IPv6 privado:

- Para obtener información importante sobre el direccionamiento IPv6 privado, consulte Direcciones IP6 privadas en la Guía del usuario de Amazon VPC.
- Para usar un rango de ULA de IPv6 privado, en CIDR para aprovisionar, elija Agregar CIDR de ULA por máscara de red y elija un tamaño de máscara de red o elija Ingresar CIDR de IPv6 privado e ingrese un rango de ULA. El espacio ULA de IPv6 válido es cualquier espacio inferior a fd00::/8 que no se superponga con el rango reservado de Amazon fd00::/16.
- Para usar un rango GUA de IPv6 privado, primero debe haber activado la opción en su IPAM (consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados). Una vez que haya activado los CIDR GUA de IPv6 privados, introduzca un GUA de IPv6 en Introducir CIDR de IPv6 privado.

13. Elija reglas de asignación opcionales para este grupo:

- Minimum netmask length (Longitud mínima de la máscara de red): la longitud mínima de la máscara de red requerida para que las asignaciones de CIDR en este grupo de IPAM sean conformes y para el bloque de CIDR de mayor tamaño que se puede asignar desde el grupo. La longitud mínima de la máscara de red debe ser inferior a su longitud máxima. Las longitudes de máscara de red posibles para las direcciones IPv6 van de 0 a 128.
- Default netmask length (Longitud predeterminada de la máscara de red): longitud predeterminada de la máscara de red para las asignaciones agregadas a este grupo. Por ejemplo, si el CIDR que se aprovisiona para este grupo es `2001:db8::/52` e ingresa 56 aquí, cualquier asignación nueva en este grupo tendrá por defecto una longitud de máscara de red de /56.
- Maximum netmask length (Longitud máxima de la máscara de red): longitud máxima de la máscara de red que se requerirá para las asignaciones de CIDR en este grupo. Este valor determina el bloque de CIDR de menor tamaño que se puede asignar desde el grupo. Por ejemplo, si ingresa /56 aquí, la longitud de máscara de red más pequeña que se puede asignar a los CIDR de este grupo es /56.
- Tagging requirements (Requisitos de etiquetado): las etiquetas necesarias para que los recursos asignen espacio del grupo. Si los recursos cambian sus etiquetas después de haber asignado espacio o si se modifican las reglas de etiquetado de asignación en el grupo, el recurso puede marcarse como no conforme.
- Locale (Configuración regional): la configuración regional que se requerirá para los recursos que utilizan CIDR de este grupo. Los recursos importados automáticamente que no tengan esta configuración regional se marcarán como no conformes. Los recursos que

no se importan automáticamente al grupo no podrán asignar espacio desde el grupo a menos que se encuentren en esta configuración regional.

14. (Opcional) Elija Tags (Etiquetas) para el grupo.
15. Elija Create pool (Crear grupo).
16. Consulte Creación de un grupo de direcciones IPv6 de desarrollo en su IPAM.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear o editar un grupo regional de IPv6 en su IPAM:

1. Si desea habilitar el aprovisionamiento de CIDR GUA IPv6 privados, modifique el IPAM con modify-ipam e incluya la opción de `enable-private-gua`. Para obtener más información, consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados.
2. Crear un grupo con create-ipam-pool.
3. Aprovisionar un nuevo CIDR en el grupo: provision-ipam-pool-cidr.
4. Para editar el grupo después de crearlo a fin de modificar las reglas de asignación: modify-ipam-pool.

Creación de un grupo de direcciones IPv6 de desarrollo en su IPAM

Siga los pasos de esta sección para crear un grupo de desarrollo dentro de su grupo regional de IPv6. Si solo necesita un grupo regional y no necesita grupos de desarrollo, diríjase a Asignación de CIDR desde un grupo del IPAM.

El siguiente ejemplo muestra la jerarquía de la estructura de grupos que puede crear al seguir las instrucciones de esta guía. En este paso, va a crear un grupo de IPAM de desarrollo:

- IPAM que opera en la región 1 de AWS y la región 2 de AWS
  - Ámbito
    - Grupo regional en la región 1 de AWS (2001:db8::/52)
      - Grupo de desarrollo (2001:db8::/54)

- Asignación para una VPC (2001:db8::/56)

En el caso anterior, los CIDR utilizados son solo ejemplos. Ilustran que cada grupo dentro del grupo de nivel superior se aprovisiona con una parte del CIDR de nivel superior.

AWS Management Console

Para crear un grupo de desarrollo dentro de un grupo regional de IPv6

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Elija Create pool (Crear grupo).
4. En Alcance de IPAM, seleccione un alcance. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
5. (Opcional) Agregue una etiqueta de nombre y una descripción para el grupo.
6. En Origen, elija Grupo de IPAM. A continuación, en Grupo de origen, elija el grupo regional de IPv6.
7. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
8. (Opcional) Elija un CIDR para aprovisionar al grupo. Solo puede aprovisionar un CIDR que se aprovisionó en el grupo de nivel superior. Puede crear un grupo sin un CIDR, pero no podrá utilizar el grupo para asignaciones hasta que le haya aprovisionado un CIDR. Puede agregar CIDR a un grupo en cualquier momento al editar el grupo.
9. Aquí tiene las mismas opciones de reglas de asignación que cuando creó el grupo regional de IPv6. Consulte Creación de un grupo regional de direcciones IPv6 en su IPAM para obtener una explicación de las opciones disponibles al crear grupos. Las reglas de asignación del grupo no se heredan del grupo que está encima de él en la jerarquía. Si no aplica ninguna regla aquí, no se establecerán reglas de asignación para el grupo.
10. (Opcional) Elija Tags (Etiquetas) para el grupo.
11. Cuando haya terminado de configurar el grupo, elija Create pool (Crear grupo).
12. Consulte Asignación de CIDR desde un grupo del IPAM.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear un grupo regional de IPv6 en su IPAM:

1. Para obtener el ID del alcance en el que desea crear el grupo: describe-ipam-scopes.
2. Para obtener el ID del grupo en el que desea crear el grupo: describe-ipam-pools.
3. Para crear el grupo: create-ipam-pool.
4. Para visualizar el grupo nuevo: describe-ipam-pools.

Repita estos pasos para crear grupos de desarrollo adicionales dentro del grupo regional de IPv6, según sea necesario.

Asignación de CIDR desde un grupo del IPAM

Una característica importante del IPAM es la capacidad de asignar y administrar el espacio de direcciones IP. Al crear una VPC, debe especificar un bloque de CIDR de direcciones IP que defina el rango de direcciones IP disponibles para esa VPC. El IPAM simplifica este proceso al proporcionar una visión global de todo su inventario de direcciones IP, lo que lo ayuda a asignar y reutilizar estratégicamente los prefijos de IP en varias VPC.

Esta asignación de espacios de direcciones es crucial para garantizar que no haya rangos de IP superpuestos, lo que podría provocar conflictos de enrutamiento y problemas de conectividad. El IPAM también le permite reservar espacio de direcciones IP para la futura expansión de la VPC, lo que evita la necesidad de tener que volver a numerar de forma compleja más adelante.

Siga los pasos de esta sección para asignar un CIDR desde un grupo de IPAM a un recurso.

> **Note**
>
> A lo largo de esta guía del usuario y en la consola de IPAM se utilizan los términos aprovisionar y asignar. Aprovisionar se utiliza cuando se agrega un CIDR a un grupo de IPAM. Asignar se utiliza cuando asocia un CIDR desde un grupo de IPAM a un recurso.

Puede asignar CIDR desde un grupo de IPAM de las siguientes formas:

- Utilice un servicio de AWS que esté integrado con IPAM, como Amazon VPC, y seleccione la opción de utilizar un grupo de IPAM para el CIDR. IPAM crea automáticamente la asignación en el grupo por usted.
- Asigne de forma manual un CIDR dentro de un grupo de IPAM a fin de reservarlo para su uso posterior con un servicio de AWS que esté integrado con IPAM, como Amazon VPC.

En esta sección, se detallan las dos opciones: cómo utilizar los servicios de AWS integrados con IPAM para aprovisionar un CIDR de grupo de IPAM y cómo reservar de forma manual el espacio de direcciones IP.

Contenido

Crear una VPC que utilice un CIDR de grupo de IPAM

Con Amazon Virtual Private Cloud (Amazon VPC), puede lanzar recursos de AWS en una red virtual aislada de manera lógica que haya definido. Esta red virtual es muy similar a la red tradicional que usaría en su propio centro de datos, pero con los beneficios que supone utilizar la infraestructura escalable de AWS.

Una nube virtual privada (VPC) es una red virtual dedicada para su cuenta de AWS. Esta infraestructura en la nube está aislada lógicamente de otras redes virtuales de la nube de AWS. Puede especificar un intervalo de direcciones IP para la VPC, añadir subredes, añadir puertas de enlace y asociar grupos de seguridad.

Siga los pasos que aparecen en Creación de una VPC en la Guía del usuario de Amazon VPC. Cuando llegue al paso donde debe elegir un CIDR para la VPC, tendrá la opción de utilizar un CIDR de un grupo de IPAM.

Si elige la opción de utilizar un grupo de IPAM al crear la VPC, AWS asigna un CIDR en el grupo de IPAM. Puede ver la asignación en IPAM al elegir un grupo en el panel de contenido de la consola de IPAM y visualizar la pestaña Resources (Recursos) del grupo.

> **Note**
>
> Para obtener instrucciones completas sobre el uso de la AWS CLI, incluida la creación de una VPC, consulte la sección Tutoriales para IP Address Manager de Amazon VPC.

Asignar de forma manual un CIDR a un grupo para reservar espacio de direcciones IP

Siga los pasos de esta sección para asignar manualmente un CIDR a un grupo. Puede hacerlo para reservar un CIDR dentro de un grupo de IPAM para su uso posterior. También puede reservar espacio en el grupo de IPAM para representar una red local. IPAM administrará esa reserva por usted e indicará si algún CIDR se superpone con el espacio IP en las instalaciones.

AWS Management Console

Para asignar un CIDR de forma manual

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, se selecciona el alcance privado predeterminado. Si no desea utilizar el alcance privado predeterminado, en el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. En el panel de contenido, elija un grupo.
5. Elija Actions (Acciones) > Create custom allocation (Crear asignación personalizada).
6. Elija si desea agregar un CIDR específico para asignar (por ejemplo, `10.0.0.0/24` para IPv4 o `2001:db8::/52` para IPv6) o agregar un CIDR por tamaño únicamente al elegir la longitud de la máscara de red (por ejemplo, `/24` para IPv4 o `/52` para IPv6).
7. Elija Allocate (Asignar).
8. Puede ver la asignación en IPAM al seleccionar Pools (Grupos) en el panel de navegación, elegir un grupo y visualizar la pestaña Allocations (Asignaciones) del grupo.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Use los siguientes comandos de la AWS CLI para asignar de forma manual un CIDR a un grupo:

1. Para obtener el ID del grupo de IPAM en el que desea crear la asignación: describe-ipam-pools.
2. Para crear la asignación: allocate-ipam-pool-cidr.
3. Para ver la asignación: get-ipam-pool-allocations.

Para liberar un CIDR asignado de forma manual, consulte Liberar una asignación.

Administración del espacio de direcciones IP en IPAM

Las tareas en esta sección son opcionales. En esta sección, se agrupan los procedimientos relacionados con el uso del IPAM. Los procedimientos están ordenados alfabéticamente.

Si desea completar las tareas de esta sección y ha delegado una cuenta de IPAM, el administrador de IPAM debe completar las tareas.

Siga los pasos de esta sección para administrar el espacio de direcciones IP en IPAM.

Contenido

Automatización de las actualizaciones de la lista de prefijos con IPAM

Una lista de prefijos administrada es un conjunto de bloques CIDR que puede utilizar como referencia en las reglas de los grupos de seguridad y en las tablas de enrutamiento, en lugar de especificar direcciones IP individuales. Por ejemplo, en lugar de crear reglas de grupo de seguridad independientes para `10.1.0.0/16`, `10.2.0.0/16` y `10.3.0.0/16`, puede crear una única lista de prefijos que incluya los tres bloques CIDR y hacer referencia a esta en una sola regla.

Hay dos tipos:

- Listas de prefijos administradas por el cliente: rangos de direcciones IP que usted define y administra
- Listas de prefijos administradas por AWS: rangos de direcciones IP para servicios de AWS (como S3 o CloudFront)

Esta característica de IPAM automatiza la administración de las listas de prefijos administradas por el cliente y mantiene las entradas CIDR sincronizadas con los cambios en la red.

El problema que esto resuelve

Sin la automatización, los equipos de red deben invertir una cantidad considerable de tiempo en actualizar manualmente las listas de prefijos cuando cambia la infraestructura y en garantizar la coherencia de dichas listas en todos los entornos y regiones.

IPAM soluciona este problema al permitir la creación de reglas que actualizan automáticamente las listas de prefijos. Puede usar dos enfoques: hacer referencia a los bloques CIDR de los grupos de IPAM o crear reglas basadas en los recursos reales de AWS, por ejemplo: “incluir todas las VPC etiquetadas con env=prod”, “incluir todas las subredes en us-east-1” o “incluir todas las direcciones IP elásticas pertenecientes a la cuenta 123456789”. Al agregar o eliminar estos recursos, IPAM actualiza la lista de prefijos con sus bloques CIDR de forma automática.

Funcionamiento

Cree reglas que indiquen a IPAM qué direcciones IP incluir en una lista de prefijos. Por ejemplo: “incluir todos los bloques CIDR de las VPC etiquetadas con env=prod”. Cuando agregue o elimine VPC de producción, IPAM actualiza la lista de prefijos de forma automática.

Cuándo se debe usar

- Grupos de seguridad: cree una regla “incluir todas las VPC etiquetadas con env=prod” para que, al agregar nuevas VPC de producción, estas se autoricen automáticamente en las reglas del grupo de seguridad
- Multirregión: implemente las mismas reglas de IPAM en varias regiones para mantener listas de prefijos idénticas sin copiar manualmente las entradas CIDR
- Infraestructura dinámica: cuando cree o elimine VPC o subredes, los bloques CIDR se agregarán o eliminarán automáticamente de las listas de prefijos, sin necesidad de actualizaciones manuales

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un IPAM con el nivel avanzado habilitado
- Una lista de prefijos administrada por el cliente (o cree una durante la configuración)
- Permisos de IAM para las operaciones de IPAM y de listas de prefijos de EC2

Pasos de configuración

Paso 1: Creación de un solucionador de lista de prefijos de IPAM

Defina qué bloques CIDR incluir en la lista de prefijos mediante la creación de un solucionador de lista de prefijos de IPAM.

AWS Management Console

Para crear un solucionador de lista de prefijos de IPAM

1. Abra la consola de IPAM.
2. En el panel de navegación, elija Solucionadores de lista de prefijos.
3. Elija Crear solucionador de lista de prefijos.
4. En el Paso 1: Configurar detalles del solucionador, seleccione lo siguiente:
   - IPAM: una instancia de IPAM
   - Familia de direcciones: IPv4 o IPv6

- Etiqueta de nombre (opcional): un nombre descriptivo
- Descripción (opcional): una descripción
- Etiquetas: etiquetas de recursos

5. Elija Siguiente.
6. En el Paso 2: Configurar las reglas, elija Agregar regla. Puede agregar hasta 99 reglas.

> **Important**
>
> Puede crear un solucionador de listas de prefijos sin incluir reglas de selección de CIDR; sin embargo, generará versiones vacías (sin bloques CIDR) hasta que se agreguen dichas reglas.

7. Elija uno de los siguientes tipos de reglas:

- CIDR estática: una lista fija de bloques CIDR que no cambia (similar a una lista manual replicada en las regiones)
- CIDR del grupo de IPAM: CIDR provenientes de grupos específicos de IPAM (por ejemplo, todos los CIDR del grupo de producción de IPAM)

  Si selecciona esta opción, elija lo siguiente:

  - Ámbito de IPAM: seleccione el ámbito de IPAM en el que desea buscar recursos
  - Condiciones de:
    - Propiedad
      - ID del grupo de IPAM: seleccione un grupo de IPAM que contenga los recursos
      - CIDR (como 10.24.34.0/23)
    - Operación: igual/no igual
    - Valor: el valor con el que se debe cumplir la condición
- CIDR de recurso de ámbito: CIDR de recursos de AWS, como VPC, subredes o direcciones IP elásticas dentro de un ámbito de IPAM

  Si selecciona esta opción, elija lo siguiente:

  - Ámbito de IPAM: seleccione el ámbito de IPAM en el que desea buscar recursos
  - Tipo de recurso: seleccione un recurso, como una VPC o una subred.
  - Condiciones de:

- :
  - ID de recurso: el identificador único de un recurso (como vpc-1234567890abcdef0)
  - Propietario del recurso (como 111122223333)
  - Región del recurso (como us-east-1)
  - Etiqueta del recurso (como clave: nombre, valor: dev-vpc-1)
  - CIDR (como 10.24.34.0/23)
- Operación: igual/no igual
- Valor: el valor con el que se debe cumplir la condición

8. Elija Siguiente.
9. Elija Validar y crear.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear un solucionador de listas de prefijos de IPAM:

- Use el comando create-ipam-prefix-list-resolver y guarde el ID del solucionador devuelto para el paso 2.

Paso 2: Creación de un destino de solucionador para conectarlo a una lista de prefijos

Vincule el solucionador a una lista de prefijos existente mediante la creación de un destino de solucionador. Use el ID del solucionador devuelto en el paso 1.

AWS Management Console

Para crear un destino de solucionador de lista de prefijos de IPAM

1. En la consola de IPAM, elija Solucionadores de listas de prefijos.
2. Elija el solucionador que creó en el paso 1.
3. En la página de detalles del solucionador, elija la pestaña Destinos.
4. Elija Crear destino.

5. Configurar el destino:
   - Región: seleccione la región donde exista la lista de prefijos administrada o donde vaya a crear una.
   - Lista de prefijos: elija una lista de prefijos administrada existente o cree una nueva
6. En Versión deseada, seleccione una de las siguientes opciones:
   - Seguir siempre la versión más reciente: elija esta opción para recibir actualizaciones automáticas cuando desee que las listas de prefijos se mantengan actualizadas con los cambios de infraestructura sin intervención manual.
   - Seguir una versión específica: elija esta opción para mantener la estabilidad cuando necesite actualizaciones predecibles y controladas, y prefiera aprobar manualmente los cambios en las listas de prefijos.
7. Elija Crear destino.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Use los siguientes comandos de la AWS CLI para crear un destino de solucionador de lista de prefijos de IPAM:

- Use el comando create-ipam-prefix-list-resolver-target con el ID del solucionador del paso 1 y el ID de la lista de prefijos existente.

IPAM ahora actualiza automáticamente la lista de prefijos según las reglas. La lista de prefijos se completará con los CIDR que coincidan con los criterios.

Paso 3: Supervisión de versiones y sincronización

Como resultado de crear un solucionador y un destino de lista de prefijos, el solucionador genera versiones de CIDR según las reglas, y el destino sincroniza esos CIDR del solucionador con una lista de prefijos administrada específica. Cada versión es una instantánea de los CIDR que coincidían con las reglas en ese momento. El número de versión aumenta cada vez que la lista de CIDR cambia debido a modificaciones en la infraestructura.

Ejemplo de la versión:

Estado inicial (versión 1)

Entorno de producción:

- vpc-prod-web (10.1.0.0/16): etiquetado con env=prod
- vpc-prod-db (10.2.0.0/16): etiquetado con env=prod

Regla del solucionador: incluir todas las VPC etiquetadas con env=prod

CIDR de la versión 1: 10.1.0.0/16, 10.2.0.0/16

Cambio en la infraestructura (versión 2)

Nueva VPC agregada:

- vpc-prod-api (10.3.0.0/16): etiquetado con env=prod

IPAM detecta automáticamente el cambio y crea una nueva versión.

CIDR de la versión 2: 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16

Esta sección explica cómo supervisar la creación de versiones mediante la consola de AWS o la CLI de AWS, y cómo verificar la sincronización correcta mediante la CLI de AWS.

Además, se recomienda configurar alarmas de CloudWatch basadas en las métricas de fallos, ya que podría ser necesario reevaluar y ajustar las reglas de selección de CIDR para mantenerse dentro de los límites de tamaño de las listas de versiones y de prefijos. Para obtener una lista de las métricas de CloudWatch relacionadas con las listas de prefijos de IPAM, consulte Métricas del solucionador de lista de prefijos de IPAM.

AWS Management Console

Para ver las versiones creadas y supervisar la sincronización del destino

1. En la consola de IPAM, elija Solucionadores de listas de prefijos.
2. Elija el solucionador que creó en el paso 1.
3. En la página de detalles del solucionador, elija la pestaña Versiones. Aquí verá las versiones creadas por el solucionador junto con los CIDR incluidos en cada versión.

4. En la página de detalles del solucionador, elija la pestaña Supervisión. En esta vista, las Métricas del solucionador de lista de prefijos de IPAM se presentan en forma de gráfico:
   - Se creó correctamente la versión del solucionador de listas de prefijos
   - Error en la creación de versión del solucionador de lista de prefijos
5. Desde la pestaña Supervisión, también puede configurar una alarma de CloudWatch. Paa ello, elija Crear alarma para la creación de versión del solucionador de lista de prefijos. Se le redirige a la consola de CloudWatch con la alarma parcialmente configurada para la métrica. Para obtener más información sobre cómo finalizar la creación de la alarma, consulte Creación de una alarma de CloudWatch basada en un umbral estático en la Guía del usuario de Amazon CloudWatch.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para supervisar las versiones y la sincronización:

1. Use el comando get-ipam-prefix-list-resolver-version-entries para ver la versión más reciente creada por el solucionador.
2. Use el comando describe-ipam-prefix-list-resolver-targets para supervisar el estado de sincronización del destino del solucionador.

El comando de supervisión muestra:

- state: estado de sincronización actual (create-complete, modify-complete y otros)
- lastSyncedVersion: última versión sincronizada correctamente
- desiredVersion: versión de destino a la que se debe sincronizar
- stateMessage: detalles del error si la sincronización falla

> **Important**
>
> Para respaldar los flujos de trabajo de reversión, IPAM conservará copias de las 10 versiones anteriores de resolución de listas de prefijos para cada uno de sus objetivos; además, IPAM

eliminará las versiones que superen este umbral si permanecen sin referencia durante 7 días más.

Paso 4: (opcional) Habilitación y desactivación de la sincronización de la lista de prefijos de IPAM

Si una lista de prefijos administrada se ha configurado como destino de una lista de prefijos de IPAM y desea realizar cambios en dicha lista sin necesitar permisos para acceder al destino del solucionador de lista de prefijos de IPAM, puede modificar la lista de prefijos administrada y desactivar la sincronización con el solucionador de lista de prefijos de IPAM. Cuando la sincronización está desactivada, los CIDR de la lista de prefijos no se actualizan automáticamente y es posible modificarlos. Cuando está habilitada, los CIDR de la lista de prefijos se actualizan automáticamente en función de las reglas de selección de CIDR del solucionador asociado.

Cambiar el estado de monitoreo de los CIDR de VPC

Siga los pasos de esta sección para cambiar el estado de monitoreo de un CIDR de VPC. Puede querer cambiar un CIDR de VPC de Monitorizado a Ignorado si no desea que IPAM administre o monitorice la VPC y permita que el CIDR asignado a dicha VPC esté disponible para su uso. Puede que quiera cambiar un CIDR de VPC de Ignored (Ignorado) a Monitored (Monitoreado) si desea que IPAM administre o supervise el CIDR de VPC.

Note

- No se pueden ignorar los CIDR de VPC del alcance público.
- Si se ignora un CIDR, se le seguirá cobrando por las direcciones IP activas en el CIDR. Para obtener más información, consulte Precios de IPAM.
- Si se ignora un CIDR, aún puede ver el historial de direcciones IP en el CIDR. Para obtener más información, consulte Ver historial de direcciones IP.

Puede cambiar el estado de supervisión de un CIDR de VPC a Monitored (Monitoreado) o a Ignored (Ignorado):

- Monitored (Monitoreado): IPAM detectó el CIDR de VPC, que se monitorea para detectar superposiciones con otros CIDR y la conformidad con las reglas de asignación.

- Ignored (Ignorado): el CIDR de VPC se ha elegido para estar exento del monitoreo. Los CIDR de VPC ignorados no se evalúan para detectar la superposición con otros CIDR o la conformidad con las reglas de asignación. Cuando se elige ignorar un CIDR de VPC, cualquier espacio asignado a él desde un grupo de IPAM se devuelve al grupo y el CIDR de VPC no se volverá a importar mediante la importación automática (si la regla de asignación de importación automática se ha establecido en el grupo).

AWS Management Console

Para cambiar el estado de monitoreo de un CIDR asignado a una VPC

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Resources (Recursos).
3. Elija el alcance que desea utilizar en el menú desplegable ubicado en la parte superior del panel de contenido.
4. En el panel de contenido, elija la VPC y vea sus detalles.
5. En VPC CIDRs (CIDR de VPC), seleccione uno de los CIDR asignados a la VPC y elija Actions (Acciones) > Mark as ignored (Marcar como ignorado) o Unmark as ignored (Desmarcar como ignorado).
6. Elija Mark as ignored (Marcar como ignorado) o Unmark as ignored (Desmarcar como ignorado).

Command line

Utilice los siguientes comandos de la AWS CLI para cambiar el estado de monitoreo de un CIDR de VPC:

1. Para obtener un ID de alcance: describe-ipam-scopes.
2. Para visualizar el estado de monitoreo actual del CIDR de VPC: get-ipam-resource-cidrs.
3. Para cambiar el estado del CIDR de VPC: modify-ipam-resource-cidr.
4. Para visualizar el estado de monitoreo nuevo del CIDR de VPC: get-ipam-resource-cidrs.

Creación de alcances adicionales

Siga los pasos de esta sección para crear un alcance adicional.

Un alcance es el contenedor de más alto nivel dentro de IPAM. Al crear un IPAM, IPAM crea dos alcances predeterminados en su nombre. Cada alcance representa el espacio IP de una única red. El alcance privado está destinado a todo el espacio privado. El alcance público está destinado a todo el espacio público. Los alcances le permiten reutilizar las direcciones IP en varias redes no conectadas sin causar superposición o conflicto de direcciones IP.

Al crear un IPAM, se crean los alcances predeterminados (uno privado y otro público) para usted. Puede crear alcances privados adicionales. No puede crear alcances públicos adicionales.

Puede crear alcances privados adicionales si necesita soporte para varias redes privadas desconectadas. Los alcances privados adicionales le permiten crear grupos y administrar recursos que utilizan el mismo espacio IP.

> **Important**
>
> Si IPAM detecta recursos con CIDR IPv4 o IPv6 privados, los CIDR de recursos se importan al alcance privado predeterminado y no aparecen en ningún alcance privado adicional que cree. Puede mover CIDR del alcance privado predeterminado a otro alcance privado. Para obtener más información, consulte Mover CIDR de VPC entre alcances.

AWS Management Console

Para crear un alcance privado adicional

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Scopes (Alcances).
3. Elija Create scope (Crear alcance).
4. Elija el IPAM al que desea agregar el alcance.
5. Agregue una descripción del alcance.
6. Elija Create scope (Crear alcance).
7. Puede ver el alcance en IPAM al seleccionar Scopes (Alcances) en el panel de navegación.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para crear un alcance privado adicional:

1. Para visualizar sus alcances actuales: describe-ipam-scopes
2. Para crear un nuevo alcance privado: create-ipam-scope
3. Para visualizar sus alcances actuales a fin de ver el alcance nuevo: describe-ipam-scopes

Eliminar un IPAM

Es posible que desee eliminar un IPAM si ya no lo necesita, si tiene que reestructurar la administración de direcciones IP o si quiere empezar de cero con una nueva configuración del IPAM. Eliminar un IPAM puede ayudar a simplificar la administración de direcciones IP y se ajusta a los cambiantes requisitos empresariales u operativos.

Siga los pasos de esta sección para eliminar un IPAM. Para obtener información sobre cómo aumentar el número predeterminado de IPAM que puede tener en lugar de eliminar un IPAM existente, consulte Cuotas de IPAM.

> **Note**
>
> Al eliminar un IPAM se eliminan todos los datos monitoreados asociados al IPAM, incluidos los datos históricos de los CIDR.

AWS Management Console

Para eliminar un IPAM

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija IPAMs (IPAM).
3. En el panel de contenido, seleccione su IPAM.
4. Elija Actions (Acciones) > Delete IPAM (Eliminar IPAM).
5. Realice una de las siguientes acciones:

   - Elija Cascade delete (Eliminación en cascada) para eliminar el IPAM, los alcances privados, los grupos en alcances privados y cualquier asignación de los grupos en alcances privados. No puede eliminar el IPAM con esta opción si hay un grupo en su alcance público. Si utiliza esta opción, IPAM hace lo siguiente:

- Anula la asignación de cualquier CIDR asignado a los recursos de VPC (tales como las VPC) en grupos de alcances privados.

  > **Note**
  >
  > Si se habilita esta opción, no se eliminan recursos de VPC. El CIDR asociado al recurso ya no estará asignado desde un grupo de IPAM, pero el CIDR en sí no se modificará.

- Quita todos los CIDR IPv4 aprovisionados a los grupos de IPAM en alcances privados.
- Elimina todos los grupos de IPAM en alcances privados.
- Elimina todos los alcances privados no predeterminados de la IPAM.
- Elimina los alcances públicos y privados predeterminados y el IPAM.

- Si no marca la casilla de verificación Cascade delete (Eliminación en cascada), para poder eliminar un IPAM, debe hacer lo siguiente:
  - Libere asignaciones dentro de los grupos de IPAM. Para obtener más información, consulte Liberar una asignación.
  - Anule el aprovisionamiento de CIDR aprovisionados a grupos dentro del IPAM. Para obtener más información, consulte Anular el aprovisionamiento del CIDR de un grupo.
  - Elimine cualquier alcance adicional que no sea predeterminado. Para obtener más información, consulte Eliminar un alcance.
  - Elimine los grupos de IPAM. Para obtener más información, consulte Eliminar un grupo.

6. Introduzca **`delete`** y luego elija Delete (Eliminar).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para eliminar un IPAM:

1. Para ver los IPAM actuales: describe-ipams.
2. Para eliminar un IPAM: delete-ipam.
3. Para ver los IPAM actualizados: describe-ipams

Para crear un IPAM nuevo, consulte Creación de un IPAM.

Eliminar un grupo

Un grupo del IPAM de AWS representa un rango definido de direcciones IP que se pueden asignar y administrar en un entorno u organización de AWS específicos. Los grupos se utilizan para organizar el espacio de direcciones IP, permitir la administración automatizada de direcciones IP y aplicar políticas de gobernanza de direcciones IP en toda la infraestructura de la nube.

Es posible que desee eliminar un grupo del IPAM para eliminar el espacio de direcciones IP no utilizado o innecesario y recuperarlo para otros fines. No puede eliminar un grupo de direcciones IP si hay asignaciones en él. Primero debe liberar las asignaciones y Anular el aprovisionamiento del CIDR de un grupo antes de poder eliminar el grupo.

Siga los pasos de esta sección para eliminar un grupo de IPAM.

AWS Management Console

Para eliminar un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. En el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. En el panel de contenido, seleccione el grupo donde desee eliminar un CIDR.
5. Elija Actions > Delete pool (Acciones > Eliminar grupo).
6. Introduzca **`delete`** y luego elija Delete (Eliminar).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para eliminar un grupo.

1. Para ver los grupos y obtener un ID de grupo de IPAM: describe-ipam-pools.

2. Par eliminar un grupo: delete-ipam-pool.
3. Para ver sus grupos: describe-ipam-pools.

Para crear un grupo nuevo, consulte Creación de un grupo IPv4 de nivel superior.

Eliminar un alcance

Es posible que desee eliminar un alcance del IPAM si ya no cumple el propósito previsto, por ejemplo, al reestructurar la red, consolidar regiones o ajustar la asignación de direcciones IP. Eliminar los alcances no utilizados puede ayudar a agilizar la configuración del IPAM y a optimizar la administración de direcciones IP en AWS.

> **Note**
>
> No puede eliminar un alcance si se da alguna de las siguientes condiciones:
>
> - El alcance es un alcance predeterminado. Al crear un IPAM, se crean automáticamente dos alcances predeterminados (uno público y otro privado) y no se pueden eliminar. Para saber si un alcance es predeterminado, consulte Scope type (Tipo de alcance) en los detalles del alcance.
> - Hay uno o varios grupos en el alcance. Primero debe Eliminar un grupo antes de poder eliminar el alcance.

AWS Management Console

Para eliminar un alcance

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Scopes (Alcances).
3. En el panel de contenido, elija el alcance que desea eliminar.
4. Elija Actions (Acciones) > Delete scope (Eliminar alcance).
5. Introduzca **`delete`** y luego elija Delete (Eliminar).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para eliminar un alcance.

1. Para visualizar los alcances: describe-ipam-scopes.
2. Para eliminar un alcance: delete-ipam-scope.
3. Para visualizar los alcances actualizados: describe-ipam-scopes.

Para crear un alcance nuevo, consulte Creación de alcances adicionales. Para eliminar el IPAM, consulte Eliminar un IPAM.

Anular el aprovisionamiento del CIDR de un grupo

Es posible que desee desaprovisionar el CIDR de un grupo para liberar espacio de direcciones IP, simplificar la administración de direcciones IP, prepararse para los cambios en la red o cumplir con los requisitos de cumplimiento normativo. El desaprovisionamiento del CIDR de un grupo permite un mejor control y optimización de las asignaciones de direcciones IP dentro del IPAM y, al mismo tiempo, garantiza que el espacio de IP no utilizado se recupere y esté disponible para su uso futuro. No puede anular el aprovisionamiento del CIDR si hay asignaciones en el grupo. Para eliminar asignaciones, consulte the section called “Liberar una asignación”.

Siga los pasos de esta sección para anular el aprovisionamiento de CIDR de un grupo de IPAM. Al anular el aprovisionamiento de todos los CIDR de grupo, el grupo ya no se puede utilizar para asignaciones. En primer lugar, debe aprovisionar un nuevo CIDR al grupo antes de poder utilizar el grupo para asignaciones.

AWS Management Console

Para anular el aprovisionamiento de un CIDR de grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).

3. En el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. En el panel de contenido, seleccione el grupo cuyos CIDR desea anular el aprovisionamiento.
5. Elija la pestaña CIDR.
6. Seleccione uno o varios CIDR y elija Deprovision CIDRs (Anular el aprovisionamiento de CIDR).
7. Elija Deprovision CIDR (Anular el aprovisionamiento de CIDR).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para anular el aprovisionamiento de un CIDR de grupo:

1. Para obtener un ID de grupo de IPAM: describe-ipam-pools
2. Para ver los CIDR actuales del grupo: get-ipam-pool-cidrs.
3. Para anular el aprovisionamiento de CIDR: deprovision-ipam-pool-cidr.
4. Para ver los CIDR actualizados: get-ipam-pool-cidrs.

Para aprovisionar un nuevo CIDR al grupo, consulte Anular el aprovisionamiento del CIDR de un grupo. Si desea eliminar el grupo, consulte Eliminar un grupo.

Edición de un grupo del IPAM

Puede que desee editar un grupo para hacer alguna de las siguientes acciones:

- Cambiar las reglas de asignación del grupo. Para obtener más información acerca de las reglas de asignación, consulte Creación de un grupo IPv4 de nivel superior.
- Modificar el nombre, la descripción u otros metadatos del grupo para mejorar la organización y la visibilidad en el IPAM.

- Cambiar las opciones del grupo, como la importación automática de los recursos detectados, para optimizar la administración automatizada de direcciones IP del IPAM.

Siga los pasos de esta sección para editar un grupo de IPAM.

AWS Management Console

Para editar un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, se selecciona el alcance privado predeterminado. Si no desea utilizar el alcance privado predeterminado, en el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte . Cómo funciona IPAM
4. En el panel de contenido, elija el grupo donde desee editar un CIDR.
5. Elija Actions (Acciones) > Edit (Editar).
6. Realice los cambios que necesite en los grupos. Para obtener más información acerca de las opciones de configuración de grupos, consulte Creación de un grupo IPv4 de nivel superior.
7. Elija Update (Actualizar).

Command line

Utilice los siguientes comandos de la AWS CLI para editar un grupo:

1. Para obtener un ID de grupo de IPAM: describe-ipam-pools
2. Para modificar el grupo: modific-ipam-pool

Habilitar distribución de costos

Cuando habilita la distribución de costos, distribuye los cargos por las direcciones IP activas a las cuentas que utilizan las direcciones IP y no al propietario del IPAM. Esto resulta útil para las grandes organizaciones en las que el administrador delegado de IPAM administra las direcciones IP de forma centralizada mediante el IPAM y cada cuenta es responsable de su propio uso, lo que elimina la necesidad de realizar cálculos de facturación manuales.

La opción de distribución de costos está disponible al crear un IPAM o al modificar un IPAM en el modo de medición, donde:

- Propietario del IPAM (predeterminado): a la cuenta AWS propietaria del IPAM se le cobran todas las direcciones IP activas administradas en IPAM.
- Propietario del recurso: la cuenta AWS propietaria de la dirección IP paga por la dirección IP activa.

Requisitos

- Su IPAM debe estar integrado con Organizaciones AWS.
- El IPAM debe haber sido creado por el administrador delegado de IPAM de su organización AWS.
- La región de origen del IPAM debe ser una región que esté habilitada de forma predeterminada. No puede ser una región de suscripción voluntaria.

Cómo funciona la carga

- Si bien puede distribuir los cargos por direcciones IP dentro de una organización, todos los cargos de IPAM se consolidan en la cuenta de pagador de la organización mediante la facturación unificada de Organizations AWS.
- Cuando la distribución de costos está habilitada, las cuentas de los miembros de la organización pueden seguir viendo su uso y los cargos individuales de la IPAM en sus facturas de cuentas.
- El ARN de IPAM aparecerá en las facturas de las cuentas individuales cuando la distribución de costos esté habilitada, lo que permite a los propietarios de los recursos rastrear su uso de IP activa de IPAM. Si lo usa Exportaciones de datos de AWS, los cargos de IPAM aparecen con el ARN de IPAM asociado en las facturas de cuentas individuales y consolidadas.
- Solo las cuentas de la organización del administrador delegado pueden recibir cargos por los recursos que poseen. Los costos de las direcciones IP ajenas a la organización corren a cargo del propietario de la IPAM.

Restricciones horarias

- Tiene 24 horas para excluirse después de habilitar la distribución de costos. Transcurridas 24 horas, no podrá cambiar la configuración durante 7 días. Después de 7 días, puede deshabilitar la distribución de costos.

Integración de VPC IPAM con la infraestructura de Infoblox

La integración entre IPAM de Amazon VPC e Infoblox conecta el Administrador de direcciones IP (IPAM) de AWS VPC con Infoblox, lo que permite administrar las direcciones IP de AWS mediante los flujos de trabajo existentes de Infoblox y, al mismo tiempo, obtener capacidades nativas de AWS en la nube.

Esta integración resuelve un desafío común en las empresas: evitar la duplicación de sistemas de administración de direcciones IP. En lugar de aprender nuevas herramientas y mantener procesos independientes para AWS y las instalaciones, puede designar Infoblox como la autoridad de administración para los ámbitos de IPAM de Amazon VPC y continuar el uso de la interfaz conocida de Infoblox para todas las operaciones relacionadas con las direcciones IP.

Información general sobre el proceso de integración

Los pasos siguientes ofrecen una visión general de todo el proceso de integración:

1. Configuración del ámbito de IPAM (descrito en este documento): el administrador delegado de IPAM de Amazon VPC crea un ámbito nuevo o modifica uno existente para usar Infoblox como autoridad externa.
2. Configuración de Infoblox (descrito fuera de este documento): consulte Siguientes pasos.
3. Creación de un grupo de nivel superior: el administrador delegado de IPAM de Amazon VPC crea un grupo dentro del ámbito que está vinculado a Infoblox. El grupo se crea inicialmente sin ningún CIDR asignado.
4. Aprovisionamiento de CIDR desde la autoridad externa: el administrador delegado de IPAM Amazon VPC aprovisiona un CIDR para el grupo. Puede solicitar cualquier CIDR disponible (Infoblox selecciona uno dentro del rango permitido) o solicitar un CIDR específico (Infoblox lo acepta o lo rechaza según la disponibilidad). IPAM se coordina automáticamente con Infoblox para obtener y aprovisionar el CIDR aprobado.
5. Continúe con las operaciones estándar de IPAM: crear grupos secundarios y VPC a partir del CIDR asignado mediante los procedimientos habituales de IPAM de Amazon VPC.

Uso de esta integración

Use esta integración si ya utiliza Infoblox, o tiene previsto hacerlo, para la administración de redes en las instalaciones y desea ampliar sus prácticas actuales de administración de direcciones IP a AWS sin mantener sistemas independientes.

Requisitos previos

Antes de configurar esta integración, asegúrese de contar con lo siguiente:

- El nivel avanzado de IPAM de VPC habilitado en la cuenta de AWS. Para obtener más información, consulte la documentación del Nivel avanzado de IPAM de VPC.
- Los permisos de IAM obligatorios que se detallan a continuación.
- Identificador del recurso de Infoblox: este ID lo proporciona el administrador de Infoblox

Rol de IAM para Infoblox

Cree un rol de IAM para que la entidad principal de Infoblox lo asuma. De otro modo, utilice un rol existente. El rol debe contar con los siguientes permisos:

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

Para obtener instrucciones sobre cómo agregar estos permisos a un rol o a una política de IAM, consulte Cómo agregar y eliminar permisos de identidades de IAM en la Guía del usuario de IAM.

> **Note**
>
> Además de los permisos necesarios para habilitar esta integración, es posible que Infoblox requiera permisos adicionales para la detección de IPAM de VPC.

Configuración de la integración de Infoblox en IPAM de VPC

Puede habilitar la integración con Infoblox al crear o modificar ámbitos desde la consola de IPAM de AWS VPC o mediante la AWS CLI.

> **Important**
>
> La integración con Infoblox solo está disponible para ámbitos privados; no es compatible con ámbitos públicos.

Creación de un ámbito nuevo con integración con Infoblox

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione IPAM y, a continuación, seleccione Ámbitos.
3. Elija Create scope (Crear alcance).
4. En Configuración del ámbito, realice lo siguiente:
   - El ID de IPAM se completa automáticamente.
   - (Opcional) En Nombre, introduzca un nombre para el ámbito.
   - (Opcional) En Descripción, introduzca una descripción para el ámbito.
5. En Autoridad del ámbito, seleccione Infoblox IPAM.
6. En Identificador del recurso de Infoblox, introduzca el identificador del recurso de Infoblox en el formato `<version>.identity.account.<entity_realm>.<entity_id>`.
7. Verifique que cuenta con los permisos de IAM necesarios, tal como se muestra en el cuadro de información.
8. Elija Create scope (Crear alcance).

El comando AWS CLI relacionado para esta acción es create-ipam-scope.

Modificación de ámbitos existentes

Para cambiar la autoridad del ámbito de IPAM de Amazon VPC a Infoblox IPAM en un ámbito existente, edite la configuración del ámbito y siga los mismos pasos de configuración descritos en el procedimiento anterior.

El comando AWS CLI relacionado para esta acción es modify-ipam-scope.

Siguientes pasos

Esta acción completa la configuración de IPAM de Amazon VPC necesaria para la integración. Después de configurar la autoridad del ámbito, puede crear un grupo de IPAM de nivel superior

dentro de ese ámbito. Para obtener más información, consulte Creación de un grupo IPv4 de nivel superior.

La integración también requiere configurar un grupo de origen de Infoblox, verificar el estado del trabajo de detección, establecer el ámbito privado para que sea administrado por Infoblox, habilitar la administración de Infoblox para IPAM de Amazon VPC y crear grupos ya sea desde la integración con Infoblox o directamente desde el portal de Infoblox.

Para obtener información sobre el componente de Infoblox de la integración, consulte la Guía del usuario de la integración de IPAM de AWS en la documentación de Infoblox.

Habilitar el aprovisionamiento de CIDR GUA IPv6 privados

Si desea que sus redes privadas admitan IPv6 y no tiene intención de enrutar el tráfico de estas direcciones a Internet, puede aprovisionar un rango GUA o ULA de IPv6 a un grupo IPAM en un alcance privado.

Para obtener información importante sobre el direccionamiento IPv6 privado, consulte Direcciones IPv6 privadas en la Guía del usuario de Amazon VPC.

Hay dos tipos de direcciones IPv6 privadas:

- Intervalos ULA de IPv6: direcciones IPv6 tal como se definen en el RFC4193. Estos rangos de direcciones siempre comienzan por “fc” o “fd”, lo que los hace fácilmente identificables. El espacio ULA de IPv6 válido es cualquier espacio inferior a fd00::/8 que no se superponga con el rango reservado de Amazon fd00::/16.
- Intervalos GUA de IPv6: direcciones IPv6 tal como se definen en el RFC3587. La opción de usar rangos GUA de IPv6 como direcciones IPv6 privadas está deshabilitada de forma predeterminada y debe estar habilitada antes de poder usarla.

Para utilizar un rango de direcciones ULA de IPv6, debe elegir la opción IPv6 al aprovisionar un CIDR a un grupo de IPAM e introducir el rango de ULA de IPv6. Sin embargo, para usar sus propios rangos GUA de IPv6 como direcciones IPv6 privadas, primero debe completar los pasos de esta sección. La opción se deshabilita de forma predeterminada.

Note

- Cuando utilice rangos GUA de IPv6 privados, requerimos que utilice los rangos GUA de IPv6 de su propiedad.
- El IPAM detecta recursos con direcciones ULA y GUA de IPv6 y supervisa los grupos en busca de espacios de direcciones ULA y GUA de IPv6 superpuestos.
- Si desea conectarse a Internet desde un recurso que tenga una dirección IPv6 privada, puede hacerlo, pero para ello debe enrutar el tráfico a través de un recurso de otra subred con una dirección IPv6 pública.
- Si tiene un rango GUA de IPv6 privado asignado a una VPC, no puede usar el espacio GUA de IPv6 público que se superponga al espacio GUA de IPv6 privado de la misma VPC.
- Se admite la comunicación entre recursos con rangos de direcciones ULA y GUA IPv6 privados (por ejemplo, a través de Direct Connect, emparejamiento de VPC, puerta de enlace de tránsito o conexiones VPN).
- Un rango GUA de IPv6 privado no se puede convertir en un rango GUA de IPv6 anunciado públicamente.

AWS Management Console

Para habilitar el aprovisionamiento de CIDR GUA de IPv6 privados

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija IPAMs (IPAM).
3. Elija su IPAM y después Acciones > Editar.
4. En CIDR GUA IPv6 privados, seleccione Habilitar el aprovisionamiento del espacio GUA CIDR en grupos de IPAM IPv6 privados.
5. Seleccione Save changes (Guardar cambios).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Use los siguientes comandos de AWS CLI para habilitar el aprovisionamiento de CIDRs GUA de IPv6 privados:

1. Ver los IPAM actuales con describe-ipams
2. Modifique el IPAM con modify-ipam e incluya la opción de `enable-private-gua`.

Una vez habilitada la opción de aprovisionar CIDR GUA de IPv6 privados, puede aprovisionar un CIDR GUA de IPv6 privado a un grupo. Para obtener más información, consulte Aprovisionamiento de CIDR en un grupo.

Aplicación del uso del IPAM para la creación de VPC con SCP

> **Note**
>
> Esta sección solo se aplica si ha habilitado la integración de IPAM con AWS Organizations. Para obtener más información, consulte Integración de IPAM con cuentas en una organización de AWS.

En esta sección se describe cómo crear una política de control de servicios en AWS Organizations que exige que los miembros de su organización usen IPAM al crear una VPC. Las políticas de control de servicios (SCP) son un tipo de política de organización que le permite administrar permisos en su organización. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.

Aplicar IPAM al crear VPC

Siga los pasos de esta sección para exigir a los miembros de su organización que usen IPAM al crear VPC.

Para crear una SCP y restringir la creación de VPC a IPAM

1. Siga los pasos de Creación de una política de control de servicios en la Guía del usuario de AWS Organizations e ingrese el siguiente texto en el editor de JSON:

   JSON

```
{
```

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

2. Adjunte la política a una o más unidades organizativas de su organización. Para obtener más información, consulte Asociar y Desasociar políticas en la Guía del usuario de AWS Organizations.

Aplicar un grupo de IPAM al crear VPC

Siga los pasos de esta sección para exigir a los miembros de su organización que usen un grupo de IPAM específico al crear VPC.

Para crear una SCP y restringir la creación de VPC a un grupo de IPAM

1. Siga los pasos de Creación de una política de control de servicios en la Guía del usuario de AWS Organizations e ingrese el siguiente texto en el editor de JSON:

   JSON

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

```
}
```

2. Cambie el valor de ejemplo `ipam-pool-0123456789abcdefg` del ID de grupo IPv4 que desea restringir a los usuarios.
3. Adjunte la política a una o más unidades organizativas de su organización. Para obtener más información, consulte Asociar y Desasociar políticas en la Guía del usuario de AWS Organizations.

Aplicar IPAM a todas las OU excepto a una lista determinada

Siga los pasos de esta sección para aplicar IPAM a todas las Unidades Organizativas (OU) excepto a una lista determinada. La política que se describe en esta sección requiere OU en la organización, excepto las OU que usted especifique en `aws:PrincipalOrgPaths` para usar IPAM para crear y expandir VPC. Las OU listadas pueden utilizar IPAM al crear VPC o especificar un rango de direcciones IP manualmente.

Para crear un SCP y aplicar IPAM a todas las OU excepto a una lista determinada

1. Siga los pasos de Creación de una política de control de servicios en la Guía del usuario de AWS Organizations e ingrese el siguiente texto en el editor de JSON:

   JSON

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

```
    }]
}
```

2. Elimine los valores de ejemplo (como `o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/`) y añada las rutas de las entidades de las organizaciones AWS de las OU que desee que tengan la opción (pero no la obligación) de utilizar IPAM. Para más información sobre las rutas de entidad, consulte Descripción de la ruta de identidad de AWS Organizations y aws:PrincipalOrgPaths en la Guía del usuario de IAM.
3. Asocie la política a la raíz de su organización. Para obtener más información, consulte Asociar y Desasociar políticas en la Guía del usuario de AWS Organizations.

Excluir las unidades organizativas del IPAM

Si su IPAM está integrado con AWS Organizations, ahora puede excluir de la administración del IPAM a una unidad organizativa (OU). Al excluir una OU, el IPAM no administrará las direcciones IP de las cuentas de esa OU. Esta característica le ofrece mayor flexibilidad a la hora de utilizar el IPAM.

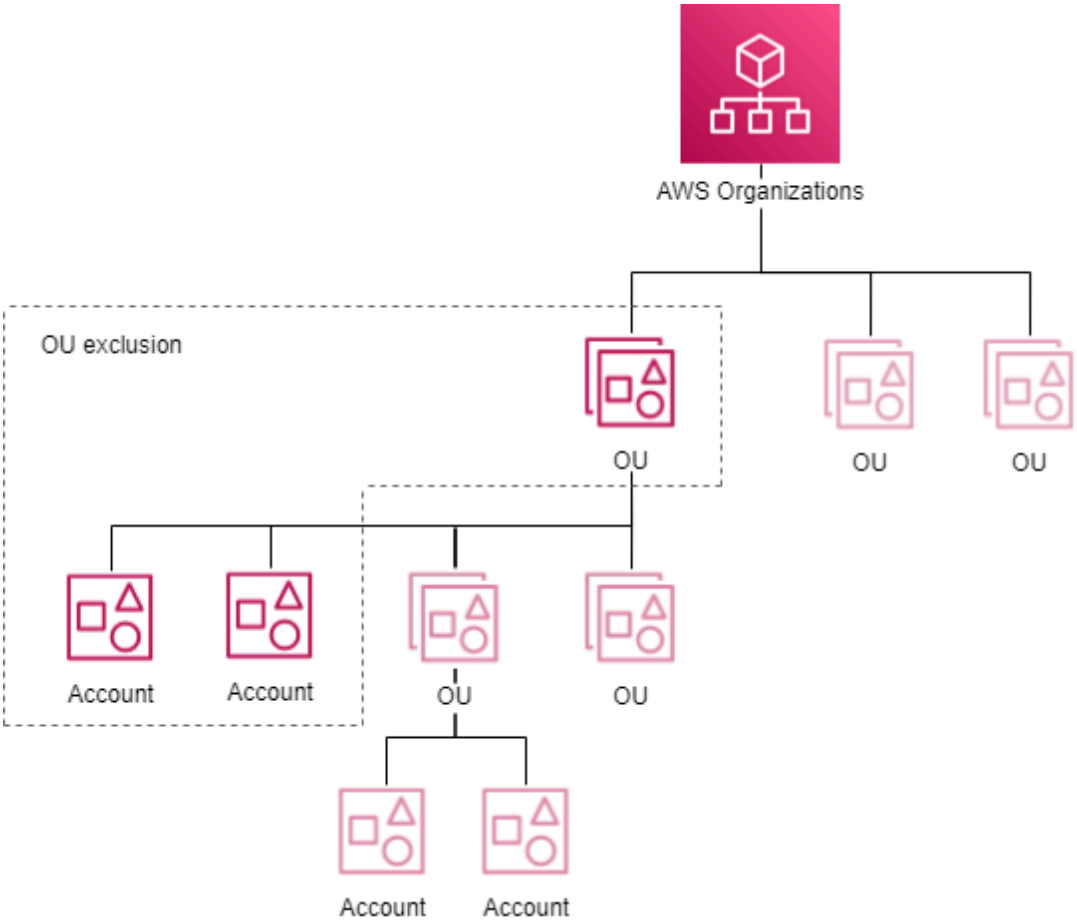
Puede usar las exclusiones de OU de las siguientes maneras:

- Habilite el IPAM para partes específicas de su empresa: si tiene varias unidades de negocio o subsidiarias en AWS Organizations, ahora puede usar el IPAM solo para las que lo necesiten.
- Mantenga sus cuentas de entorno de pruebas separadas: puede excluir sus cuentas de entorno de pruebas del IPAM y centrarse únicamente en las cuentas que realmente importan para la administración de su IP.

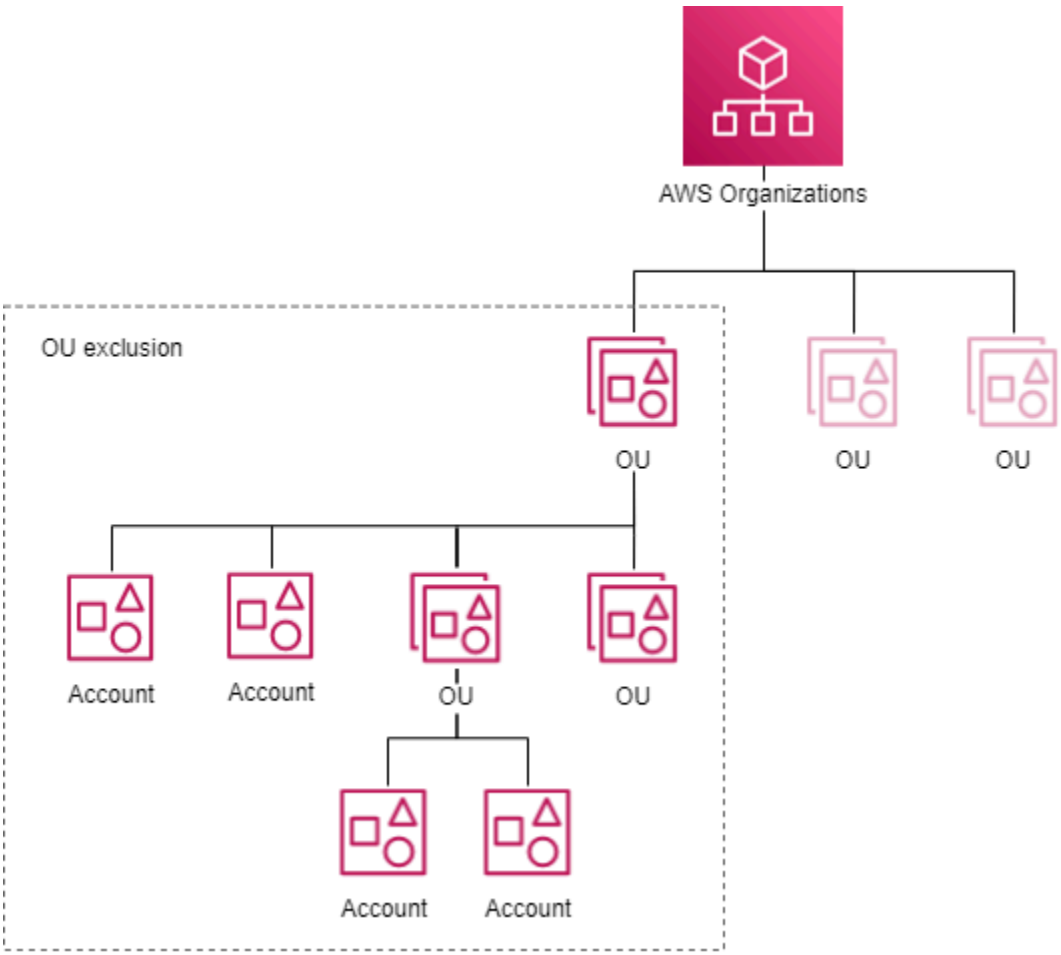
Cómo funcionan las exclusiones de OU

En los diagramas de esta sección, se muestran dos casos de uso para agregar exclusiones de OU en el IPAM.

En el primer diagrama, se muestra el impacto de añadir una exclusión de unidad organizativa (OU) únicamente en una OU principal. Como resultado, el IPAM no administrará las direcciones IP de las cuentas de la OU principal. El IPAM administrará las direcciones IP de las cuentas de las demás OU fuera de la exclusión.



En el segundo diagrama, se muestra el impacto de añadir una exclusión de unidad organizativa (OU) en una OU principal y en todas las OU secundarias. En consecuencia, el IPAM no administrará las direcciones IP de las cuentas de la OU principal ni de las cuentas de ninguna OU secundaria. El IPAM administrará las direcciones IP de las cuentas de las OU fuera de la exclusión.



Añadir o eliminar exclusiones de OU

Complete los pasos de esta sección para añadir o eliminar exclusiones de OU.

> **Note**
>
> - La cuenta de administrador de IPAM delegada no está excluida, incluso si se encuentra dentro de una OU excluida.
> - Su IPAM debe estar integrado con AWS Organizations para añadir una exclusión de OU. La organización debe tener OU integradas.
> - Debe ser el administrador delegado del IPAM para ver, añadir o eliminar las exclusiones de OU.
> - El IPAM tarda un tiempo en descubrir las unidades organizativas creadas recientemente.

- Hay una cuota predeterminada del número de exclusiones que puede añadir por detección de recursos. Para obtener más información, consulte Exclusiones de unidades organizativas por detección de recursos en Cuotas de IPAM.
- Si comparte la detección de un recurso con otra cuenta, esa cuenta puede ver las exclusiones de OU que contiene, entre otras cosas, el identificador de la organización, el identificador raíz y los identificadores de las unidades organizativas de la organización del propietario de la detección de recursos.

AWS Management Console

Para añadir o eliminar exclusiones de OU

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Detecciones de recursos.
3. Elija su detección de recursos predeterminada.
4. Elija Edit (Edición de).
5. En Exclusiones de unidades organizativas, haga lo siguiente:
   - Para añadir una exclusión de OU:
     - Si desea excluir la OU y todas sus OU secundarias:
       - Busque la OU en la tabla y marque la casilla de verificación. Todas las OU secundarias se seleccionan automáticamente.
     - Si desea excluir únicamente las cuentas de OU principales:
       - Busque la OU en la tabla y marque la casilla de verificación. Todas las OU secundarias se seleccionan automáticamente. Deseleccione todas las OU secundarias.
     - Como alternativa, puede usar la columna Acciones para seleccionar solo una OU principal o una OU principal y secundaria:
       - Seleccionar todas las OU secundarias: incluya las OU secundarias en la exclusión. Al elegir una OU, esta se añade a la pantalla. Cada OU contiene el identificador y la ruta de la entidad de la exclusión de la OU.
       - Seleccionar solo esta OU: incluya solo esta OU en la exclusión. Al elegir una OU, esta se añade a la pantalla. Cada OU contiene el identificador y la ruta de la entidad de la exclusión de la OU.

- Copiar la ruta de la entidad de la OU: copie la ruta de la entidad organizativa para utilizarla según sea necesario.

- Si ya conoce la ruta de la entidad de AWS Organizations o quiere crearla:
  - Elija Introducir la exclusión de la unidad organizativa e ingrese la ruta de la entidad de la exclusión de la OU. Cree la ruta para las OU utilizando los identificadores de AWS Organizations separados por una `/`. Incluya todas las OU secundarias terminando la ruta con `/*`.
    - Ejemplo 1
      - Ruta hacia una OU secundaria: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
      - En este ejemplo, `o-a1b2c3d4e5` es el ID de la organización, `r-f6g7h8i9j0example` es el ID raíz, `ou-ghi0-awsccccc` es un ID de OU y `ou-jkl0-awsddddd` es un ID de OU secundaria.
      - El IPAM no administrará las direcciones IP de las cuentas de la OU secundaria.
    - Ejemplo 2
      - Ruta en la que todas las OU secundarias formarán parte de la exclusión: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
      - En este ejemplo, el IPAM no administrará las direcciones IP de las cuentas de la OU (`ou-ghi0-awsccccc`) ni de las cuentas de ninguna OU que sea secundaria a la OU.
- Para eliminar una exclusión de una OU:
  - Seleccione la X situada junto a una OU que ya se haya añadido. El `/*` que aparece después del ID de la OU indica que se trata de una OU principal y que las secundarias forman parte de la exclusión.

6. Seleccione Save changes (Guardar cambios).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

1. Consulte los detalles de la detección de recursos para obtener el ID de la detección de recursos predeterminada para el siguiente paso con describe-ipam-resource-discovery.

Input:

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

Salida:

```
{

    "IpamResourceDiscoveries": [

        {

            "OwnerId": "111122223333",

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

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

            "OperatingRegions": [

                {

                    "RegionName": "us-east-1"

                },

                {

                    "RegionName": "us-west-1"

                },

                {

                    "RegionName": "us-west-2"

                }

            ],
```

```
            "IsDefault": true,

            "State": "modify-complete",

            "Tags": []

        }

    ]

}
```

2. Añada o elimine una exclusión de unidades organizativas de una detección de recursos con modify-ipam-resource-discovery y las opciones `--add-organizational-unit-exclusions` o `--remove-organizational-unit-exclusions`. Deberá introducir una ruta de entidad de AWS Organizations. Cree la ruta para las OU utilizando los identificadores de AWS Organizations separados por una `/`. Incluya todas las OU secundarias terminando la ruta con `/*`. No puede incluir la misma ruta de entidad más de una vez en los parámetros de adición o eliminación.

   - Ejemplo 1
     - Ruta hacia una OU secundaria: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd/`
     - En este ejemplo, `o-a1b2c3d4e5` es el ID de la organización, `r-f6g7h8i9j0example` es el ID raíz, `ou-ghi0-awsccccc` es un ID de OU y `ou-jkl0-awsddddd` es un ID de OU secundaria.
     - El IPAM no administrará las direcciones IP de las cuentas de la OU secundaria.
   - Ejemplo 2
     - Ruta en la que todas las OU secundarias formarán parte de la exclusión: `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/*`
     - En este ejemplo, el IPAM no administrará las direcciones IP de las cuentas de la OU (`ou-ghi0-awsccccc`) ni de las cuentas de ninguna OU que sea secundaria a la OU.

> **Note**
>
> El conjunto de exclusiones resultante no debe “superponerse”, lo que significa que dos o más exclusiones de unidades organizativas no deben excluir la misma unidad organizativa.
> Ejemplo de rutas de entidades que no se superponen:
>
> - Ruta 1 =“o-1/r-1/ou-1/”
> - Ruta 2 =“o-1/r-1/ou-1/ou-2/”
>
> Estas rutas no se superponen porque la ruta 1 solo excluye las cuentas incluidas en ou-1 y la ruta 2 solo excluye las cuentas en ou-2.
> Ejemplo de rutas de entidades que se superponen:
>
> - Ruta 1 =“o-1/r-1/ou-1/*”
> - Ruta 2 =“o-1/r-1/ou-1/ou-2/”
>
> Estas rutas se superponen porque la ruta 1 representa tanto “o-1/r-1/ou-1/” como “o-1/r-1/ou-1/ou-2/”, y “o-1/r-1/ou-1/ou-2/” se superpone a la ruta 2.

Input:

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

Salida:

```
{
    "IpamResourceDiscovery": {
        "OwnerId": "111122223333",
```

```
        "IpamResourceDiscoveryId": "ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryArn": "arn:aws:ec2::111122223333:ipam-resource-
discovery/ipam-res-disco-1234567890abcdef0",
        "IpamResourceDiscoveryRegion": "us-east-1",
        "OperatingRegions": [
            {
                "RegionName": "us-east-1"
            }
        ],
        "IsDefault": false,
        "State": "modify-in-progress",
        "OrganizationalUnitExclusions": [
            {
                "OrganizationsEntityPath": "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-
ghi0-awsccccc/*"
            }
        ]
    }
}
```

Modificar un nivel de IPAM

El IPAM ofrece dos niveles: el nivel gratuito y el nivel avanzado. El cambio al nivel avanzado del Administrador de direcciones IP de Amazon VPC proporciona un control más detallado de la administración de direcciones IP. Esto puede resultar beneficioso a medida que aumenta la complejidad de su red, ya que le permite optimizar y administrar mejor su espacio de direcciones IP. Para obtener más información sobre las características disponibles en el nivel gratuito y los costos asociados al nivel avanzado, consulte la pestaña de IPAM en la Página de precios de Amazon VPC.

Note

Antes de poder cambiar del nivel avanzado al nivel gratuito, debe:

- Eliminar los grupos de alcance privado.
- Eliminar los alcances privados no predeterminados.
- Eliminar los grupos con configuraciones regionales distintas de la región de origen del IPAM.
- Eliminar las asociaciones de detección de recursos no predeterminadas.

- Eliminar las asignaciones de grupos a cuentas que no sean del propietario del IPAM.

AWS Management Console

Para modificar el nivel de IPAM

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija IPAMs (IPAM).
3. En el panel de contenido, seleccione su IPAM.
4. Elija Actions (Acciones) > Edit (Editar).

> **Note**
>
> Si utiliza el nivel gratuito, verá la leyenda El recuento estimado total de IP activas de IPAM es...
> El recuento total de IP activas es la cantidad de direcciones IP activas en su IPAM que se le cobraría si pasara del nivel gratuito al nivel avanzado. Una dirección IP activa se define como una dirección IP o un prefijo asociados con una interfaz de red elástica (ENI) que está asignada a un recurso, como una instancia de EC2.
>
> - Esta métrica solo está disponible para los clientes del nivel gratuito.
> - Si su IPAM está integrado con AWS Organizations, el recuento de IP activas cubre todas las cuentas de la organización.
> - No se puede ver un desglose del recuento de IP activas por tipo de IP (pública/privada) o por clase (IPv4/IPv6).
> - El IPAM solo cuenta las IP de las ENI que son propiedad de las cuentas supervisadas. Es posible que el recuento no sea exacto en el caso de las subredes compartidas. Las direcciones IP se excluyen si el propietario de la subred o de la ENI no está cubierto por el IPAM.

5. Elija el Nivel de IPAM que desea utilizar para el IPAM.
6. Seleccione Save changes (Guardar cambios).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para ver y modificar un nivel de IPAM:

1. Para ver los IPAM actuales: describe-ipams.
2. Modificar el nivel de IPAM: modify-ipam
3. Para ver los IPAM actualizados: describe-ipams

Modificar las regiones operativas del IPAM

Las regiones operativas son regiones AWS en las que el IPAM puede administrar los CIDR de dirección IP. IPAM solo descubre y monitorea los recursos en las regiones de AWS que selecciona como regiones operativas.

Agregar una región operativa a un IPAM le permite administrar el espacio de direcciones IP en varias regiones de AWS. Esto puede mejorar la utilización de las direcciones IP, permitir la segmentación regional y respaldar una infraestructura distribuida geográficamente. La ampliación del alcance regional del IPAM proporciona una mayor flexibilidad y control sobre la administración general de direcciones IP.

AWS Management Console

Para modificar las regiones operativas del IPAM

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija IPAMs (IPAM).
3. En el panel de contenido, seleccione su IPAM.
4. Elija Actions (Acciones) > Edit (Editar).
5. En Configuración del IPAM, elija las Regiones operativas que desea utilizar para el IPAM.
6. Seleccione Save changes (Guardar cambios).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para ver y modificar las regiones operativas del IPAM:

1. Para ver los IPAM actuales: describe-ipams.
2. Agregar o eliminar regiones operativas del IPAM: modify-ipam
3. Para ver los IPAM actualizados: describe-ipams

Aprovisionamiento de CIDR en un grupo

Siga los pasos de esta sección para aprovisionar CIDR en un grupo. Si ya aprovisionó un CIDR al crear el grupo, es posible que tenga que aprovisionar CIDR adicionales si un grupo se acerca a la asignación completa. Para monitorear el uso del grupo, consulte Monitorear el uso de CIDR con el panel de IPAM.

> **Note**
>
> A lo largo de esta guía del usuario y en la consola de IPAM se utilizan los términos aprovisionar y asignar. Aprovisionar se utiliza cuando se agrega un CIDR a un grupo de IPAM. Asignar se utiliza cuando asocia un CIDR de un grupo de IPAM con una VPC o una dirección IP elástica.

AWS Management Console

Para aprovisionar CIDR en un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, se selecciona el alcance privado predeterminado. Si no desea utilizar el alcance privado predeterminado, en el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte . Cómo funciona IPAM.

4. En el panel de contenido, elija el grupo al que desee agregarle un CIDR.
5. Elija Actions > Provision CIDRs (Acciones > Aprovisionar CIDR).
6. Realice una de las siguientes acciones:

   - Si va a aprovisionar un CIDR a un grupo del ámbito público, introduzca la máscara de red.
   - Si va a aprovisionar un CIDR a un grupo de IPv4 del ámbito privado, introduzca el CIDR.
   - Si va a aprovisionar un CIDR a un grupo de IPv6 del ámbito privado, tenga en cuenta lo siguiente:
     - Para obtener información importante sobre el direccionamiento IPv6 privado, consulte Direcciones IPv6 privadas en la Guía del usuario de Amazon VPC.
     - Para usar un rango de ULA de IPv6 privado, en CIDR para aprovisionar, elija Agregar CIDR de ULA por máscara de red y elija un tamaño de máscara de red o elija Ingresar CIDR de IPv6 privado e ingrese un rango de ULA. Los rangos válidos para la ULA de IPv6 privada son de /9 a /60, empezando por fd80::/9.
     - Para usar un rango GUA de IPv6 privado, primero debe haber activado la opción en su IPAM (consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados). Una vez que haya activado los CIDR GUA de IPv6 privados, introduzca un GUA de IPv6 en Introducir CIDR de IPv6 privado.

   > **Note**
   >
   > - De manera predeterminada, puede agregar un bloque de CIDR de IPv6 proporcionado por Amazon a un grupo regional. Para obtener información sobre cómo aumentar el límite predeterminado, consulte Cuotas de IPAM.
   > - Cada CIDR que desee aprovisionar debe estar disponible en el alcance.
   > - Si está aprovisionando CIDR en un grupo dentro de otro grupo, el espacio de CIDR que desee aprovisionar debe estar disponible en dicho grupo.

7. Elija Aprovisionar.
8. Puede ver el CIDR en IPAM al seleccionar Pools (Grupos) en el panel de navegación, elegir un grupo y visualizar la pestaña de CIDR del grupo.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para aprovisionar los CIDR en un grupo:

1. Para obtener el ID de un grupo de IPAM: describe-ipam-pools
2. Para obtener los CIDR que se aprovisionan en el grupo: get-ipam-pool-cidrs
3. Para aprovisionar un nuevo CIDR en el grupo: provision-ipam-pool-cidr
4. Para obtener los CIDR que se aprovisionan en el grupo y ver el nuevo CIDR: get-ipam-pool-cidrs

Mover CIDR de VPC entre alcances

Trasladar los CIDR de un ámbito a otro le permite optimizar la asignación de direcciones IP, organizarlas por región, separar las preocupaciones, garantizar el cumplimiento y adaptarse a los cambios en la infraestructura. Esta flexibilidad lo ayuda a administrar su espacio de direcciones IP de manera eficiente a medida que sus cargas de trabajo evolucionan.

Siga los pasos de esta sección para mover un CIDR de VPC de un alcance a otro.

⚠ Important

- Solo puede mover los CIDR de VPC. Al mover un CIDR de VPC, los CIDR de subred de la VPC también se mueven automáticamente.
- Solo puede mover CIDR de VPC de un alcance privado a otro. No se pueden mover los CIDR de VPC de un alcance público a un alcance privado o de un alcance privado a otro público.
- La misma cuenta de AWS debe ser propietaria de ambos alcances.
- Si un CIDR de VPC se asigna actualmente desde un grupo de ámbito privado, la solicitud de movimiento se realiza correctamente, pero el CIDR de VPC no se moverá hasta que libere la asignación CIDR de VPC del grupo actual. Para obtener información sobre cómo liberar una asignación, consulte Liberar una asignación.

AWS Management Console

Para mover un CIDR asignado a una VPC

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Resources (Recursos).
3. En el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar.
4. En el panel de contenido, elija una VPC y vea sus detalles.
5. En VPC CIDRs (CIDR de VPC), seleccione uno de los CIDR asignados al recurso y elija Actions (Acciones) >Move CIDR to different scope (Mover CIDR a un alcance diferente).
6. Seleccione el alcance al que desea mover el CIDR de VPC.
7. Elija Move CIDR to different scope (Mover CIDR a un ámbito diferente).

Command line

Usa los siguientes comandos de AWS CLI para mover un CIDR de VPC:

1. Para obtener un CIDR de VPC en el alcance actual: get-ipam-resource-cidrs
2. Para mover un CIDR de VPC: modify-ipam-resource-cidr
3. Para obtener un CIDR de VPC en el otro alcance: get-ipam-resource-cidrs

Definición de la estrategia de asignación de IPv4 pública con políticas de IPAM

Una política de IPAM es un conjunto de reglas que definen cómo se asignan a los recursos de AWS las direcciones IPv4 públicas de los grupos de IPAM. Cada regla asigna un servicio de AWS a los grupos de IPAM que el servicio utilizará para obtener las direcciones IP. Una sola política puede tener varias reglas y aplicarse a varias regiones de AWS. Si el grupo de IPAM se queda sin direcciones, los servicios recurren a las direcciones IP proporcionadas por Amazon. Una política se puede aplicar a una cuenta de AWS individual o a una entidad dentro de AWS Organizations. Si usa el modelo “traiga su propia IP (BYOIP)”, podrá reducir los costos de IPv4 pública de AWS.

Cuándo usar las políticas de IPAM

Use las políticas de IPAM para:

- Reducir los costos de IPv4 pública mediante el uso de direcciones BYOIP
- Controlar de forma centralizada qué grupos de IP utilizan los recursos de AWS
- Garantizar una asignación de IP coherente en la organización

Funcionamiento

Cuando crea un recurso de AWS que necesita una dirección IP pública en una cuenta con políticas de IPAM aplicadas:

- IPAM comprueba las reglas de política en orden.
- Si una regla coincide con el tipo de recurso, IPAM asigna una dirección IP del grupo especificado.
- Si el grupo está vacío y el desbordamiento está habilitado, Amazon proporciona una dirección IP.
- Si ninguna regla coincide, se aplica el comportamiento predeterminado.

Servicios y recursos admitidos

Puede crear políticas de IPAM para definir cómo se asignan las direcciones IPv4 públicas de los grupos de IPAM a los siguientes servicios y recursos de AWS:

- Direcciones IP elásticas (EIP)
- Equilibradores de carga de aplicación (ALB)
- Amazon Relational Database Service (RDS)
- Puertas de enlace NAT regionales

> **Important**
>
> Si al crear un recurso de AWS selecciona un grupo de IPAM específico o un ID de asignación de EIP, esa selección anulará la política de IPAM.

Requisitos previos

- Un IPAM en la cuenta de administrador delegado con el nivel avanzado habilitado
- Un grupo de IPAM público con direcciones IPv4
- Permisos de IAM para operaciones de IPAM y EC2

Terminología

Política de IPAM

Una política de IPAM es un conjunto de reglas que definen cómo se asignan a los recursos de AWS las direcciones IPv4 públicas de los grupos de IPAM. Cada regla asigna un servicio de AWS a los grupos de IPAM que el servicio utilizará para obtener las direcciones IP. Una sola política puede tener varias reglas y aplicarse a varias regiones de AWS. Si el grupo de IPAM se queda sin direcciones, los servicios recurren a las direcciones IP proporcionadas por Amazon. Una política se puede aplicar a una cuenta de AWS individual o a una entidad dentro de AWS Organizations. Una política se puede aplicar a una cuenta de AWS individual o a una entidad dentro de AWS Organizations.

Reglas de asignación

Configuraciones opcionales dentro de una política de IPAM que asignan tipos de recursos de AWS a grupos de IPAM específicos. Si no se define ninguna regla, los tipos de recursos utilizan de forma predeterminada las direcciones IP proporcionadas por Amazon.

Target

Una cuenta de AWS individual o una entidad dentro de una organización de AWS a la que se puede aplicar una política de IPAM.

Paso 1: creación de una política de IPAM

Uso de la consola de AWS:

Siga estos pasos para crear una política de IPAM mediante la consola de AWS:

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación izquierdo, elija Políticas.
3. Elija Create Policy (Crear política).
4. Introduzca un nombre para la política (opcional).
5. Seleccione el IPAM que desea asociar a esta política.
6. (Opcional) Añada etiquetas.
7. Elija Create Policy (Crear política).

Uso de AWS CLI:

Utilice el comando create-ipam-policy.

Paso 2: agregar reglas de asignación

Después de crear la política, debe agregar reglas de asignación que definan cómo se asignan las direcciones IP:

Uso de la consola de AWS:

Siga estos pasos para agregar reglas de asignación mediante la consola de AWS:

1. En el panel de navegación izquierdo, elija Políticas.
2. Elija la política que creó en el paso anterior.
3. En la página de detalles de la política, seleccione la pestaña Reglas de asignación.
4. Seleccione Crear reglas de asignación.
5. Realice la Configuración del servicio:
   - Configuración regional: seleccione la región de AWS (us-east-1) o la zona local donde desea que se aplique esta política.
   - Tipo de recurso: seleccione el servicio o tipo de recurso de AWS para esta política (direcciones IP elásticas, instancias de bases de datos de RDS, equilibradores de carga de aplicación o puertas de enlace NAT en modo de disponibilidad regional).
6. Realice la Configuración de reglas:
   - Grupo de IPAM: seleccione el grupo de IPAM que proporcionará las direcciones IP.
   - Revise los detalles del grupo (configuración regional, origen de IP pública, espacio disponible y rangos CIDR disponibles).
7. (Opcional) Seleccione Agregar nueva regla para crear reglas adicionales.
8. Seleccione Crear regla de asignación.

Uso de AWS CLI:

Utilice el comando modify-ipam-policy-allocation-rules.

Paso 3: Habilitar la política

Especifique qué cuentas deben utilizar esta política.

Uso de la consola de AWS:

Siga estos pasos para habilitar la política mediante la consola de AWS:

1. En la página de detalles de la política, seleccione la pestaña Destinos.
2. Seleccione Administrar destinos de la política.
3. Realice una de las siguientes acciones:

   - Para el uso en una sola cuenta (IPAM no integrado con AWS Organizations), seleccione Habilitar para la cuenta.
   - Para IPAM integrado con AWS Organizations (cuando es el administrador delegado):
     - En la sección Estructura organizativa, seleccione las cuentas o las unidades organizativas donde desea aplicar esta política.
     - Marque la casilla Habilitado para cada destino.
     - Elija Save changes (Guardar cambios).
     - Importante: habilitar esta política reemplazará cualquier política de IPAM activa en las cuentas o unidades organizativas seleccionadas.

Uso de AWS CLI:

Use el comando enable-ipam-policy según la configuración:

Para el uso en una sola cuenta (IPAM no integrado con AWS Organizations):

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

En IPAM integrado con AWS Organizations (cuando es el administrador delegado), establezca una política que se dirija a una cuenta de la organización de AWS:

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

En IPAM integrado con AWS Organizations (cuando es el administrador delegado), establezca una política que se dirija a una unidad organizativa:

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

```
    --ipam-policy-id ipam-policy-12345678 \
    --organization-target-id ou-123
```

> **Important**
>
> Al habilitar esta política, se sustituirá cualquier política de IPAM activa en las cuentas o unidades organizativas seleccionadas.

Paso 4: probar la política

Cree un recurso nuevo del tipo que configuró (por ejemplo, una EIP) en una de las cuentas de destino. El recurso usará automáticamente una dirección IP del grupo de IPAM.

> **Important**
>
> Si al crear un recurso de AWS selecciona un grupo de IPAM específico o un ID de asignación de EIP, esa selección anulará la política de IPAM.

Paso 5: supervisar el uso

Compruebe el grupo de IPAM en la consola para ver las direcciones IP asignadas a los recursos.

Liberar una asignación

Si planea eliminar un grupo, es posible que tenga que liberar una asignación de grupo. Una asignación es una asignación de CIDR desde un grupo de IPAM a otro recurso o grupo de IPAM.

No se pueden eliminar grupos si tienen CIDR aprovisionados. No puede desaprovisionar los CIDR si están asignados a recursos.

> **Note**
>
> - Para liberar una asignación manual, siga los pasos de esta sección o llame a la API ReleaseIpamPoolAllocation.
> - Para liberar una asignación en un ámbito privado, debe ignorar o eliminar el CIDR del recurso. Para obtener más información, consulte Cambiar el estado de monitoreo de los

CIDR de VPC. Transcurrido un tiempo, IPAM de Amazon VPC liberará automáticamente la asignación en su nombre.

Example

Ejemplo

Si tiene un CIDR de VPC en un ámbito privado, para liberar la asignación debe ignorar o eliminar el CIDR de la VPC. Transcurrido un tiempo, IPAM de Amazon VPC liberará automáticamente la asignación del CIDR de la VPC desde el grupo del IPAM.

- Para liberar una asignación de un ámbito público, debe eliminar el CIDR del recurso. No puede ignorar los CIDR de recursos públicos. Para obtener más información, consulte Efectúe una limpieza en Lleve su propio CIDR IPv4 público a IPAM únicamente por medio de la AWS CLI o Efectúe una limpieza en Lleve su propio CIDR IPv6 a IPAM únicamente por medio de la AWS CLI. Transcurrido un tiempo, IPAM de Amazon VPC liberará automáticamente la asignación en su nombre.

Para que el IPAM de Amazon VPC libere asignaciones en su nombre, todos los permisos de la cuenta deben estar configurados correctamente para el uso de una sola cuenta o el uso de varias cuentas.

Cuando publica un CIDR administrado por su IPAM, IPAM de Amazon VPC recicla el CIDR en un grupo de IPAM. Si utiliza IPAM en el nivel avanzado, el CIDR tarda unos minutos en quedar disponible para futuras asignaciones. Si utiliza IPAM en el nivel gratuito, el CIDR tarda hasta 48 horas en quedar disponible para futuras asignaciones. Para obtener más información acerca de los grupos y las asignaciones, consulte Cómo funciona IPAM.

AWS Management Console

Para liberar una asignación de grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. En el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.

4. En el panel de contenido, elija el grupo en el que se encuentra la asignación.
5. Elija la pestaña Allocations (Asignaciones).
6. Seleccione una o varias asignaciones. Puede identificar las asignaciones por su tipo de recurso:
   - custom: una asignación personalizada.
   - vpc: una asignación de VPC.
   - ipam-pool: una asignación de grupos de IPAM.
   - ec2-public-ipv4-pool: asignación de grupos IPv4 públicos.
   - subred: una asignación de subred.
7. Elija Actions (Acciones) > Release custom allocation (Publicar asignación personalizada).
8. Elija Deallocate CIDR (Anular asignación de CIDR).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguientes comandos de la AWS CLI para liberar una asignación de grupo:

1. Para obtener un ID de grupo de IPAM: describe-ipam-pools
2. Para ver las asignaciones actuales en el grupo: get-ipam-pool-allocations
3. Para liberar una asignación: release-ipam-pool-assignation
4. Para consultar las asignaciones actualizadas: get-ipam-pool-allocations

Para agregar una nueva asignación, consulte Asignación de CIDR desde un grupo del IPAM. Para eliminar el grupo después de liberar las asignaciones, primero debe Anular el aprovisionamiento del CIDR de un grupo.

Compartir un grupo de IPAM mediante AWS RAM

Siga los pasos de esta sección para compartir un grupo de IPAM mediante AWS Resource Access Manager (RAM). Cuando comparte un grupo de IPAM con RAM, las “entidades principales” pueden asignar los CIDR del grupo a recursos de AWS, como VPC, desde sus respectivas cuentas. Una

entidad principal es un concepto de RAM que hace alusión a cualquier cuenta de AWS, rol de IAM o unidad organizativa de AWS Organizations. Para obtener más información, consulte Cómo compartir los recursos de AWS en la Guía del usuario de AWS RAM.

> **Note**
>
> - Solo puede compartir un grupo de IPAM con AWS RAM si ha integrado IPAM con AWS Organizations. Para obtener más información, consulte Integración de IPAM con cuentas en una organización de AWS. No se puede compartir un grupo de IPAM con AWS RAM si se es un usuario de IPAM de una sola cuenta.
> - Debe habilitar el uso compartido de recursos con AWS Organizations en AWS RAM. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM.
> - El uso compartido de RAM solo está disponible en la región de AWS de origen de IPAM. Debe crear el recurso compartido en la región de AWS en la que se encuentra IPAM, no en la región del grupo de IPAM.
> - La cuenta que cree y elimine recursos compartidos del grupo de IPAM debe tener los siguientes permisos en la política de IAM asociada a su rol de IAM:
>   - `ec2:PutResourcePolicy`
>   - `ec2:DeleteResourcePolicy`
> - Puede agregar varios grupos de IPAM a un recurso compartido de RAM.
> - Si bien puede compartir grupos de IPAM con cualquier cuenta de AWS fuera de una AWS Organization, IPAM solo supervisará las direcciones IP en cuentas fuera de Organization si el propietario de la cuenta ha seguido el proceso de compartir su detección de recursos con el administrador delegado de IPAM, tal como se describe en Integración de IPAM con cuentas ajenas a su organización.

AWS Management Console

Para compartir un grupo de IPAM mediante RAM

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).

3. De forma predeterminada, se selecciona el alcance privado predeterminado. Si no desea utilizar el alcance privado predeterminado, en el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. En el panel de contenido, elija el grupo que desea compartir y, luego, Actions >View details (Acciones > Ver detalles).
5. En Resource sharing (Uso compartido de recursos), elija Create resource share (Crear recursos compartidos). Como resultado, se abrirá la consola de AWS RAM. Creará el grupo compartido en AWS RAM.
6. Elija Create a resource share (Crear un recurso compartido).
7. Agregue un nombre para el recurso compartido.
8. En Select resource type (Seleccionar tipo de recurso), seleccione IPAM pools (Grupos de IPAM) y elija uno o varios grupos de IPAM.
9. Elija Siguiente.
10. Elija uno de los permisos para el recurso compartido:

    - AWSRAMDefaultPermissionsIpamPool: elija este permiso para permitir que las entidades principales vean los CIDR y las asignaciones en el grupo de IPAM compartido y asignen o liberen CIDR en el grupo.
    - AWSRAMPermissionIpamPoolByoipCidrImport: Elija este permiso para permitir que las entidades principales importen CIDR de BYOIP en el grupo de IPAM compartido. Solo necesitará este permiso si tiene CIDR de BYOIP existentes y desea importarlos a IPAM y compartirlos con las entidades principales. Para obtener información adicional acerca de los CIDR de BYOIP para IPAM, consulte Tutorial: Transferir un CIDR IPv4 de BYOIP a IPAM.
11. Elija las entidades principales a las que se les permite acceder a este recurso. Si las entidades principales van a importar CIDR de BYOIP existentes a este grupo de IPAM compartido, agregue la cuenta del propietario de CIDR de BYOIP como entidad principal.
12. Revise las opciones de recurso compartido y las entidades principales con las que se compartirá y elija Create (Crear).

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. Allí encontrará descripciones detalladas de las opciones que puede utilizar cuando ejecuta los comandos.

Utilice los siguientes comandos de la AWS CLI para compartir un grupo de IPAM mediante RAM:

1. Para obtener el ARN de IPAM: describe-ipam-pools
2. Para crear el recurso compartido: create-resource-share
3. Para ver el recurso compartido: get-resource-shares

Como resultado de crear el recurso compartido en RAM, otras entidades principales ahora pueden asignar CIDR a recursos mediante el grupo de IPAM. Para obtener información sobre el monitoreo de recursos creados por entidades principales, consulte Monitorear el uso de CIDR por recurso. Para obtener más información acerca de cómo crear una VPC y asignar un CIDR desde un grupo de IPAM compartido, consulte Creación de una VPC en la Guía del usuario de Amazon VPC.

Trabajo con las detecciones de recursos

La detección de recursos es un componente del IPAM que permite al IPAM administrar y supervisar los recursos que pertenecen a la cuenta propietaria de la detección de recursos. Esto permite al IPAM mantener un inventario actualizado del uso de direcciones IP en todas sus cargas de trabajo, lo que facilita la administración y la planificación de las direcciones IP.

Cuando crea un IPAM, se crea una detección de recursos de manera predeterminada. También puede crear una detección de recursos independientemente de un IPAM e integrarlo con un IPAM propiedad de otra cuenta u organización. Si el propietario de la detección de recursos es el administrador delegado de una organización, IPAM supervisará los recursos de todos los miembros de la organización.

> **Note**
>
> Crear, compartir y asociar detecciones de recursos forma parte del proceso de integración de IPAM con cuentas ajenas a sus organizaciones (consulte Integración de IPAM con cuentas ajenas a su organización). Si no va a crear un IPAM ni integrarlo con cuentas ajenas a su organización, no necesita crear, compartir ni asociar las detecciones de recursos.

En esta sección, se agrupan los procedimientos relacionados con las detecciones de recursos.

Contenido

Creación de una detección de recursos para integrarla con otro IPAM

En esta sección, se describe cómo crear una detección de recursos. Cuando crea un IPAM, se crea una detección de recursos de manera predeterminada. La cuota predeterminada para la detección de recursos por región es 1. Para obtener más información acerca de las cuotas de IPAM, consulte Cuotas de IPAM.

> **Note**
>
> Crear, compartir y asociar detecciones de recursos forma parte del proceso de integración de IPAM con cuentas ajenas a sus organizaciones (consulte Integración de IPAM con cuentas ajenas a su organización). Si no va a crear un IPAM ni integrarlo con cuentas ajenas a su organización, no necesita crear, compartir ni asociar las detecciones de recursos.

Si va a integrar un IPAM con cuentas ajenas a sus organizaciones, este es un paso obligatorio que debe completar la cuenta de administrador de la organización secundaria. Para obtener más información acerca de los roles en este proceso, consulte Información general del proceso.

AWS Management Console

Creación de una detección de recursos

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Detecciones de recursos.
3. Elija Crear detección de recursos.

4. Seleccione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir al Administrador de direcciones IP de Amazon VPC replicar los datos de las cuentas de origen en la cuenta delegada de IPAM). Si no selecciona esta opción, no puede crear una detección de recursos.
5. (Opcional) Agregue una etiqueta de Nombre a la detección de recursos. Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar etiquetas para buscar y filtrar los recursos o hacer un seguimiento de los costos de AWS.
6. (Opcional) Añada una descripción.
7. En Regiones operativas, seleccione las regiones de AWS en las que se detectarán los recursos. La región actual se establecerá automáticamente como una de las regiones operativas. Si está creando la detección de recursos para poder compartirla con un IPAM de la región operativa `us-east-1`, asegúrese de seleccionar `us-east-1` aquí. Si olvida una región operativa, puede regresar más adelante y editar la configuración de la detección de recursos.

   > **Note**
   >
   > En la mayoría de los casos, la detección de recursos debe tener las mismas regiones operativas que el IPAM; si no, solo obtendrá la detección de recursos en esa región.

8. (Opcional) Elija Etiquetas adicionales para el grupo.
9. Seleccione Crear.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

- Cree una detección de recursos: create-ipam-resource-discovery

Visualización de detalles de la detección de recursos

Ver los detalles de la detección de recursos en el IPAM de AWS puede proporcionar información valiosa como la siguiente:

- Identificar los recursos de AWS específicos que se han importado y sus asignaciones de direcciones IP asociadas.
- Supervisar el estado y el progreso del proceso de detección de recursos.
- Solucionar cualquier problema o discrepancia entre el IPAM y los recursos detectados.
- Analizar la utilización y las tendencias de las direcciones IP.

Esta información puede ayudarlo a optimizar la administración de direcciones IP y garantizar la alineación entre el IPAM y sus implementaciones de recursos reales.

AWS Management Console

Visualización de detalles de la detección de recursos

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Detecciones de recursos.
3. Elija una detección de recursos.
4. En Detalles de detección de recursos, vea los detalles relacionados con la detección de recursos, como Predeterminada, que indica si la detección de recursos es la predeterminada. La detección de recursos predeterminada es la detección de recursos que se crea automáticamente al crear un IPAM.
5. En las pestañas, puede ver los detalles de una detección de recursos:

    - Recursos detectados: recursos monitoreados en el marco de una detección de recursos. IPAM monitorea los CIDR de los siguientes tipos de recursos: VPC, grupos IPv4 públicos, subredes de VPC y direcciones IP elásticas.
        - Nombre (ID de recurso): ID de detección de recurso.
        - IPs asignadas: porcentaje del espacio de direcciones IP que está en uso. Para convertir el decimal en un porcentaje, multiplique el decimal por 100. Tenga en cuenta lo siguiente:
            - Para los recursos que son VPC, este es el porcentaje del espacio de direcciones IP en la VPC que ocupan los CIDR de subred.
            - Para los recursos que son subredes, si la subred tiene un CIDR IPv4 aprovisionado, este es el porcentaje de espacio de direcciones IPv4 en la subred que está en uso. Si la subred tiene un CIDR IPv6 aprovisionado, no se representa el porcentaje de

espacio de direcciones IPv6 en uso. El porcentaje de espacio de direcciones IPv6 en uso no se puede calcular actualmente.

- Para los recursos que son grupos IPv4 públicos, este es el porcentaje del espacio de direcciones IP del grupo que se ha asignado a las direcciones IP elásticas (EIP).

- CIDR: CIDR del recurso.
- Región: región del recurso.
- ID del propietario: ID del propietario del recurso.
- Tiempo de muestra: el último tiempo de detección exitosa de un recurso.

- Cuentas detectadas: cuentas de AWS que se están monitoreando en el marco de una detección de recursos. Si ha integrado IPAM con AWS Organizations, todas las cuentas de la organización son cuentas detectadas.
  - ID de cuenta: el ID de la cuenta.
  - Región: la región de AWS desde la que se devuelve la información de la cuenta.
  - Hora del último intento de detección: hora del último intento de detección de recursos.
  - Hora de la última detección exitosa: hora de la última detección de recursos exitosa.
  - Estado: motivo del error de detección de recursos.
- Regiones operativas: las regiones operativas para la detección de recursos.
- Uso compartido de recursos: si se ha compartido la detección de recursos, aparece el ARN del recurso compartido.
  - ARN del recurso compartido: ARN del recurso compartido.
  - Estado: el estado actual del recurso compartido. Los valores posibles son los siguientes:
    - Activo: el recurso compartido está activo y disponible para su uso.
    - Eliminado: el recurso compartido se eliminó y ya no está disponible para su uso.
    - Pendiente: hay una invitación para aceptar el recurso compartido a la espera de una respuesta.
  - Creado el: cuándo se creó el recurso compartido.
- Etiquetas: una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar etiquetas para buscar y filtrar los recursos o hacer un seguimiento de los costos de AWS.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

- Ver detalles de detección de recursos: describe-ipam-resource-discoveries

Uso compartido de una detección de recursos con otra cuenta de AWS

Siga los pasos de esta sección para compartir una detección de recursos mediante AWS Resource Access Manager. Para obtener más información sobre AWS RAM, consulte Cómo compartir los recursos de AWS en la Guía del usuario de AWS RAM.

> **Note**
>
> Crear, compartir y asociar detecciones de recursos forma parte del proceso de integración de IPAM con cuentas ajenas a sus organizaciones (consulte Integración de IPAM con cuentas ajenas a su organización). Si no va a crear un IPAM ni integrarlo con cuentas ajenas a su organización, no necesita crear, compartir ni asociar las detecciones de recursos.

Al crear un IPAM que monitorea cuentas ajenas a su organización, la cuenta de administrador de la organización secundaria comparte la detección de recursos con la cuenta de IPAM de la organización principal mediante AWS RAM. Primero debe compartir la detección de recursos con la cuenta de IPAM de la organización principal antes de que la cuenta de IPAM de la organización principal asocie la detección de recursos a su IPAM. Para obtener más información acerca de los roles en este proceso, consulte Información general del proceso.

> **Note**
>
> - Al crear un recurso compartido con AWS RAM para compartir la detección de recursos, debe crear el recurso compartido en la región de origen del IPAM de la organización principal.
> - La cuenta que crea y elimina un recurso compartido para una detección de recursos debe tener los siguientes permisos en la política de IAM:
>   - ec2:PutResourcePolicy

- ec2:DeleteResourcePolicy
- Si comparte la detección de un recurso con otra cuenta, esa cuenta puede ver las exclusiones de OU del recurso, lo que incluye, entre otras cosas, el identificador de la organización, el identificador raíz y los identificadores de las unidades organizativas de la organización del propietario de la detección de recursos.

Si va a integrar un IPAM con cuentas ajenas a sus organizaciones, este es un paso obligatorio que debe completar la cuenta de administrador de la organización secundaria.

AWS Management Console

Uso compartido de una detección de recursos

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Detecciones de recursos.
3. Seleccione la pestaña Uso compartido de recursos.
4. Elija Crear recurso compartido. Se abre la consola de AWS RAM, que es donde creará el recurso compartido.
5. En la consola de AWS RAM, elija Configuración.
6. Seleccione Habilitar el uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.
7. Elija Create a resource share (Crear un recurso compartido).
8. Agregue un nombre para el recurso compartido.
9. En Seleccionar tipo de recurso, seleccione Detección de recursos de IPAM y elija la detección de recursos.
10. Elija Siguiente.
11. En Asociar permisos, puede ver el permiso predeterminado que se habilitará para las entidades principales a las que se les concede acceso a este recurso compartido:
    - AWSRAMPermissionIpamResourceDiscovery
    - Acciones permitidas por este permiso:
      - ec2:AssociateIpamResourceDiscovery
      - ec2:GetIpamDiscoveredAccounts
      - ec2:GetIpamDiscoveredPublicAddresses

- ec2:GetIpamDiscoveredResourceCidrs

12. Especifique las entidades principales a las que se les permite acceder a este recurso compartido. En Entidades principales, elija la cuenta de IPAM de la organización principal y, a continuación, elija Agregar.
13. Elija Siguiente.
14. Revise las opciones de recurso compartido y las entidades principales con las que se compartirá. Luego, elija Crear recurso compartido.
15. Una vez compartida la detección de recursos, la cuenta de IPAM de la organización principal debe aceptarla y, a continuación, asociarla a un IPAM. Para obtener más información, consulte Asociación de una detección de recursos a un IPAM.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

1. Para crear el recurso compartido: create-resource-share
2. Para ver el recurso compartido: get-resource-shares

Asociación de una detección de recursos a un IPAM

En esta sección, se describe cómo asociar una detección de recursos a un IPAM. Al asociar la detección de recursos a un IPAM, el IPAM monitorea todos los CIDR de recursos y las cuentas detectadas en la detección de recursos. Al crear un IPAM, se crea una detección de recursos predeterminada para el IPAM y se asocia automáticamente a este.

La cuota predeterminada para las asociaciones de detección de recursos es 5. Para obtener más información (incluido cómo ajustar esta cuota), consulte Cuotas de IPAM.

> **Note**
>
> Crear, compartir y asociar detecciones de recursos forma parte del proceso de integración de IPAM con cuentas ajenas a sus organizaciones (consulte Integración de IPAM con cuentas ajenas a su organización). Si no va a crear un IPAM ni integrarlo con cuentas ajenas a su organización, no necesita crear, compartir ni asociar las detecciones de recursos.

Si va a integrar un IPAM con cuentas ajenas a sus organizaciones, este es un paso obligatorio que debe completar la cuenta de IPAM de la organización principal. Para obtener más información acerca de los roles en este proceso, consulte Información general del proceso.

AWS Management Console

Asociación de la detección de recursos

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija IPAMs (IPAM).
3. Seleccione Detecciones asociadas y, a continuación, elija Asociar detecciones de recursos.
4. En Detecciones de recursos de IPAM, elija una detección de recursos que la cuenta de administrador de la organización secundaria haya compartido con usted.
5. Elija Asociar.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

- Asociar una detección de recursos: associate-ipam-resource-discovery

Desasociación de una detección de recursos

En esta sección, se describe cómo desasociar la detección de recursos de un IPAM. Al desasociar la detección de recursos de un IPAM, el IPAM ya no monitorea todos los CIDR de recursos y las cuentas detectadas en la detección de recursos.

> **Note**
>
> No puede desasociar una asociación de detección de recursos predeterminada. Una asociación de detección de recursos predeterminada es aquella que se crea automáticamente al crear un IPAM. Sin embargo, la asociación de detección de recursos predeterminada se elimina si se elimina el IPAM.

La cuenta de IPAM de la organización principal debe completar este paso. Para obtener más información acerca de los roles en este proceso, consulte Información general del proceso.

AWS Management Console

Desasociación de una detección de recursos

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija IPAMs (IPAM).
3. Seleccione Detecciones asociadas y, a continuación, elija Desasociar detecciones de recursos.
4. En Detecciones de recursos de IPAM, elija una detección de recursos que la cuenta de administrador de la organización secundaria haya compartido con usted.
5. Elija Desasociar.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

- Para desasociar una detección de recursos: disassociate-ipam-resource-discovery

Eliminación de una detección de recursos

En esta sección, se describe cómo eliminar una detección de recursos.

> **Note**
>
> No puede eliminar una detección de recursos predeterminada. Una detección de recursos predeterminada es aquella que se crea automáticamente al crear un IPAM. Sin embargo, la detección de recursos predeterminada se elimina si elimina el IPAM.

La cuenta de administrador de la organización secundaria debe completar este paso. Para obtener más información acerca de los roles en este proceso, consulte Información general del proceso.

AWS Management Console

Para eliminar una detección de recursos

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Detecciones de recursos.
3. Seleccione una detección de recursos y elija Acciones > Eliminar detección de recursos.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

- Para eliminar una detección de recursos: delete-ipam-resource-discovery

Seguimiento del uso de direcciones IP en IPAM

El Administrador de direcciones IP de Amazon VPC ofrece características de seguimiento del uso de direcciones IP que pueden beneficiar a cualquiera que administre entornos de red complejos. El IPAM proporciona visibilidad de las tendencias de asignación, utilización y consumo de direcciones IP en AWS. Esto lo ayuda a identificar las direcciones IP no utilizadas o utilizadas de manera ineficiente, a optimizar el espacio de direcciones y a evitar el posible agotamiento de las direcciones IP.

El IPAM hace un seguimiento del uso de las direcciones IP en el nivel de CIDR, alcance e IPAM, y proporciona informes y análisis detallados. Esto resulta útil para las implementaciones a gran escala, configuraciones de varias cuentas y requisitos de red en constante evolución.

Al aprovechar el seguimiento del uso de IPAM, puede tomar decisiones informadas, mejorar la administración de las direcciones IP y garantizar una utilización eficiente de los recursos de IP.

> **Note**
>
> Las tareas que se describen en esta sección son opcionales. Si desea completar las tareas de esta sección y ha delegado una cuenta de IPAM, dicha cuenta de IPAM debe completar las tareas.

Contenido

Monitorear el uso de CIDR con el panel de IPAM

El panel IPAM del Administrador de direcciones IP de Amazon VPC le permite supervisar el uso de CIDR en varios escenarios clave:

- Identifique el espacio de direcciones IP no utilizado o infrautilizado: el panel proporciona visibilidad del uso de CIDR, lo que le permite identificar los CIDR con capacidad disponible que se puede recuperar o reasignar.
- Optimice la administración de direcciones IP: al hacer un seguimiento minucioso del uso de CIDR, podrá tomar decisiones fundamentadas sobre la expansión, la contratación o la reasignación de los bloques de direcciones IP para cumplir con los cambiantes requisitos empresariales y de infraestructura.
- Evite el agotamiento de las direcciones IP: supervisar el uso de CIDR ayuda a anticipar cuándo necesitará adquirir espacio de direcciones IP adicional, lo que le permite planificar de forma proactiva y evitar interrupciones en el servicio debido al agotamiento de las direcciones IP.
- Garantice el cumplimiento y la gobernanza: el panel IPAM puede ayudar a demostrar los patrones de uso de las direcciones IP para cumplir con los requisitos reglamentarios o las políticas internas en materia de administración de direcciones IP.
- Solucione problemas de red: los datos detallados de uso de CIDR pueden ayudar a identificar las causas fundamentales de los problemas de conectividad de la red o de los conflictos de recursos.

Al supervisar de cerca el uso de CIDR a través del panel IPAM, puede mejorar la eficiencia, la resiliencia y el cumplimiento de la administración de direcciones IP dentro de AWS.

AWS Management Console

Para monitorear el uso de CIDR con el panel de IPAM

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Panel.
3. De forma predeterminada, al ver el panel, se selecciona el alcance privado predeterminado. Si no desea utilizar el alcance privado predeterminado, en el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. El panel presenta una descripción general de los grupos de IPAM y los CIDR dentro de un alcance. De este modo, podrá agregar, eliminar, cambiar el tamaño y mover widgets para personalizar el panel.

    - Alcance: los detalles de este alcance. Un alcance es el contenedor de más alto nivel dentro de IPAM. Un IPAM contiene dos alcances predeterminados, uno privado y otro público.

Cada alcance representa el espacio IP de una única red. Puede tener varios alcances privados, pero solo puede tener un alcance público.

- ID del alcance: los detalles de este alcance.
- Tipo de alcance: el tipo de alcance.
- ID de IPAM: el ID de IPAM donde se encuentra el alcance.
- Grupos de IPAM en este alcance: el ID de IPAM donde se encuentra el alcance.
- Ver los recursos de red en este ámbito: lo lleva a la sección Recursos de la consola de IPAM.
- Buscar en el historial de una dirección IP en este ámbito: lo lleva a la sección Buscar historial de IP de la consola de IPAM.

- Tipos de CIDR de recursos: los tipos de CIDR de recursos incluidos en el alcance.
  - Subred: el número de CIDR para subredes.
  - VPC: el número de CIDR para VPC.
  - EIP: el número de CIDR para direcciones IP elásticas.
  - Grupos IPv4 públicos: el número de CIDR para grupos IPv4 públicos.
- Estado de administración: el estado de administración de los CIDR.
  - CIDR no administrados: el número de CIDR de recursos para recursos no administrados en este alcance.
  - CIDR ignorados: el número de CIDR de recursos que ha elegido estar exentos del monitoreo con IPAM en el alcance de aplicación. IPAM no evalúa los recursos ignorados para la superposición o la conformidad dentro de un alcance de aplicación. Cuando se elija ignorar un recurso, cualquier espacio asignado a él desde un grupo de IPAM se devuelve al grupo y el recurso no se volverá a importar mediante la importación automática (si la regla de asignación de importación automática se ha establecido en el grupo).
  - CIDR administrados: el número de CIDR de recursos para recursos administrables (VPC o grupos IPv4 públicos) que se asignan desde un grupo de IPAM del alcance.
- CIDR de recursos superpuestos: el número de CIDR superpuestos y no superpuestos. Los CIDR superpuestos pueden provocar un enrutamiento incorrecto en las VPC.
  - CIDR superpuestos: el número de CIDR que se superponen actualmente dentro de los grupos de IPAM de este alcance. Los CIDR superpuestos pueden provocar un enrutamiento incorrecto en las VPC.

    - CIDR que no se superponen: el número de CIDR que no se superponen actualmente dentro de los grupos de IPAM de este alcance.
- CIDR de recursos conformes: número de CIDR de recursos conformes.
    - CIDR conforme: el número de CIDR de recursos que cumplen las reglas de asignación de los grupos de IPAM del alcance.
    - CIDR no conforme: el número de CIDR de recursos que no cumplen las reglas de asignación de los grupos de IPAM del alcance.
- Estado de superposición: número de CIDR que se superponen a lo largo del tiempo.
    - OverlappingResourceCidrs: el número de CIDR que se superponen actualmente dentro de los grupos de IPAM de este alcance. Los CIDR superpuestos pueden provocar un enrutamiento incorrecto en las VPC.
- Estado de cumplimiento: el número de CIDR que cumplen las reglas de asignación de los grupos de IPAM en el alcance frente a los que no lo cumplen a lo largo del tiempo.
    - CompliantResourceCidrs: el número de CIDR de recursos que cumplen las reglas de asignación.
    - NonCompliantResourceCidrs: el número de CIDR de recursos que no cumplen las reglas de asignación.
- Utilización de VPC: VPC (IPv4 e IPv6) con la utilización de IP más alta o más baja. Puede utilizar esta información para configurar las alarmas de Amazon CloudWatch para recibir alertas si se infringe un umbral de utilización de IP. Para obtener más información, consulte Métricas de utilización de recursos del IPAM.
- Utilización de subredes: subredes (solo IPv4) con la utilización de IP más alta o más baja. Puede utilizar esta información para decidir si desea conservar o eliminar los recursos que están infrautilizados. Para obtener más información, consulte Métricas de utilización de recursos del IPAM.
- VPC con las IP más altas asignadas: las VPC que tienen el mayor porcentaje de espacio de direcciones IP asignado a las subredes. Esto es útil para mostrarle si necesita aprovisionar espacio de direcciones IP adicional a las VPC.
- VPC con más espacio de IP asignado: las VPC que tienen el mayor porcentaje de espacio de direcciones IP asignado a las subredes. Esto es útil para mostrarle si necesita aprovisionar espacio de direcciones IP adicional a las VPC.
- Asignación de grupos: el porcentaje de espacio IP que se ha asignado a recursos y asignaciones manuales del alcance a lo largo del tiempo.

- Asignación de grupos: el porcentaje del espacio IP de un grupo que se ha asignado a otros grupos del alcance a lo largo del tiempo.

Command line

La información que se muestra en el panel proviene de métricas almacenadas en Amazon CloudWatch. Para obtener más información acerca de las métricas almacenadas en Amazon CloudWatch, consulte Supervisar IPAM con Amazon CloudWatch. Utilice las opciones de Amazon CloudWatch en la Referencia de AWS CLI para ver las métricas de las asignaciones en los grupos y alcances de IPAM.

Si descubre que el CIDR que se aprovisiona para un grupo está casi totalmente asignado, es posible que deba aprovisionar CIDR adicionales. Para obtener más información, consulte Aprovisionamiento de CIDR en un grupo.

Monitorear el uso de CIDR por recurso

La vista Recursos del Administrador de direcciones IP de Amazon VPC proporciona una visión general centralizada del uso de las direcciones IP en todos sus recursos de AWS. Esto le permite identificar rápidamente qué recursos consumen direcciones IP, hacer un seguimiento de las tendencias de asignación de direcciones y optimizar la administración de direcciones IP para adaptarla a las cambiantes necesidades empresariales y de infraestructura.

En IPAM, un recurso es una entidad de servicio de AWS a la que se le asigna una dirección IP o un bloque de CIDR. El IPAM administra algunos recursos, pero solo supervisa otros recursos, por lo que es importante entender la diferencia entre ambos conceptos:

- Recurso administrado: un recurso administrado tiene un CIDR asignado desde un grupo de IPAM. IPAM monitorea el CIDR para detectar posibles solapamientos de direcciones IP con otros CIDR del grupo y monitorea la conformidad del CIDR con las reglas de asignación de un grupo. IPAM admite los siguientes tipos de recursos:
  - Direcciones IP elásticas
  - Grupos IPv4 públicos

> **Note**
>
> Los grupos IPv4 públicos y los grupos de IPAM se administran mediante distintos recursos en AWS. Los grupos IPv4 públicos son recursos de una sola cuenta que le permiten convertir sus CIDR de propiedad pública en direcciones IP elásticas. Los grupos de IPAM se pueden utilizar para asignar el espacio público a grupos IPv4 públicos.

  - VPC
- Recurso monitoreado: si IPAM monitorea un recurso, significa que el recurso ha sido detectado por IPAM y puede ver detalles sobre el CIDR del recurso cuando utiliza `get-ipam-resource-cidrs` con AWS CLI, o al ver Resources (Recursos) en el panel de navegación. IPAM admite el monitoreo de los siguientes recursos:
  - Direcciones IP elásticas
  - Grupos IPv4 públicos
  - VPC
  - Subredes de la VPC

AWS Management Console

Para monitorear el uso de CIDR por recurso

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Resources (Recursos).
3. En el menú desplegable de la IP: en la parte superior del panel de contenido, elija la dirección IP que desea utilizar: IPv4 o IPv6.
4. En el menú desplegable de alcance en la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
5. Utilice el mapa CIDR de recursos para ver el espacio de direcciones IP disponible, asignado y superpuesto en un alcance:
   - Disponible: hay un rango de direcciones IP disponible para su asignación.
   - Cumple con las normas y no se superpone: se asigna un rango de direcciones IP a un recurso administrado por el IPAM.

- Ocupado: se asigna un rango de direcciones IP a un recurso.
- Superposición: se ha asignado un rango de direcciones IP a varios recursos y hay una superposición.
- No compatible: un rango de direcciones IP no es compatible. Hay un recurso que utiliza el rango de direcciones IP que no cumple con las reglas de asignación establecidas para el grupo.

En el mapa de CIDR, elija un bloque de direcciones IP en la parte inferior del mapa para ver los recursos en bloques CIDR más pequeños. Elija un bloque de direcciones IP en la parte superior del mapa para ver los recursos en bloques CIDR de mayor tamaño.

6. En la tabla, puede ver los siguientes detalles sobre los recursos del alcance:

- Nombre (ID de recurso): el nombre y el ID de recurso del recurso.
- CIDR: el CIDR asociado al recurso.
- Estado de administración: el estado del recurso.
  - Managed (Administrado): el recurso tiene un CIDR asignado desde un grupo de IPAM e IPAM lo está monitoreando para detectar la posible superposición y conformidad de CIDR con las reglas de asignación del grupo.
  - Unmanaged (No administrado): el recurso no tiene un CIDR asignado desde un grupo de IPAM e IPAM no lo está monitoreando para detectar la posible conformidad de CIDR con las reglas de asignación del grupo. Se monitorea el CIDR para detectar superposiciones.
  - Ignored (Ignorado): el recurso se ha elegido para estar exento del monitoreo. Los recursos ignorados no se evalúan para la superposición ni la conformidad con las reglas de asignación. Cuando se elija ignorar un recurso, cualquier espacio asignado a él desde un grupo de IPAM se devuelve al grupo y el recurso no se volverá a importar mediante la importación automática (si la regla de asignación de importación automática se ha establecido en el grupo).
  - -: este recurso no es uno de los tipos de recursos que IPAM puede administrar.
- Compliance status (Estado de conformidad): el estado de conformidad del CIDR.
  - Compliant (Conforme): un recurso administrado cumple las reglas de asignación del grupo de IPAM.
  - Noncompliant (No conforme): el CIDR del recurso no cumple una o más de las reglas de asignación del grupo de IPAM.

Example

Si una VPC tiene un CIDR que no cumple con los parámetros de longitud de máscara de red del grupo de IPAM o si el recurso no se encuentra en la misma región de AWS que el grupo de IPAM, se marcará como no conforme.

- Unmanaged (No administrado): el recurso no tiene un CIDR asignado desde un grupo de IPAM e IPAM no lo está monitoreando para detectar la posible conformidad de CIDR con las reglas de asignación del grupo. Se monitorea el CIDR para detectar superposiciones.
- Ignored (Ignorado): el recurso se ha elegido para estar exento del monitoreo. Los recursos ignorados no se evalúan para la superposición ni la conformidad con las reglas de asignación. Cuando se elija ignorar un recurso, cualquier espacio asignado a él desde un grupo de IPAM se devuelve al grupo y el recurso no se volverá a importar mediante la importación automática (si la regla de asignación de importación automática se ha establecido en el grupo).
- -: este recurso no es uno de los tipos de recursos que IPAM puede administrar.

- Overlap status (Estado de superposición): el estado de superposición de CIDR.
  - Nonoverlapping (Sin superposición): el CIDR del recurso no se superpone con otro CIDR del mismo alcance.
  - Overlapping (Superposición): el CIDR del recurso se superpone con otro CIDR del mismo alcance. Tenga en cuenta que si se superpone un CIDR del recurso, podría superponerse con una asignación manual.
  - Ignored (Ignorado): el recurso se ha elegido para estar exento del monitoreo. IPAM no evalúa los recursos ignorados para la superposición ni la conformidad con las reglas de asignación. Cuando se elija ignorar un recurso, cualquier espacio asignado a él desde un grupo de IPAM se devuelve al grupo y el recurso no se volverá a importar mediante la importación automática (si la regla de asignación de importación automática se ha establecido en el grupo).
  - -: este recurso no es uno de los tipos de recursos que IPAM puede administrar.
- IPs asignadas: para los recursos que son VPC, es el porcentaje de espacio de direcciones IP en la VPC que ocupan los CIDR de subred. Para los recursos que son subredes, si la subred tiene un CIDR IPv4 aprovisionado, este es el porcentaje de espacio de direcciones IPv4 en la subred que está en uso. Si la subred tiene un CIDR IPv6 aprovisionado, no se representa el porcentaje de espacio de direcciones IPv6 en uso. El porcentaje de espacio

de direcciones IPv6 en uso no se puede calcular actualmente. Para los recursos que son grupos IPv4 públicos, este es el porcentaje del espacio de direcciones IP del grupo que se ha asignado a las direcciones IP elásticas (EIP).

- Region (Región): la región de AWS del recurso.
- Owner ID (ID del propietario): el ID de cuenta de AWS del usuario que creó este recurso.
- Tipo de recurso: si el recurso es una VPC, una subred, una dirección IP elástica o un grupo de IPv4 público.
- Pool ID (ID del grupo): ID del grupo de IPAM en el que se encuentra el recurso.

7. Utilice Filtrar recursos para filtrar la tabla de recursos por propiedad de columna, como el ID de la VPC o el estado de conformidad.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Utilice los siguiente comandos de la AWS CLI para monitorear el uso de CIDR por recurso:

1. Para obtener el ID de alcance: describe-ipam-scopes
2. Para solicitar información de recursos: get-ipam-resource-cidrs

Supervisar IPAM con Amazon CloudWatch

IPAM almacena de forma automática las métricas relacionadas con el uso de direcciones IP (como el espacio de direcciones IP disponible en los grupos de IPAM y la cantidad de CIDR de recursos que cumplen con las reglas de asignación) y la utilización de los recursos en el espacio de nombres de Amazon CloudWatch `AWS/IPAM` en su región de origen de su IPAM.

La integración del IPAM con CloudWatch mejora su capacidad de supervisar, analizar y optimizar la administración de direcciones IP en AWS.

Los casos de uso incluyen los siguientes:

- Seguimiento de las tendencias de uso de las direcciones IP: CloudWatch puede supervisar el uso del grupo de CIDR, la asignación del alcance y otras métricas del IPAM, lo que lo ayuda a identificar de forma proactiva los posibles riesgos de agotamiento de las direcciones IP.

- Configuración de alertas basadas en el uso: puede configurar las alarmas de CloudWatch para que le notifiquen cuando el uso de CIDR alcance los umbrales predeterminados, lo que permite una intervención y optimización oportunas.
- Supervisión de los eventos del IPAM: CloudWatch puede capturar y analizar los eventos relacionados con el IPAM, como las asignaciones y las modificaciones del alcance de CIDR, lo que proporciona visibilidad de las actividades de administración de direcciones IP.
- Generación de paneles personalizados: al combinar los datos del IPAM con otras métricas de AWS, puede crear paneles completos para visualizar y analizar su panorama de direcciones IP junto con los indicadores de infraestructura y rendimiento relacionados.

Contenido

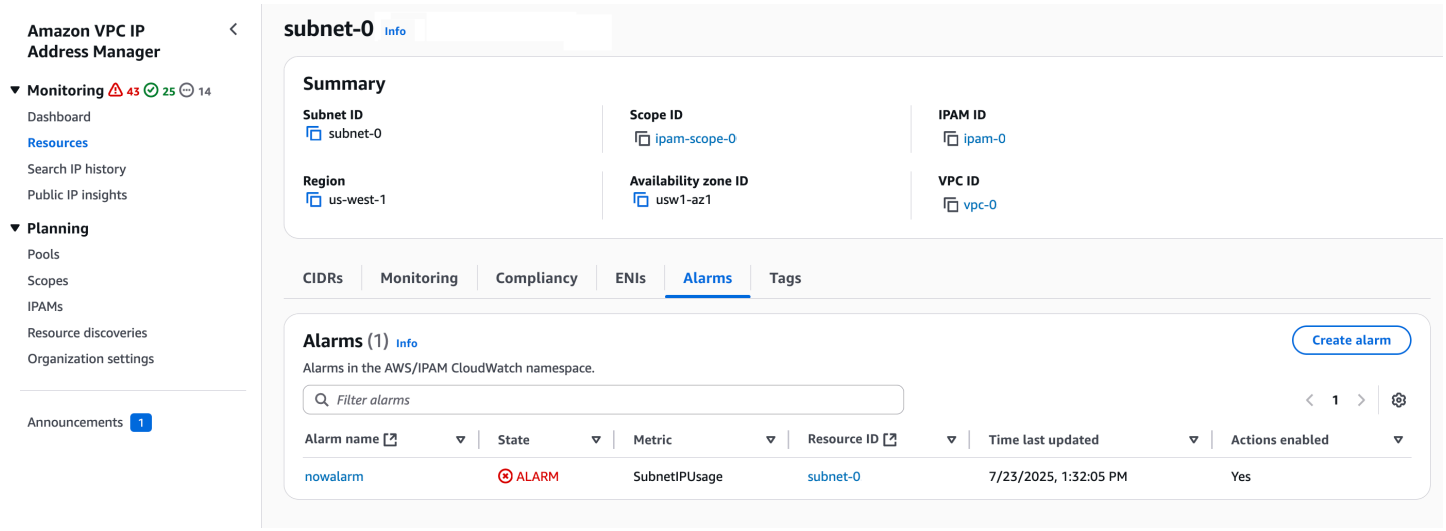
Administrar alarmas desde la consola de IPAM

Cree y administre alarmas de Amazon CloudWatch directamente de la consola de IPAM. Las alarmas para las Métricas del IPAM o Métricas de utilización de recursos del IPAM que estén en estado de INSUFFICIENT_DATA o ALARM aparecerán como barras de advertencia en la parte superior de la consola y como indicadores visuales en el panel de navegación de la izquierda al lado de Monitorización.

Para administrar las alarmas de recursos específicos, seleccione Recursos y luego elija una VPC, una subred o un grupo. Al abrirse la página de detalles de dicho recurso, debe seleccionar la pestaña Alarmas.

La pestaña Alarmas muestra todas las alarmas de CloudWatch que están asociadas al recurso seleccionado. Allí se pueden observar los detalles de las alarmas, monitorear los estados actuales y acceder a las opciones de configuración. Además, la pestaña indica las alarmas del espacio de nombres `AWS/IPAM` que son importantes para el recurso que está consultando.

La siguiente captura de pantalla muestra la interfaz de administración de alarmas en la consola de IPAM:



La pestaña Alarmas ofrece un resumen detallado de las alarmas de CloudWatch en el espacio de nombres `AWS/IPAM` de Amazon CloudWatch en la región de origen de IPAM:

- Nombre de la alarma: nombre de la alarma de CloudWatch que define el usuario.
- Estado: estado actual de la alarma de CloudWatch:
  - ALARM: la métrica está fuera del umbral definido.
  - OK: la métrica está dentro del umbral definido.
  - INSUFFICIENT_DATA: no hay datos suficientes para determinar el estado de la alarma.
- Métrica: la métrica específica de CloudWatch que la alarma monitorea.
- ID de recurso: el identificador único del recurso de AWS que la alarma está monitoreando.
- Última actualización: fecha y hora en que se modificó o evaluó por última vez el estado de la alarma.
- Acciones habilitadas: indica si las acciones de CloudWatch están habilitadas para la alarma:
  - Sí: la alarma puede activar las acciones configuradas cuando se cumplan las condiciones.
  - No: la alarma está monitorizando pero no ejecuta acciones.

Por otra parte, si está consultando los gráficos de utilización en la pestaña Monitoreo de una VPC, una subred o un grupo, tiene la opción de crear una alarma para la utilización del recurso. Luego, se le redirigirá a la consola de CloudWatch con los datos ya rellenados del recurso y las métricas. Desde allí, puede configurar un umbral de alarma para recibir una notificación cuando la utilización haya llegado a un porcentaje específico, por ejemplo.

Métricas del IPAM

El IPAM publica datos sobre sus IPAM, grupos y alcance en Amazon CloudWatch. Utilice estas métricas para crear alarmas para grupos de IPAM para notificarle si los grupos de direcciones están a punto de agotarse o si los recursos no cumplen las reglas de asignación establecidas en un grupo. La creación de alarmas y la configuración de notificaciones con Amazon CloudWatch se encuentra fuera del ámbito de esta sección. Para obtener más información, consulte Uso de las alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

A continuación, se enumeran las métricas y las dimensiones que IPAM envía a Amazon CloudWatch.

Métricas del IPAM

El espacio de nombres de `AWS/IPAM` incluye las siguientes métricas del IPAM.

Nombre de métrica	Descripción
TotalActiveIpCount	El recuento total de IP activas es la cantidad de direcciones IP activas en su IPAM que se le cobraría si pasara del nivel gratuito al nivel avanzado. Una dirección IP activa se define como una dirección IP o un prefijo asociados con una interfaz de red elástica (ENI) que está asignada a un recurso, como una instancia de EC2. • Esta métrica solo está disponible para los clientes del nivel gratuito. • Si su IPAM está integrado con AWS Organizations, el recuento de IP activas cubre todas las cuentas de la organización. • No se puede ver un desglose del recuento de IP activas por tipo de IP (pública/privada) o por clase (IPv4/IPv6). • El IPAM solo cuenta las IP de las ENI que son propiedad de las cuentas supervisadas. Es posible que el recuento no sea exacto en el caso de las subredes compartidas. Las direcciones IP se excluyen si el propietario de la subred o de la ENI no está cubierto por el IPAM.

Métricas de grupos de IPAM

El espacio de nombres de `AWS/IPAM` incluye las siguientes métricas de grupo para el IPAM.

Nombre de métrica	Descripción
CompliantResourceCidrs	La cantidad de CIDR de recursos administrados que cumplen las reglas de asignación de los grupos de IPAM. Para obtener más información acerca de las reglas de asignación, consulte Creación de un grupo IPv4 de nivel superior.
NoncompliantResourceCidrs	La cantidad de CIDR de recursos administrados que no cumplen las reglas de asignación de los grupos de IPAM. Para obtener más información acerca de las reglas de asignación, consulte Creación de un grupo IPv4 de nivel superior.
PercentAllocated	El porcentaje del espacio IP de un grupo que se ha asignado a otros grupos.
PercentAssigned	El porcentaje del espacio IP de un grupo que se ha asignado a recursos, incluidas las asignaciones manuales.
PercentAvailable	El porcentaje del espacio IP de un grupo que no se ha asignado a otros grupos ni a otros recursos.

Métricas de alcance de IPAM

El espacio de nombres de `AWS/IPAM` incluye las siguientes métricas de alcance para el IPAM.

Nombre de métrica	Descripción
CompliantResourceCidrs	La cantidad de CIDR de recursos que cumplen las reglas de asignación de los grupos de IPAM en el alcance.
ManagedResourceCidrs	La cantidad de CIDR de recursos para recursos administrables (VPC o grupos IPv4 públicos) que se asignan desde un grupo de IPAM en el alcance.

Nombre de métrica	Descripción
NoncompliantResourceCidrs	La cantidad de CIDR de recursos que no cumplen las reglas de asignación de los grupos de IPAM en el alcance.
OverlappingResourceCidrs	La cantidad de CIDR de recursos que se superponen en el alcance.
UnmanagedResourceCidrs	La cantidad de CIDR de recursos en el alcance que están asociados actualmente a recursos administrados, pero que IPAM no administra.

Métricas de IP pública de IPAM

El espacio de nombres de `AWS/IPAM` incluye las siguientes métricas IP públicas para IPAM.

Nombre de métrica	Descripción
AmazonOwnedContigIPs	Número de direcciones IP dentro de los CIDR que se aprovisionan a los grupos de IPv4 públicos contiguos proporcionados por Amazon que son propiedad del IPAM.
AllocatedAmazonOwnedContigIPs	Número de direcciones IP que se han asignado desde un bloque de CIDR de grupos de IPv4 públicos contiguos proporcionados por Amazon.
UnallocatedAmazonOwnedContigIPs	Número de direcciones IP dentro del bloque de CIDR de grupos de IPv4 públicos contiguos proporcionados por Amazon que son propiedad del IPAM.
AssociatedAmazonOwnedContigIPs	Número de direcciones IP elásticas que se han asignado desde un bloque de CIDR de grupos de IPv4 públicos contiguos proporcionados por Amazon y que están asociadas a una interfaz de red elástica.
UnassociatedAmazonOwnedContigIPs	Número de direcciones IP elásticas que se han asignado desde un bloque de CIDR de grupos de IPv4 públicos contiguos

Nombre de métrica	Descripción
	proporcionados por Amazon y que no están asociadas a una interfaz de red elástica.

Métricas del solucionador de lista de prefijos de IPAM

Recomendamos configurar alarmas de CloudWatch basadas en métricas de fallos, ya que podría ser necesario reevaluar y ajustar las reglas del solucionador de lista de prefijos de IPAM para mantenerse dentro de los límites de tamaño de versión y de lista de prefijos.

Nombre de métrica	Descripción
IpamPrefixListResolverSyncFailure	El solucionador de lista de prefijos no se pudo sincronizar con el destino. Esto puede ocurrir si se supera una cuota, como “entradas CIDR por versión del solucionador de lista de prefijos”, si no se encuentra la lista de prefijos de destino o si la sincronización está desactivada en la lista de prefijos administrada de destino.
IpamPrefixListResolverSyncSuccess	El solucionador de lista de prefijos se sincronizó correctamente con el destino.
IpamPrefixListResolverVersionCreationSuccess	La versión se creó correctamente.
IpamPrefixListResolverVersionCreationFailure	No se pudo crear la versión. Esto puede ocurrir si ha alcanzado la cuota de “entradas CIDR por versión del solucionador de lista de prefijos”.

Dimensiones de la métrica

Para filtrar las métricas del IPAM, utilice las siguientes dimensiones.

Dimensión	Descripción
AddressFamily	La familia de direcciones IP de los CIDR de recursos (IPv4 o IPv6).
Locale	La región de AWS en la que el grupo de IPAM está disponible para asignaciones.
PoolID	El ID de un grupo.
ScopeID	El ID de un alcance.

Para obtener información sobre el monitoreo de las VPC con Amazon CloudWatch, consulte Métricas de CloudWatch para las VPC en la Guía del usuario de Amazon Virtual Private Cloud.

Métricas de utilización de recursos del IPAM

IPAM publica las métricas de utilización de IP de los recursos que IPAM supervisa en Amazon CloudWatch. Estos recursos son:

- VPC (IPv4 e IPv6)
- Subredes (IPv4)
- Grupos IPv4 públicos

IPAM calcula y publica las métricas de utilización de IP por separado por familia de direcciones IP (IPv4 o IPv6). La utilización de IP de un recurso se calcula en todos sus CIDR de la misma familia de direcciones.

Para cada combinación de tipos de recursos y familias de direcciones, IPAM utiliza tres reglas para determinar qué métricas publicar:

- Hasta 50 recursos con la mayor utilización de IP. Puede utilizar esta información para configurar las alarmas para recibir alertas si se infringe un umbral de utilización de IP.
- Hasta 50 recursos con la menor utilización de IP. Puede utilizar esta información para decidir si desea conservar o eliminar los recursos que están infrautilizados.
- Hasta 50 recursos más. Puede utilizar esta información para realizar un seguimiento coherente de la utilización de IP de los recursos que pueden no quedar fuera del grupo de utilización alta o baja.

- Hasta 50 VPC que contengan un CIDR asignado desde un grupo de IPAM (priorizadas según el tamaño total de los bloques de CIDR).
- Hasta 50 subredes cuya VPC contenga un CIDR asignado desde un grupo de IPAM (priorizadas según el tamaño total de los bloques de CIDR).
- Hasta 50 grupos de IPv4 públicas que contengan un CIDR asignado desde un grupo de IPAM (priorizadas según el tamaño total de los bloques de CIDR).

Después de aplicar cada regla, las métricas se agregan y se publican con el mismo nombre de métrica para cada tipo de recurso. Consulte a continuación para obtener información detallada sobre los nombres de las métricas y sus dimensiones.

> **Important**
>
> Hay un límite único para cada tipo de recurso, familia de direcciones y combinación de reglas. El valor predeterminado de cada límite es 50. Para ajustar estos límites, debe ponerse en contacto con el Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.

Example Ejemplo

Supongamos que su IPAM supervisa 2500 VPC y 10 000 subredes, todas con CIDR de IPv4 e IPv6. IPAM publica las siguientes métricas de utilización de IP:

- Hasta 150 métricas de uso de IP IPv4 de VPC, que incluyen:
  - Las 50 VPC con la mayor utilización de IP IPv4
  - Las 50 VPC con la menor utilización de IPv4
  - Hasta 50 VPC que contienen un CIDR de IPv4 asignado desde un grupo de IPAM
- Hasta 150 métricas de uso de IPv6 de VPC, que incluyen:
  - Las 50 VPC con la mayor utilización de IP IPv6
  - Las 50 VPC con la menor utilización de IPv6
  - Hasta 50 VPC que contienen un CIDR de IPv6 asignado desde un grupo de IPAM
- Hasta 150 métricas de uso de IPv4 de subredes, que incluyen:
  - Las 50 subredes con la mayor utilización de IP IPv4
  - Las 50 subredes con la menor utilización de IP IPv4

- Hasta 50 subredes cuya VPC contiene un CIDR de IPv4 asignado desde un grupo de IPAM

Métricas de VPC

El nombre y la descripción de las métricas de VPC se muestran a continuación.

Nombre de métrica	Descripción
VpcIPUsage	El total de IP cubiertas por los CIDR en las subredes de la VPC dividido entre el total de IP cubiertas por los CIDR en la VPC. Esto se calcula en todos los CIDR de VPC del mismo alcance de IPAM y por separado para los CIDR de IPv4 e IPv6.

A continuación, se indican las dimensiones que puede utilizar para filtrar las métricas de VPC.

Dimensión	Descripción
AddressFamily	La familia de direcciones IP de los CIDR de recursos (IPv4 o IPv6).
OwnerID	El ID del propietario de la VPC.
Región	La región de AWS en la que se encuentra la VPC.
ScopeID	El ID del alcance de IPAM al que pertenece la VPC.
VpcID	Es el ID de la VPC.

Métricas de subred

El nombre y la descripción de las métricas de subred se muestran a continuación.

Nombre de métrica	Descripción
SubnetIPUsage	El número de IP activas dividido entre el total de IP en el CIDR de IPv4 de la subred.

A continuación, se indican las dimensiones que puede utilizar para filtrar las métricas de subred.

Dimensión	Descripción
AddressFamily	La familia de direcciones IP de los CIDR de recursos (solo IPv4).
OwnerID	El ID del propietario de la subred.
Región	La región de AWS en la que se encuentra la subred.
ScopeID	El ID del alcance de IPAM al que pertenece la subred.
SubnetID	El ID de la subred.
VpcID	El ID de la VPC a la que pertenece la subred.

Métricas de grupos de IPv4 públicos

El nombre y la descripción de las métricas de grupos de IPv4 públicos se muestran a continuación.

Nombre de métrica	Descripción
PublicIPv4PoolIPUsage	El número de EIP del grupo de IPv4 público dividido entre el total de IP del grupo.

A continuación, se indican las dimensiones que puede utilizar para filtrar las métricas de grupos de IPv4 públicos.

Dimensión	Descripción
OwnerID	El ID del propietario del grupo de IPv4 público.
PublicIPv4PoolID	El ID del grupo de IPv4 público.
Región	La región de AWS en la que se encuentra el grupo de IPv4 público.

Dimensión	Descripción
ScopeID	El ID del alcance de IPAM al que pertenece el grupo de IPv4 público.

Métricas de Información sobre IP públicas

A continuación, se muestran los nombres y las descripciones de las métricas de Información sobre IP públicas.

Nombre de métrica	Descripción
AmazonOwnedElasticIPs	La cantidad de direcciones IP elásticas propiedad de Amazon que ha aprovisionado o asignado a los recursos de su cuenta de AWS.
AssociatedAmazonOwnedElasticIPs	La cantidad de direcciones IP elásticas propiedad de Amazon que ha asociado con los recursos de su cuenta de AWS.
AssociatedBringYourOwnIPs	La cantidad de direcciones IPv4 públicas que ha traído a AWS mediante Traiga sus propias direcciones IP (BYOIP) y ha asociado con recursos en su cuenta de AWS.
BringYourOwnIPs	La cantidad de direcciones IPv4 públicas que ha traído a AWS mediante Traiga sus propias direcciones IP (BYOIP).
EC2PublicIPs	La cantidad de direcciones IPv4 públicas asignadas a instancias de EC2 cuando las instancias se lanzaron en una subred predeterminada o en una subred configurada para asignar de forma automática una dirección IPv4 pública.
ServiceManagedBringYourOwnIPs	La cantidad de direcciones IPv4 públicas que ha traído a AWS mediante Traiga sus propias direcciones IP (BYOIP) que ha aprovisionado y administrado un servicio de AWS.
ServiceManagedIPs	La cantidad de direcciones IPv4 públicas aprovisionadas y administradas por un servicio de AWS.

Nombre de métrica	Descripción
UnassociatedAmazonOwnedElasticIPs	La cantidad de direcciones IP elásticas propiedad de Amazon que no ha asociado con los recursos de su cuenta de AWS.
UnassociatedBringYourOwnIPs	La cantidad de direcciones IPv4 públicas que ha traído a AWS mediante Traiga sus propias direcciones IP (BYOIP) y no ha asociado con recursos en su cuenta de AWS.

A continuación, se indican las dimensiones que puede utilizar para filtrar las métricas de Información sobre IP públicas.

Dimensión	Descripción
IpamId	El ID del IPAM al que pertenece la dirección IP.
Región	La región de AWS en la que se encuentra la dirección IP pública.

Consejo rápido para crear alarmas

Para crear rápidamente una alarma de Amazon CloudWatch para recursos con una alta utilización de direcciones IP, abra la consola de CloudWatch y seleccione Métricas, Todas las métricas, seleccione la pestaña Consulta, seleccione el Espacio de nombres `AWS/IPAM > VPC IP Usage Metrics`, `AWS/IPAM > Subnet IP Usage Metrics` o `AWS/IPAM > Public IPv4 Pool IP Usage Metrics`, seleccione elNombre de métrica `MAX(VpcIPUsage)`, `MAX(SubnetIPUsage)` o `MAX(PublicIPv4PoolIPUsage)`, y seleccione Crear alarma. Para obtener más información, consulte Crear alarmas en las consultas de Metrics Insights en la Guía del usuario de Amazon CloudWatch.

Ver historial de direcciones IP

Siga los pasos de esta sección para ver el historial de una dirección IP o CIDR en un alcance de IPAM. Puede utilizar los datos históricos para analizar y realizar auditorías a las políticas de enrutamiento y la seguridad de red. IPAM retiene de forma automática los datos de monitoreo de direcciones IP durante un máximo de tres años.

Puede utilizar los datos históricos de IP a fin de buscar el cambio de estado de las direcciones IP o CIDR para los siguientes tipos de recursos:

- VPC
- Subredes de la VPC
- Direcciones IP elásticas
- instancias de EC2
- Interfaces de red de EC2 conectadas a instancias

Important

Si bien IPAM no monitorea las instancias de Amazon EC2 ni las interfaces de red de EC2 que están conectadas a instancias, usted puede utilizar la característica Buscar historial de IP para buscar datos históricos en los CIDR de instancia de EC2 e interfaz de red.

Note

- Si mueve un recurso de un alcance de IPAM a otro, el registro de historial anterior finaliza y se crea un registro de historial nuevo bajo el alcance nuevo. Para obtener más información, consulte Mover CIDR de VPC entre alcances.
- Si eliminas o transfieres un recurso a una AWS cuenta que no está supervisada por tu IPAM, el historial nuevo relacionado con el recurso no estará visible y tu IPAM no supervisará el recurso. Sin embargo, se podrá seguir buscando la dirección IP del recurso.
- Si es ustedIntegración de IPAM con cuentas ajenas a su organización, el propietario del IPAM, puede ver el historial de direcciones IP de todos los CIDR de recursos que pertenecen a esas cuentas.

AWS Management Console

Para ver el historial de un CIDR

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Buscar historial de IP.

3. Ingrese una dirección IP IPv4 o IPv6 o un CIDR. Debe ser un CIDR específico para el recurso.
4. Elija un ID de alcance de IPAM.
5. Elija un intervalo de fecha/hora.
6. Si desea filtrar los resultados por VPC, ingrese un ID de VPC. Utilice esta opción si el CIDR aparece en varias VPC.
7. Elija Buscar.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

- Ver el historial de un CIDR: get-ipam-address-history

Para ver ejemplos sobre cómo puede utilizar la AWS CLI para analizar y auditar el uso de direcciones IP, consulte Tutorial: View IP address history using the AWS CLI.

Los resultados de la búsqueda se organizan en las siguientes columnas:

- Sampled end time (Hora de finalización de la muestra): hora de finalización de la muestra de la asociación de recurso a CIDR dentro del alcance de IPAM. Los cambios se recopilan en instantáneas periódicas, por lo que la hora de finalización podría haber ocurrido antes de esta hora específica.
- Sampled start time (Hora de inicio de la muestra): hora de inicio de la muestra de la asociación de recurso a CIDR dentro del alcance de IPAM. Los cambios se recopilan en instantáneas periódicas, por lo que la hora de inicio podría haber ocurrido antes de esta hora específica.

  Example

  Para comprender las horas que ve en Sampled start time (Hora de inicio de la muestra) y Sampled end time (Hora de finalización de la muestra), veamos un ejemplo de caso de uso:

  A las 14.00 h., se creó una VPC con el CIDR 10.0.0.0/16. A las 15.00 h, crea un grupo de IPAM e IPAM con el CIDR 10.0.0.0/8 y selecciona la opción de importación automática para permitir que IPAM descubra e importe cualquier CIDR que se encuentre dentro del rango de direcciones

IP 10.0.0.0/8. Dado que IPAM recopila los cambios en los CIDR en instantáneas periódicas, no descubre el CIDR de VPC existente hasta las 15.05 h. Cuando busca el ID de esta VPC mediante la característica Buscar historial de IP, la hora de inicio de muestra para la VPC es a las 15.05 h, que es cuando IPAM la descubrió, no a las 14.00 h, que es cuando usted creó la VPC. Ahora, digamos que decide eliminar la VPC a las 17.00 h. Cuando se elimina la VPC, el CIDR 10.0.0.0/16 que se asignó a la VPC se recicla de nuevo en el grupo de IPAM. IPAM toma su instantánea periódica a las 17.05 h y recopila el cambio. Cuando busca el ID de esta VPC en Buscar historial de IP, la hora de finalización de muestra para el CIDR de la VPC es a las 17.05 h, no a las 17.00 h, que es cuando se eliminó la VPC.

- Resource ID (ID de recurso): ID generado cuando se asoció el recurso al CIDR.
- Name (Nombre): el nombre del recurso (si procede).
- Compliance status (Estado de conformidad): el estado de conformidad del CIDR.
  - Compliant (Conforme): un recurso administrado cumple las reglas de asignación del grupo de IPAM.
  - Noncompliant (No conforme): el CIDR del recurso no cumple una o más de las reglas de asignación del grupo de IPAM.

    Example

    Si una VPC tiene un CIDR que no cumple con los parámetros de longitud de máscara de red del grupo de IPAM o si el recurso no se encuentra en la misma región de AWS que el grupo de IPAM, se marcará como no conforme.
  - Unmanaged (No administrado): el recurso no tiene un CIDR asignado desde un grupo de IPAM e IPAM no lo está monitoreando para detectar la posible conformidad de CIDR con las reglas de asignación del grupo. Se monitorea el CIDR para detectar superposiciones.
  - Ignored (Ignorado): el recurso administrado se ha elegido para estar exento del monitoreo. Los recursos ignorados no se evalúan para la superposición ni la conformidad con las reglas de asignación. Cuando se elija ignorar un recurso, cualquier espacio asignado a él desde un grupo de IPAM se devuelve al grupo y el recurso no se volverá a importar mediante la importación automática (si la regla de asignación de importación automática se ha establecido en el grupo).
  - -: este recurso no es uno de los tipos de recursos que IPAM puede monitorear o administrar.
- Overlap status (Estado de superposición): el estado de superposición de CIDR.
  - Nonoverlapping (Sin superposición): el CIDR del recurso no se superpone con otro CIDR del mismo alcance.

  - Overlapping (Superposición): el CIDR del recurso se superpone con otro CIDR del mismo alcance. Tenga en cuenta que si se superpone un CIDR del recurso, podría superponerse con una asignación manual.
  - Ignored (Ignorado): el recurso administrado se ha elegido para estar exento del monitoreo. IPAM no evalúa los recursos ignorados para la superposición ni la conformidad con las reglas de asignación. Cuando se elija ignorar un recurso, cualquier espacio asignado a él desde un grupo de IPAM se devuelve al grupo y el recurso no se volverá a importar mediante la importación automática (si la regla de asignación de importación automática se ha establecido en el grupo).
  - -: este recurso no es uno de los tipos de recursos que IPAM puede monitorear o administrar.
- Tipo de recurso
  - vpc: el CIDR se encuentra asociado a una VPC.
  - subnet (subred): el CIDR se encuentra asociado a una subred de VPC.
  - eip: el CIDR se encuentra asociado a una dirección IP elástica.
  - instance (instancia): el CIDR se encuentra asociado a una instancia de EC2.
  - network-interface (interfaz de red): el CIDR se encuentra asociado a una interfaz de red.
- VPC ID (ID de VPC): el ID de la VPC a la que pertenece este recurso (si procede).
- Region (Región): la región de AWS de este recurso.
- Owner ID (ID del propietario): el ID de cuenta de AWS del usuario que creó este recurso (si procede).

Ver Información sobre IP públicas

Puede utilizar Información sobre IP públicas para ver lo siguiente:

- Si su IPAM se ha integrado con las cuentas en una organización de AWS, puede ver todas las direcciones IPv4 públicas que utilizan los servicios en todas las regiones de AWS de toda su organización de AWS.
- Si su IPAM se ha integrado con una única cuenta, puede ver todas las direcciones IPv4 públicas que utilizan los servicios en todas las regiones de AWS en su cuenta.

Una dirección IP pública es una dirección IPv4 a la que se puede enrutar desde Internet. Se necesita una dirección IPv4 pública para poder acceder directamente a un recurso desde Internet a través de IPv4.

> **Note**
>
> AWS cobra por todas las direcciones IPv4 públicas, incluidas las direcciones IPv4 públicas asociadas a las instancias en ejecución y las direcciones IP elásticas. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.

Puede ver información sobre los siguientes tipos de direcciones IPv4 públicas:

- Direcciones IP elásticas (EIP): direcciones IPv4 públicas y estáticas proporcionadas por Amazon que puede asociar a una instancia de EC2, una interfaz de red elástica o un recurso de AWS.
- Direcciones IPv4 públicas de EC2: direcciones IPv4 públicas que Amazon ha asignado a una instancia de EC2 (si la instancia de EC2 se lanza en una subred predeterminada o si la instancia se lanza en una subred configurada para asignar automáticamente una dirección IPv4 pública).
- Direcciones BYOIPv4: direcciones IPv4 públicas en el rango de direcciones IPv4 que ha llevado a AWS mediante Traiga sus propias direcciones IP (BYOIP).
- Direcciones IPv4 administradas por un servicio: direcciones IPv4 públicas aprovisionadas automáticamente en recursos de AWS y administrada por un servicio de AWS. Por ejemplo, las direcciones IPv4 públicas en Amazon ECS, Amazon RDS o Amazon WorkSpaces.

La Información sobre IP públicas muestra todas las direcciones IPv4 públicas que utilizan los servicios entre regiones. Puede utilizar esta información para identificar el uso de direcciones IPv4 públicas y ver las recomendaciones para liberar las direcciones IP elásticas no utilizadas.

- Tipos de IP públicas: número de direcciones IPv4 públicas organizadas por tipo.
  - EIP propiedad de Amazon: direcciones IP elásticas que ha aprovisionado o asignado a los recursos de su cuenta de AWS.
  - IP públicas de EC2: direcciones IPv4 públicas asignadas a instancias de EC2 cuando las instancias se lanzaron en una subred predeterminada o en una subred configurada para asignar automáticamente una dirección IPv4 pública.
  - BYOIP: direcciones IPv4 públicas que ha traído a AWS mediante Traiga sus propias direcciones IP (BYOIP).
  - IP administradas por servicios: direcciones IPv4 públicas aprovisionadas y administradas por un servicio de AWS.

- BYOIP administrado por un servicio: direcciones IPv4 públicas incorporadas a AWS y administradas por un servicio de AWS.
- EIP contiguas propiedad de Amazon: direcciones IP elásticas asignadas desde un grupo del IPAM de IPv4 públicas contiguas proporcionadas por Amazon.

- Uso de EIP: la cantidad de direcciones IP elásticas organizadas según la forma en que se utilizan.
  - EIP asociadas propiedad de Amazon: direcciones IP elásticas que ha aprovisionado en su cuenta de AWS y que ha asociado a una instancia de EC2, una interfaz de red o un recurso de AWS.
  - BYOIP asociadas: direcciones IPv4 públicas que ha traído a AWS utilizando BYOIP que ha asociado a una interfaz de red.
  - EIP propiedad de Amazon no asociadas: direcciones IP elásticas que ha aprovisionado en su cuenta de AWS, pero que no ha asociado a ninguna interfaz de red.
  - BYOIP no asociadas: direcciones IPv4 públicas que ha traído a AWS utilizando BYOIP, pero que no ha asociado a ninguna interfaz de red.
  - EIP contiguas asociadas propiedad de Amazon: direcciones IP elásticas asignadas desde un grupo del IPAM de IPv4 públicas contiguas proporcionadas por Amazon y asociadas a un recurso.
  - EIP contiguas propiedad de Amazon sin asociar: direcciones IP elásticas asignadas desde un grupo del IPAM de IPv4 públicas contiguas proporcionadas por Amazon y no asociadas a ningún recurso.
- Uso de IPv4 contiguas propiedad de Amazon: una tabla en la que se muestra el uso de direcciones IPv4 públicas contiguas a lo largo del tiempo y los grupos del IPAM de IPv4 relacionados propiedad de Amazon.
- Direcciones IP públicas: tabla de direcciones IPv4 públicas y sus atributos.
  - Direcciones IP: la dirección IPv4 pública.
  - Asociada: si la dirección está asociada o no a una instancia de EC2, una interfaz de red o un recurso de AWS.
    - Asociada: la dirección IPv4 pública está asociada a una instancia de EC2, una interfaz de red o un recurso de AWS.
    - No asociada: la dirección IPv4 pública no está asociada a ningún recurso y está inactiva en su cuenta de AWS.
  - Tipo de dirección: el tipo de dirección IP.
    - EIP propiedad de Amazon: la dirección IPv4 pública es una dirección IP elástica.

  - BYOIP: la dirección IPv4 pública se trajo a AWS mediante BYOIP.
  - IP pública de EC2: la dirección IPv4 pública se asignó automáticamente a una instancia de EC2.
  - Servicio administrado por traiga su propia IP (BYOIP): la dirección IPv4 pública se trajo a AWS mediante traiga su propia IP (BYOIP).
  - IP administradas por servicios: un servicio de AWS aprovisionó y administra las direcciones IPv4 públicas.
- Servicio: el servicio al que está asociada la dirección IP.
  - AGA: una AWS Global Accelerator. Si se utiliza un acelerador de enrutamiento personalizado, sus IP públicas no aparecen en la lista. Para ver estas IP públicas, consulte Ver tus aceleradores de enrutamiento personalizados.
  - Database Migration Service: una instancia de replicación de AWS Database Migration Service (DMS).
  - Redshift: un clúster de Amazon Redshift.
  - RDS: una instancia de Amazon Relational Database Service (RDS).
  - Equilibrador de carga (EC2): un equilibrador de carga de aplicación o un equilibrador de carga de red.
  - Puerta de enlace NAT (VPC): una puerta de enlace NAT pública de Amazon VPC.
  - Site-to-Site VPN: una puerta de enlace privada virtual de AWS Site-to-Site VPN.
  - Otros: otro servicio que no se puede identificar actualmente.
- Nombre (ID de EIP): si esta dirección IPv4 pública es una asignación de direcciones IP elásticas, se trata del nombre y el ID de la asignación de EIP.
- ID de interfaz de red: si esta dirección IPv4 pública está asociada a una interfaz de red, se trata del ID de la interfaz de red.
- ID de instancia: si esta dirección IPv4 pública está asociada a una instancia de EC2, se trata del ID de la instancia.
- Grupos de seguridad: si esta dirección IPv4 pública está asociada a una instancia de EC2, se trata del nombre y el ID del grupo de seguridad asignado a la instancia.
- Grupo de IPv4 público: si se trata de una dirección IP elástica de un grupo de direcciones IP propiedad de Amazon y administrado por Amazon, el valor es «-». Si se trata de una dirección IP elástica de un rango de direcciones IP de su propiedad y que ha traído a Amazon (mediante BYOIP), el valor es el ID del grupo de IPv4 público.

- Grupo de borde de red: si se anuncia la dirección IP, se trata de la región de AWS desde la que se anuncia la dirección IP.
- ID del propietario: el número de cuenta de AWS del propietario del recurso.
- Tiempo de muestra: el último tiempo de detección de recursos exitoso.
- ID de detección de recursos: ID de la detección de recursos que ha descubierto esta dirección IPv4 pública.
- Recurso de servicio: ARN o ID del recurso.

Si tiene asignada una dirección IP elástica a su cuenta, pero no está asociada a una interfaz de red, se mostrará un banner informándole de que tiene EIP no asociadas en su cuenta y que debe liberarlas.

> **Important**
>
> La Información sobre IP públicas se ha actualizado recientemente. Si aparece un error relacionado con la falta de permisos para llamar a GetIpamDiscoveredPublicAddresses, se debe actualizar el permiso administrado adjunto a la detección de recursos que recibió. Póngase en contacto con la persona que creó la detección de recursos y pídale que actualice el permiso administrado `AWSRAMPermissionIpamResourceDiscovery` a la versión predeterminada. Para obtener más información, consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM.

AWS Management Console

Para ver la información sobre las direcciones IP públicas

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, seleccione Información sobre IP públicas.
3. Para ver los detalles de una dirección IP pública, selecciónela haciendo clic en ella.
4. Consulte la siguiente información sobre la dirección IP:
   - Detalles: la misma información visible en las columnas del panel principal de Información sobre IP públicas, como el Tipo de direcciónyel Servicio.

- Reglas de grupos de seguridad entrantes: si esta dirección IP está asociada a una instancia de EC2, estas son las reglas del grupo de seguridad que controlan el tráfico entrante a la instancia.
- Reglas de grupos de seguridad salientes: si esta dirección IP está asociada a una instancia de EC2, estas son las reglas del grupo de seguridad que controlan el tráfico saliente de la instancia.
- Etiquetas: pares de clave y valor que funcionan como metadatos para organizar los recursos de AWS.

Command line

Utilice el siguiente comando para obtener las direcciones IP públicas detectadas por IPAM: get-ipam-discovered-public-addresses

Tutoriales para IP Address Manager de Amazon VPC

En los siguientes tutoriales, aprenderá a realizar tareas de IPAM comunes mediante AWS CLI. Para obtener AWS CLI, consulte Acceso a IPAM. Para más información sobre los conceptos de IPAM que se mencionan en estos tutoriales, consulte Cómo funciona IPAM.

Contenido

Introducción a IPAM con la CLI de AWS

En este tutorial, se muestra el proceso de configuración y uso del administrador de direcciones IP (IPAM) de Amazon VPC con la CLI de AWS usando una sola cuenta de AWS. Al final de este tutorial, habrá creado un IPAM, una jerarquía de grupos de direcciones IP y habrá asignado un CIDR a una VPC.

Requisitos previos

Antes de empezar este tutorial, asegúrese de contar con lo siguiente:

- Una cuenta de AWS con permisos para crear y administrar los recursos de IPAM.
- La CLI de AWS instalada y configurada con las credenciales adecuadas. Para obtener información sobre cómo instalar la CLI de AWS, consulte Instalar o actualizar la versión más reciente de la CLI de AWS. Para obtener información acerca de la configuración de la CLI de AWS, consulte Fundamentos de configuración.

- Comprensión básica del direccionamiento IP y la notación CIDR.
- Conocimientos básicos de los conceptos sobre Amazon VPC.
- Completar el tutorial lleva aproximadamente 30 minutos.

Creación de un IPAM

El primer paso es crear un IPAM con regiones de operación. Un IPAM le ayudará a planificar, rastrear y supervisar las direcciones IP de sus cargas de trabajo de AWS.

Cree un IPAM con regiones operativas en us-east-1 y us-west-2:

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

Este comando crea un IPAM y le permite administrar las direcciones IP en las regiones especificadas. Las regiones operativas son las regiones de AWS en las que el IPAM puede administrar los CIDR de la dirección IP.

Verifique que se haya creado su IPAM:

```
aws ec2 describe-ipams
```

Anote el ID de IPAM de la salida, ya que lo necesitará en los pasos siguientes.

Espere a que el IPAM esté completamente creado y disponible (aproximadamente 20 segundos):

```
sleep 20
```

Obtención del ID del alcance de IPAM

Al crear un IPAM, AWS crea automáticamente un alcance privado y otro público. Para este tutorial, utilizaremos el alcance privado.

Recupere los detalles del IPAM y extraiga el ID del alcance privado:

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

Sustituya `ipam-0abcd1234` por su ID del IPAM real.

En la salida, identifique y anote el ID del alcance privado del campo `PrivateDefaultScopeId`. Tendrá un aspecto similar a `ipam-scope-0abcd1234`.

Creación de un grupo IPv4 de nivel superior

Ahora, crearemos un grupo de nivel superior en el alcance privado. Este grupo servirá como elemento principal para todos los demás grupos en nuestra jerarquía.

Cree un grupo IPv4 de nivel superior:

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

Reemplace `ipam-scope-0abcd1234` con su ID de alcance privado real.

Espere a que el grupo esté completamente creado y disponible:

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

Reemplace `ipam-pool-0abcd1234` con su ID de grupo de nivel superior real. El estado debe ser `create-complete` antes de continuar.

Una vez que el grupo esté disponible, aprovisione un bloque CIDR en él:

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

Espere a que el CIDR esté completamente aprovisionado:

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

El estado debe ser `provisioned` antes de continuar.

Creación de un grupo regional de IPv4

Luego, cree un grupo regional dentro del grupo de nivel superior. Este grupo será específico de una región de AWS en particular.

Cree un grupo regional de IPv4:

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

Reemplace `ipam-scope-0abcd1234` con su ID de alcance privado real y `ipam-pool-0abcd1234` con su ID de grupo de nivel superior.

Espere a que el grupo regional esté completamente creado y disponible:

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

Reemplace `ipam-pool-1abcd1234` con su ID del grupo regional real. El estado debe ser `create-complete` antes de continuar.

Una vez que el grupo esté disponible, aprovisione un bloque CIDR en él:

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

Espere a que el CIDR esté completamente aprovisionado:

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

El estado debe ser `provisioned` antes de continuar.

Creación de un grupo IPv4 de desarrollo

Ahora, cree un grupo de desarrollo dentro del grupo regional. Este grupo se utilizará para entornos de desarrollo.

Cree un grupo IPv4 de desarrollo:

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

Reemplace `ipam-scope-0abcd1234` con su ID de alcance privado real y `ipam-pool-1abcd1234` con su ID de grupo regional.

Nota: Es importante incluir el parámetro `--locale` para que coincida con la ubicación del grupo principal.

Espere a que el grupo de desarrollo esté completamente creado y disponible:

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

Reemplace `ipam-pool-2abcd1234` por el ID de su grupo de desarrollo real. El estado debe ser `create-complete` antes de continuar.

Una vez que el grupo esté disponible, aprovisione un bloque CIDR en él:

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

Espere a que el CIDR esté completamente aprovisionado:

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

El estado debe ser `provisioned` antes de continuar.

Creación de una VPC que utilice un CIDR de grupo de IPAM

Por último, cree una VPC que utilice un CIDR de su grupo de IPAM. Esto demuestra cómo se puede utilizar el IPAM para asignar espacio de direcciones IP a los recursos de AWS.

Cree una VPC que utilice un CIDR de grupo de IPAM:

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

Reemplace `ipam-pool-2abcd1234` por el ID de su grupo de desarrollo real.

El parámetro `--ipv4-netmask-length 26` especifica que desea asignar un bloque CIDR /26 (64 direcciones IP) desde el grupo. Se elige la longitud de esta máscara de red para garantizar que sea más pequeña que el bloque CIDR del grupo (/24).

Verifique que se haya creado su VPC:

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

Verificación de la asignación del grupo de IPAM

Compruebe que el CIDR se haya asignado desde su grupo de IPAM:

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

Reemplace `ipam-pool-2abcd1234` por el ID de su grupo de desarrollo real.

Este comando muestra todas las asignaciones del grupo de IPAM especificado, incluida la VPC que acaba de crear.

Solución de problemas

A continuación se presentan algunos problemas comunes que pueden surgir al trabajar con un IPAM:

- Errores de permisos: asegúrese de que su usuario o rol de IAM tenga los permisos necesarios para crear y administrar los recursos del IPAM. Es posible que necesite los permisos `ec2:CreateIpam`, `ec2:CreateIpamPool` y otros relacionados.

- Límite de recursos superado: de forma predeterminada, solo puede crear un IPAM por cuenta. Si ya tiene un IPAM, tendrá que eliminarlo antes de crear uno nuevo o deberá usar el existente.
- Fallos en la asignación de los CIDR: al aprovisionar los CIDR a los grupos, asegúrese de que el CIDR que intenta aprovisionar no se superponga con las asignaciones existentes en otros grupos.
- Tiempos de espera de las solicitudes de API agotados: si aparecen errores “RequestExpired”, es posible que se deban a problemas de latencia de la red o de sincronización horaria. Vuelva a intentar ejecutar el comando.
- Errores de estado incorrecto: si recibe errores “IncorrectState”, es posible que se deban a que está intentando realizar una operación en un recurso que no está en el estado correcto. Espere a que el recurso se haya creado o aprovisionado por completo antes de continuar.
- Errores del tamaño de la asignación: si recibe errores “InvalidParameterValue” sobre el tamaño de la asignación, asegúrese de que la longitud de la máscara de red que solicita sea adecuada para el tamaño del grupo. Por ejemplo, no puede asignar un CIDR de /25 desde un grupo de /24.
- Infracciones de dependencia: al limpiar los recursos, es posible que aparezca el error “DependencyViolation”. Esto se debe a que los recursos dependen unos de otros. Asegúrese de eliminar los recursos siguiendo el orden inverso al de su creación y de desaprovisionar los CIDR antes de eliminar los grupos.

Eliminar recursos

Cuando haya completado este tutorial, debería limpiar los recursos que creó para evitar incurrir en gastos innecesarios.

1. Elimine la VPC:

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

2. Desaprovisione el CIDR del grupo de desarrollo:

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

3. Elimine el grupo de desarrollo:

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

4. Desaprovisione el CIDR del grupo regional:

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

5. Elimine el grupo regional:

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

6. Desaprovisione el CIDR del grupo de nivel superior:

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

7. Elimine el grupo de nivel superior:

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

8. Elimine el IPAM:

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

Reemplace todos los ID con los ID de sus recursos reales.

> **Note**
>
> Es posible que tenga que esperar entre estas operaciones para que los recursos se eliminen por completo antes de continuar con el siguiente paso. Si aparecen infracciones de dependencia, espere unos segundos y vuelva a intentarlo.

Pasos a seguir a continuación

Ahora que ha aprendido a crear y usar un IPAM con la CLI de AWS, tal vez quiera explorar otras características avanzadas:

- Planificar el aprovisionamiento de direcciones IP: Aprenda a planificar su espacio de direcciones IP de forma eficaz.
- Monitorear el uso de CIDR por recurso: Comprenda cómo supervisar el uso de direcciones IP.

- Compartir un grupo de IPAM mediante AWS RAM: Aprenda a compartir grupos de IPAM entre cuentas de AWS.
- Integración de IPAM con cuentas en una organización de AWS: Descubra cómo utilizar el IPAM en toda su organización.

Tutorial: crear un IPAM y grupos utilizando la consola

En este tutorial se crea un IPAM, se integra con AWS Organizations, se crean grupos de direcciones IP y se crea una VPC con un CIDR a partir de un grupo de IPAM.

Este tutorial le muestra cómo puede utilizar IPAM para organizar el espacio de direcciones IP basado en diferentes necesidades de desarrollo. Una vez que haya completado este tutorial, tendrá un grupo de direcciones IP para los recursos de preproducción. A continuación, puede crear otros grupos en función de sus necesidades de enrutamiento y seguridad, como un grupo para recursos de producción.

Aunque puede utilizar IPAM como usuario único, la integración con AWS Organizations le permite gestionar direcciones IP en todas las cuentas de su organización. Este tutorial cubre la integración de IPAM con las cuentas de una organización. No explica lo siguiente: Integración de IPAM con cuentas ajenas a su organización.

> **Note**
>
> A efectos de este tutorial, las instrucciones le indicarán que nombre los recursos de IPAM de una forma determinada, que cree recursos IPAM en regiones específicas y que utilice rangos CIDR de direcciones IP específicos para sus grupos. Con ello se pretende conseguir una agilización de las opciones disponibles en IPAM y que pueda empezar a utilizarlo rápidamente. Una vez que haya completado este tutorial, puede decidir crear un nuevo IPAM y configurarlo de manera diferente.

Contenido

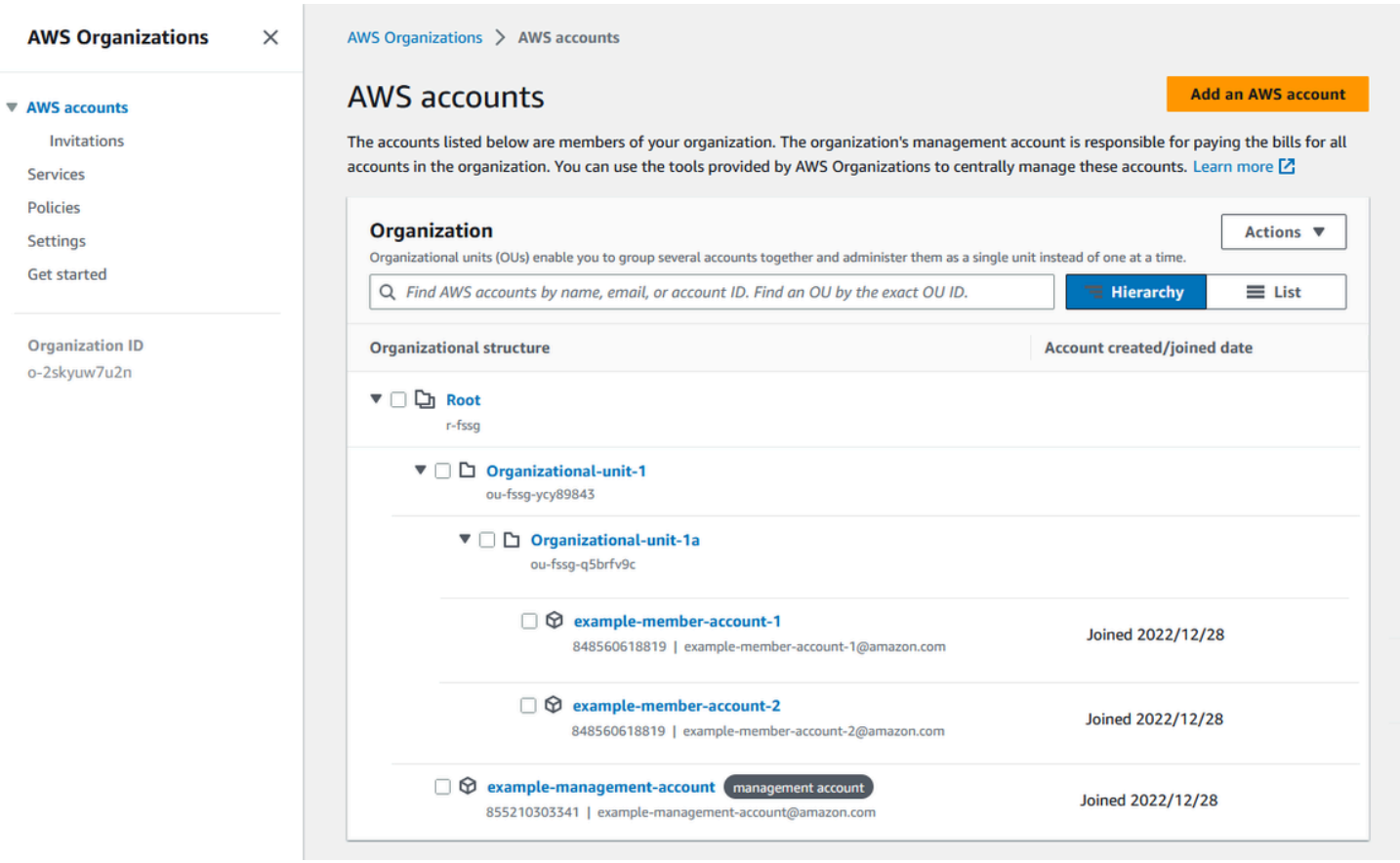
Requisitos previos

Antes de empezar, debe haber creado una cuenta de AWS Organizations con al menos un miembro. Para obtener instrucciones sobre cómo hacerlo, consulte Creación y administración de una organización en la Guía del usuario de AWS Organizations.

Cómo AWS Organizations se integra con IPAM

Esta sección muestra un ejemplo de las cuentas de AWS Organizations que se utilizan en este tutorial. Hay tres cuentas en su organización que utilizará al realizar la integración con IPAM en este tutorial:

- La cuenta de administración (llamada example-management-account en la siguiente imagen) permite iniciar sesión en la consola de IPAM y delegar un administrador de IPAM. No puede utilizar la cuenta de administración de la organización como administrador de IPAM.
- Una cuenta miembro (llamada example-member-account-1 en la siguiente imagen) como cuenta de administrador de IPAM. La cuenta de administrador de IPAM es responsable de crear un IPAM y utilizarlo para administrar y monitorear el uso de direcciones IP en toda la organización. Cualquier cuenta de miembro de su organización puede ser delegada como administrador de IPAM.
- Una cuenta de miembro (denominada example-member-account-2 en lo que sigue) como cuenta de desarrollador. Esta cuenta crea una VPC con un CIDR asignado desde un grupo de IPAM.



Además de las cuentas, necesitará el ID de la unidad organizativa (ou-fssg-q5brfv9c en la imagen anterior) que contiene la cuenta de miembro que utilizará como cuenta de desarrollador. Se necesita este ID para que, en un paso posterior, cuando comparta su grupo de IPAM, pueda compartirlo con esta OU.

> **Note**
>
> Para más información sobre tipos de cuentas de AWS Organizations, como las de administración y las de miembros, consulte la terminología y los conceptos AWS Organizations.

Paso 1: Delegue un administrador de IPAM

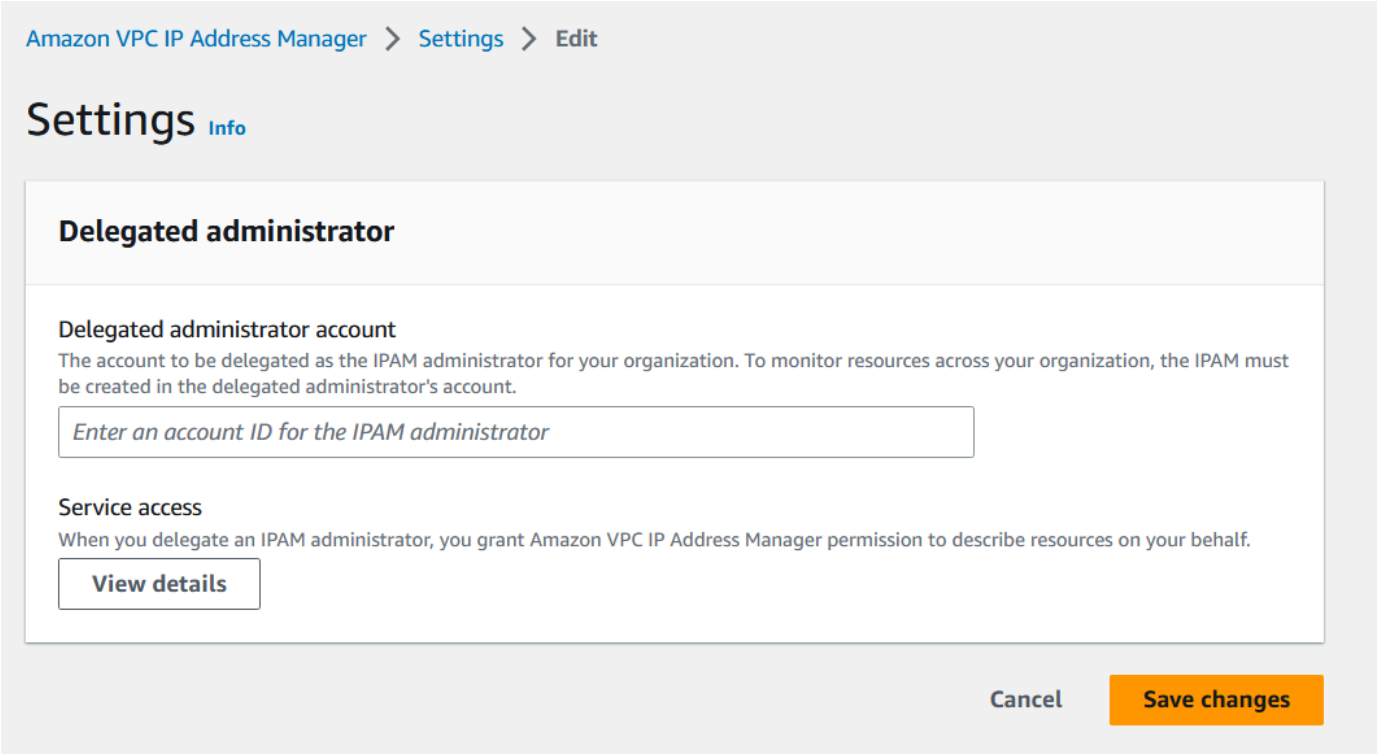
En este paso, delegará una cuenta de miembro de AWS Organizations como administrador de IPAM. Al delegar un administrador de IPAM, se crea automáticamente un rol vinculado al servicio en cada una de sus cuentas de miembro de AWS Organizations. IPAM supervisa el uso de la dirección IP en

estas cuentas asumiendo el rol vinculado al servicio en cada cuenta miembro. A continuación, puede descubrir los recursos y sus CIDR independientemente de su unidad organizativa.

No puede completar este paso a menos que tenga los permisos necesarios AWS Identity and Access Management (IAM). Para obtener más información, consulte Integración de IPAM con cuentas en una organización de AWS.

Para delegar una cuenta de administrador IPAM

1. Utilizando la cuenta de administración de AWS Organizations, abra la consola de IPAM en https://console.aws.amazon.com/iam/.
2. En la Consola de administración de AWS, seleccione la región de AWS donde quiera trabajar con IPAM.
3. En el panel de navegación, elija Configuración de la organización.
4. Elija Delegar. La opción Delegar solo está disponible si ha iniciado sesión en la consola como la cuenta de administración de AWS Organizations.
5. Introduzca el ID de cuenta de AWS para una cuenta de miembro de la organización. El administrador de IPAM debe ser una cuenta de miembro de AWS Organizations, no la cuenta de administración.



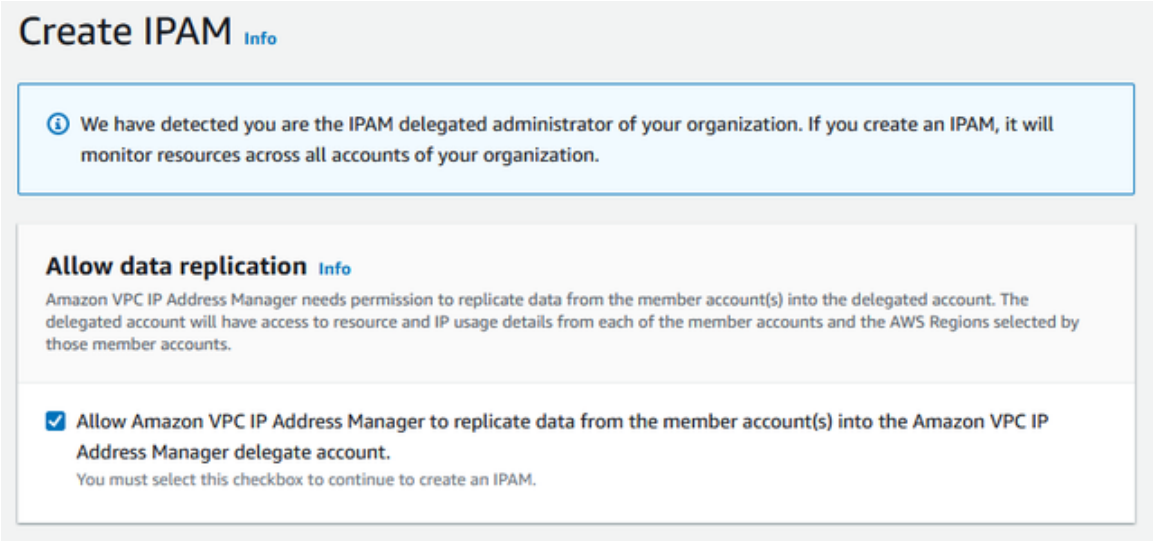
6. Seleccione Save changes (Guardar cambios). La información del administrador delegado se rellena con detalles relacionados con la cuenta del miembro.

Paso 2: Cree un IPAM

En este paso, creará un IPAM. Cuando se crea un IPAM, este crea automáticamente dos ámbitos para el mismo: el ámbito privado, destinado a todo el espacio privado, y el ámbito público, destinado a todo el espacio público. Los alcances, junto con los grupos y las asignaciones, son componentes clave de su IPAM. Para obtener más información, consulte Cómo funciona IPAM.

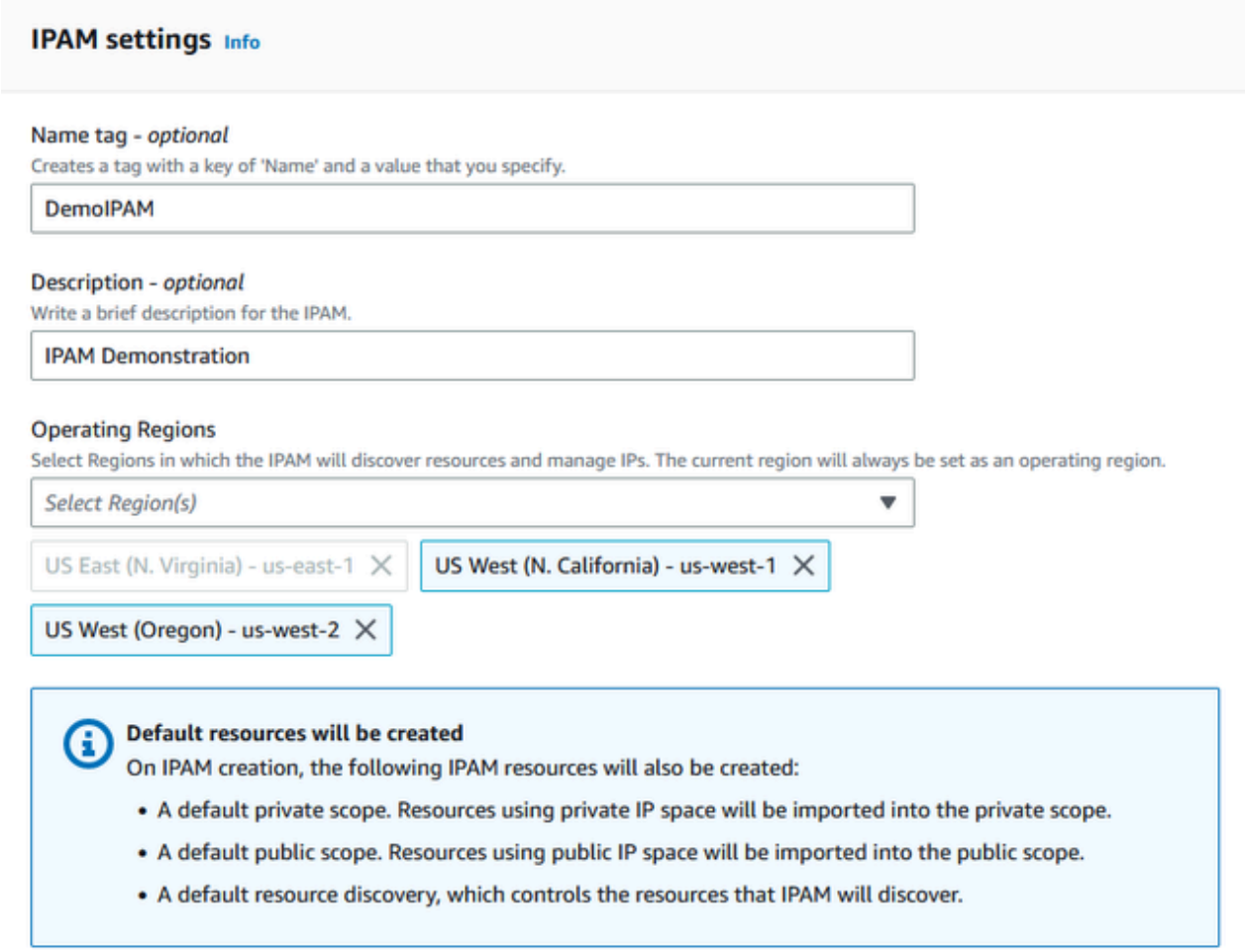
Para crear un IPAM

1. Utilizando la cuenta de miembro AWS Organizations delegada como administrador de IPAM en el paso anterior, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En la AWS Management Console, elija la región de AWS en la que desea crear el IPAM. Cree el IPAM en su región principal de operaciones.
3. En la página de inicio del servicio, elija Create IPAM (Crear IPAM).
4. Seleccione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir al Administrador de direcciones IP de Amazon VPC replicar los datos de las cuentas de origen en la cuenta delegada de IPAM). Si no selecciona esta opción, no puede crear un IPAM.

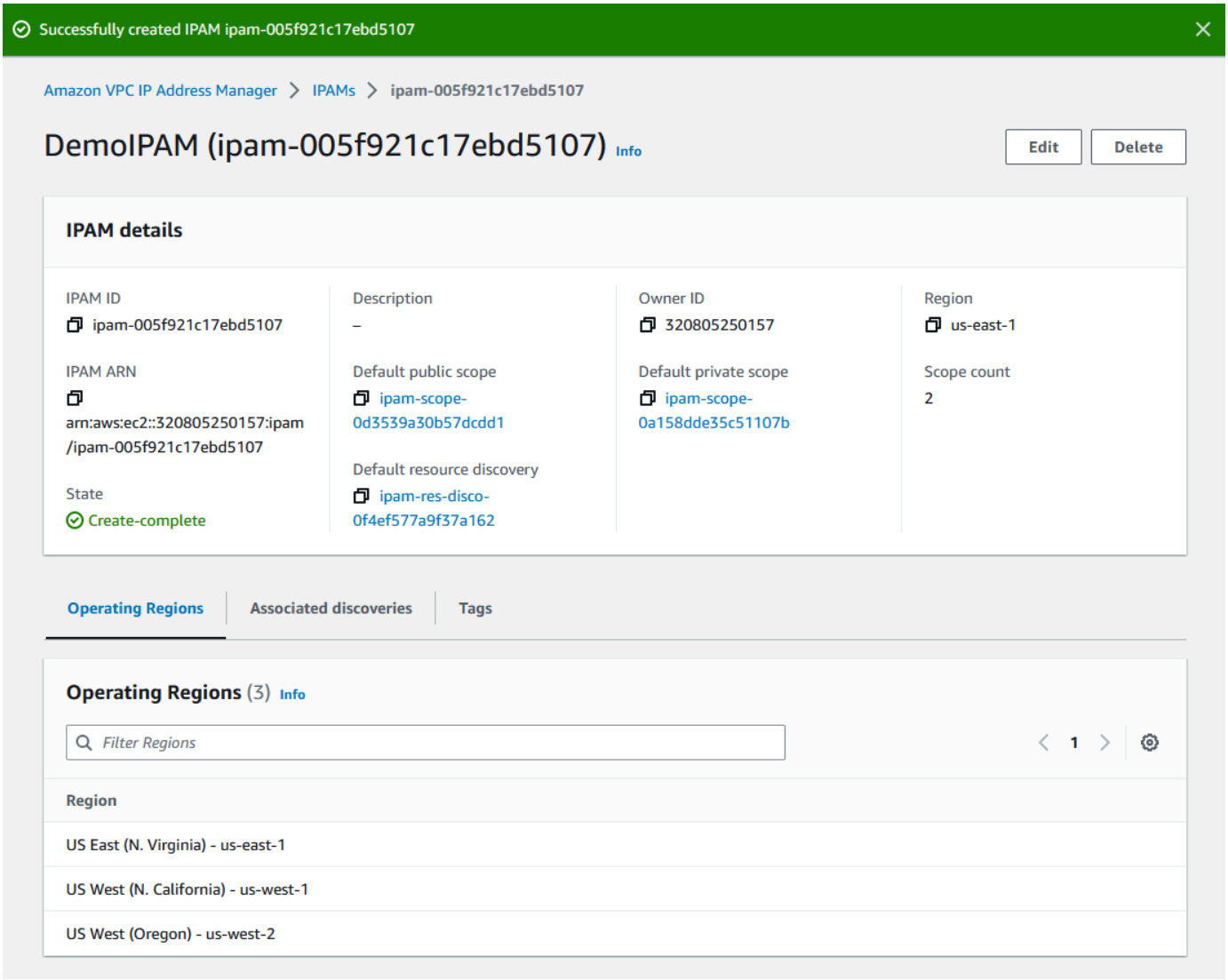


5. En Regiones operativas, seleccione las regiones de AWS en las que este IPAM puede administrar y localizar recursos. La región de AWS en la que va a crear su IPAM se selecciona automáticamente como una de las regiones operativas. En este tutorial, la región de origen

de nuestro IPAM es us-east-1, por lo que elegiremos us-west-1 y us-west-2 como regiones operativas adicionales. Si olvida una región operativa, puede editar la configuración de IPAM más tarde y añadir o eliminar regiones.



6. Elija Create IPAM (Crear IPAM).



Paso 3: Cree un grupo de IPAM de nivel superior

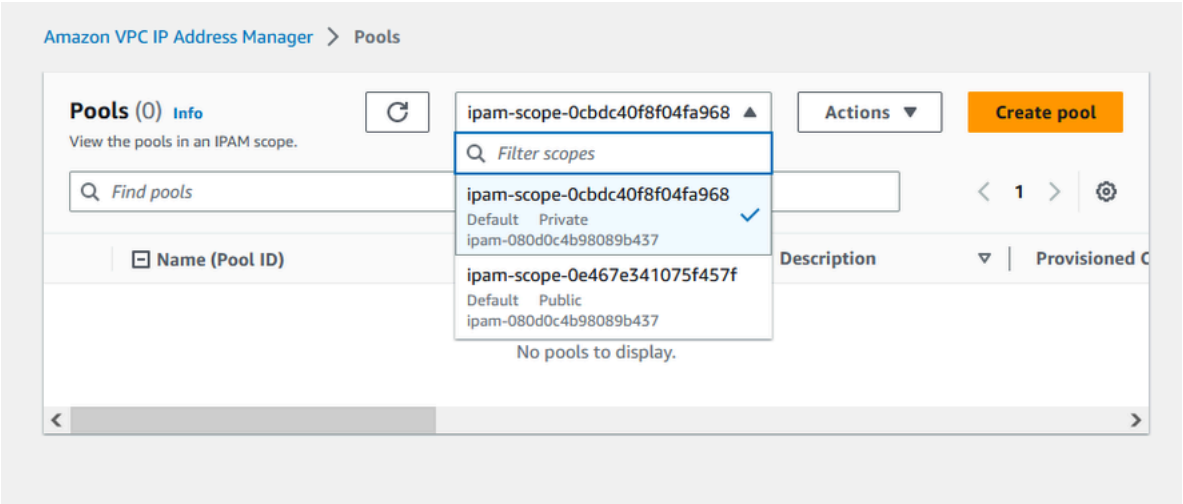
En este tutorial, se crea una jerarquía de grupos, empezando por el grupo de IPAM de nivel superior. En los pasos siguientes, creará un par de grupos regionales y un grupo de desarrollo para preproducción en uno de los grupos regionales.

Para más información sobre las jerarquías de grupos que se pueden crear con IPAM, consulte Ejemplos de planes de grupos de IPAM.

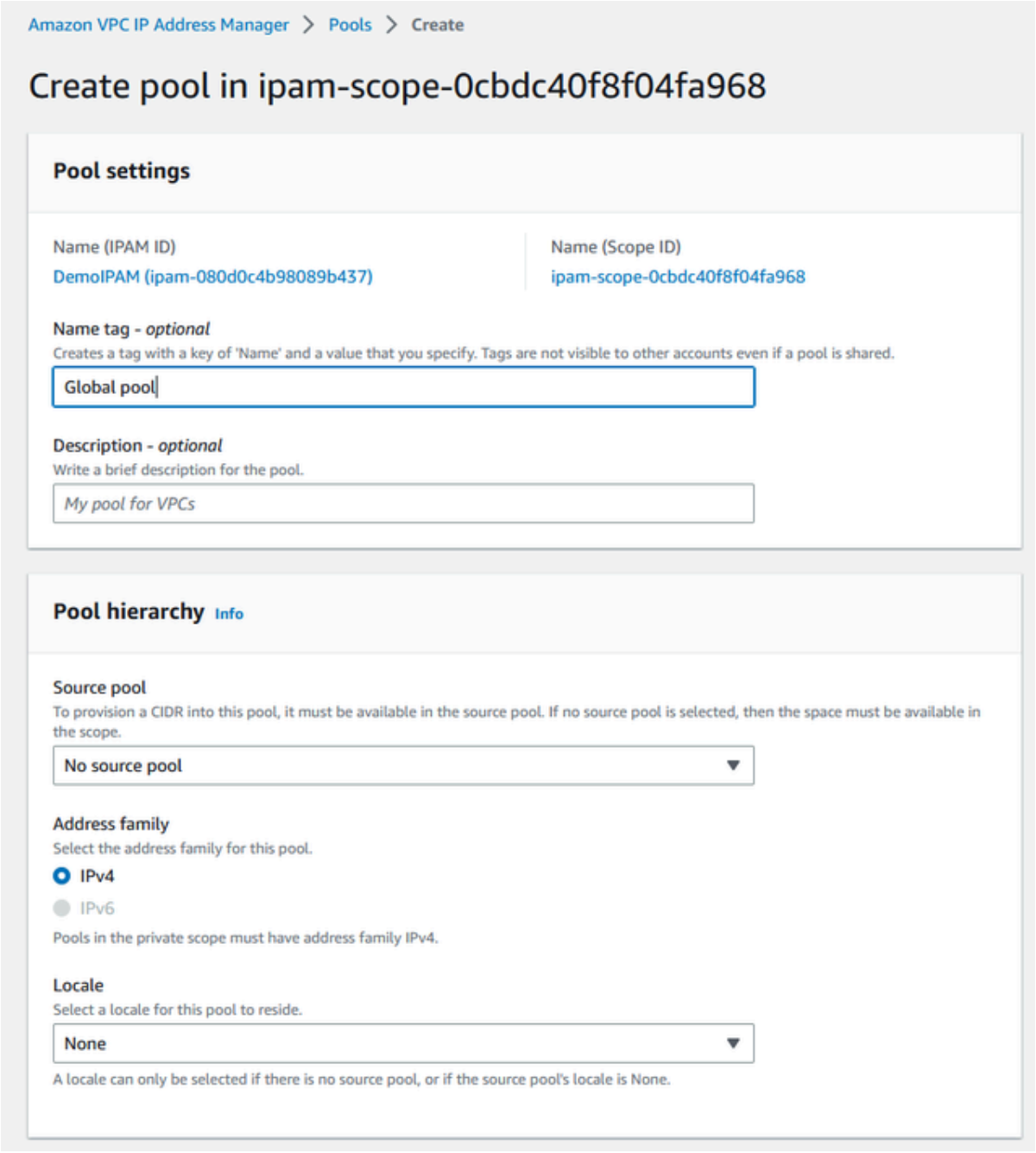
Crear un grupo de nivel superior

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.

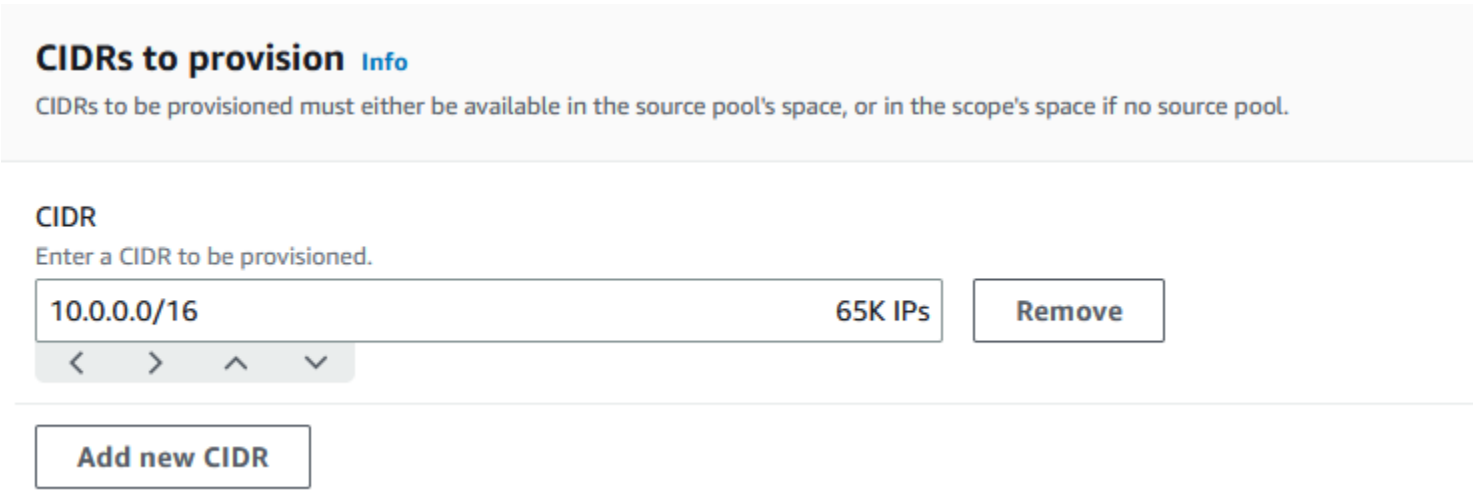
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado.



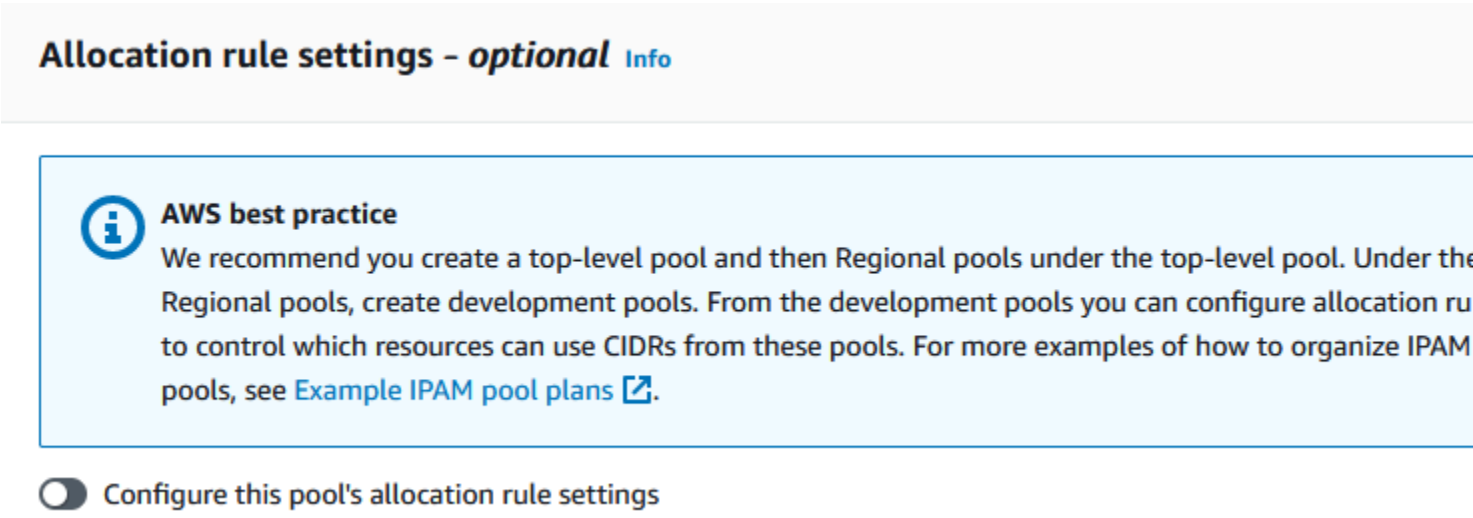
4. Elija Create pool (Crear grupo).
5. En Álcance de IPAM, deje seleccionado el alcance privado.
6. (Opcional) Añada una etiqueta de nombre y una descripción para el grupo, como “Grupo global”.
7. En Origen, elija Alcance del IPAM. Dado que se trata de un grupo de nivel superior, no tendrá un grupo de origen.
8. En Address family (Familia de direcciones), elija IPv4.
9. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
10. Para Locale (Configuración regional), elija None (Ninguna). Las cuentas regionales son las regiones de AWS en las que desea que este grupo de IPAM esté disponible para asignaciones. En la siguiente sección de este tutorial establecerá la configuración regional de los grupos regionales que cree.



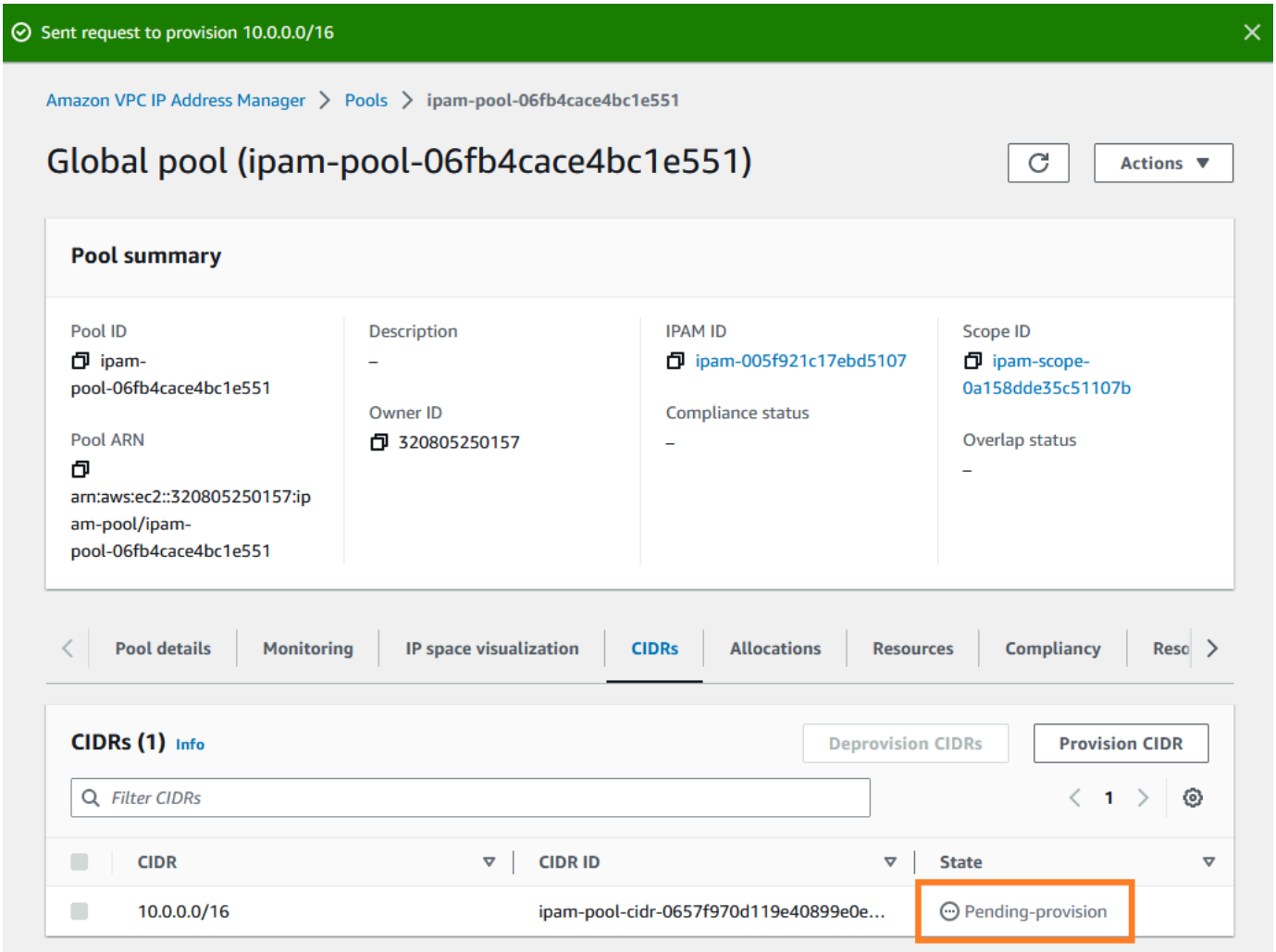
11. Elija un CIDR para aprovisionar al grupo. En este ejemplo, aprovisionamos 10,0.0.0/16.



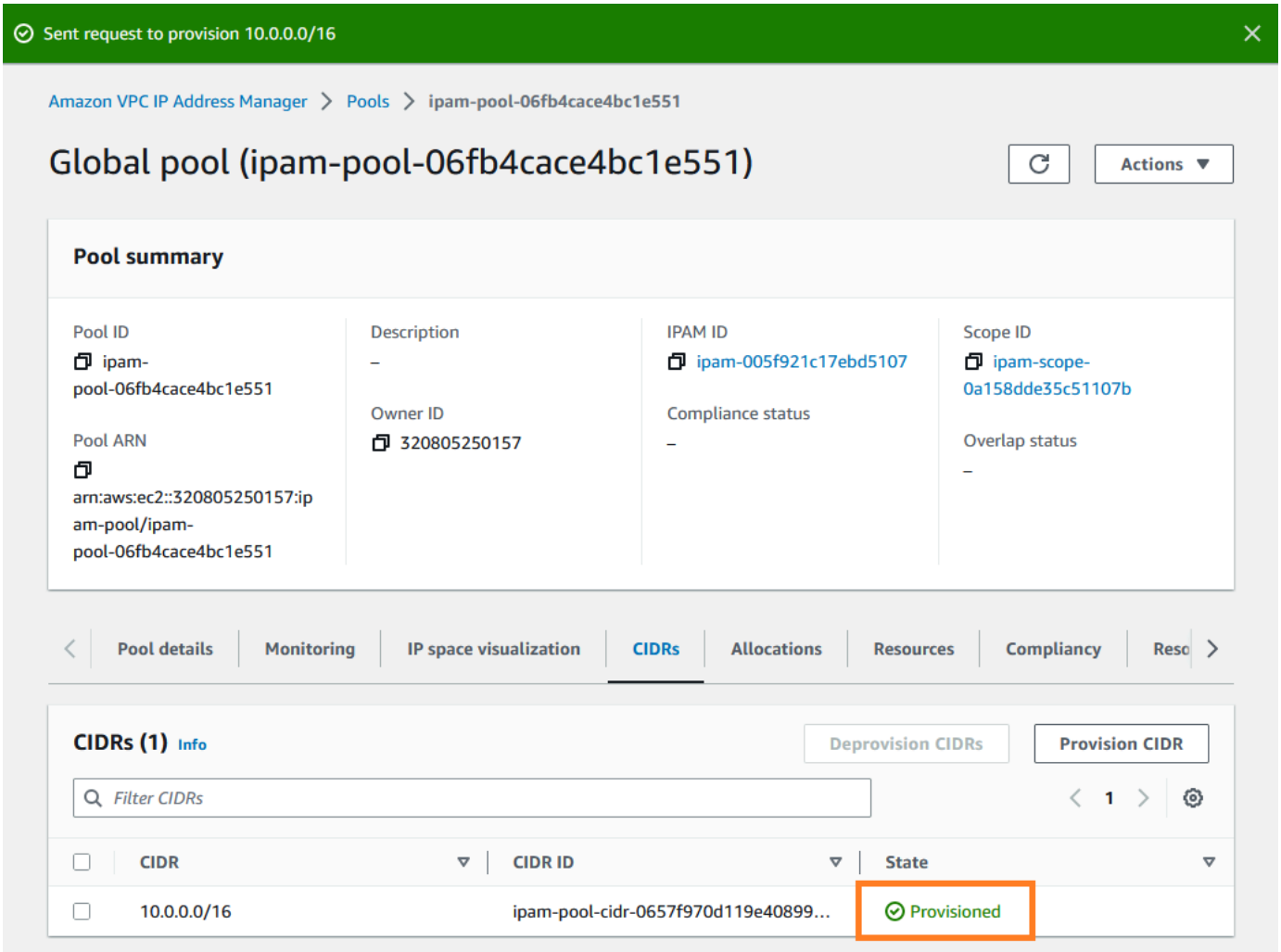
12. Deje deshabilitada la opción Configuración de las reglas de asignación de este grupo. Este es nuestro grupo de nivel superior, y no se asignarán CIDR a las VPC directamente desde este grupo. En su lugar, los asignará desde un grupo secundario que creará a partir de este grupo.



13. Elija Create pool (Crear grupo). El grupo se crea y el CIDR se encuentra en estado Pendiente de aprovisionamiento:



14. Espere a que el estado sea Aprovisionado antes de pasar al siguiente paso.



Ahora que ha creado el grupo de nivel superior, creará grupos regionales en us-west-1 y us-west-2.

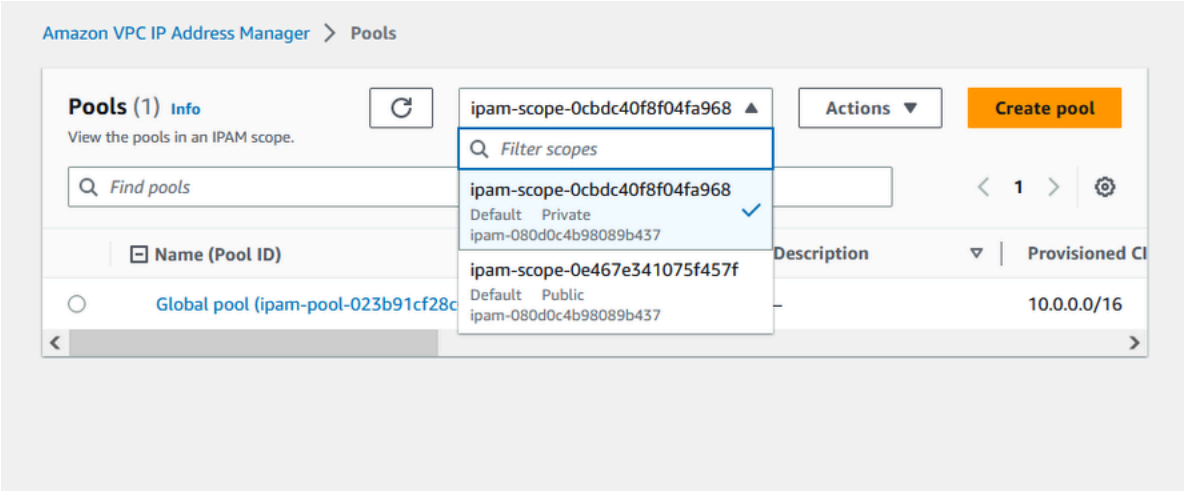
Paso 4: Cree grupos de IPAM regionales

Esta sección muestra cómo organizar direcciones IP utilizando dos grupos regionales. En este tutorial, seguiremos uno de los planes de grupo de IPAM de ejemplo y crearemos dos grupos regionales que pueden utilizarse por las cuentas miembro de la organización para asignar CIDR a las VPC.

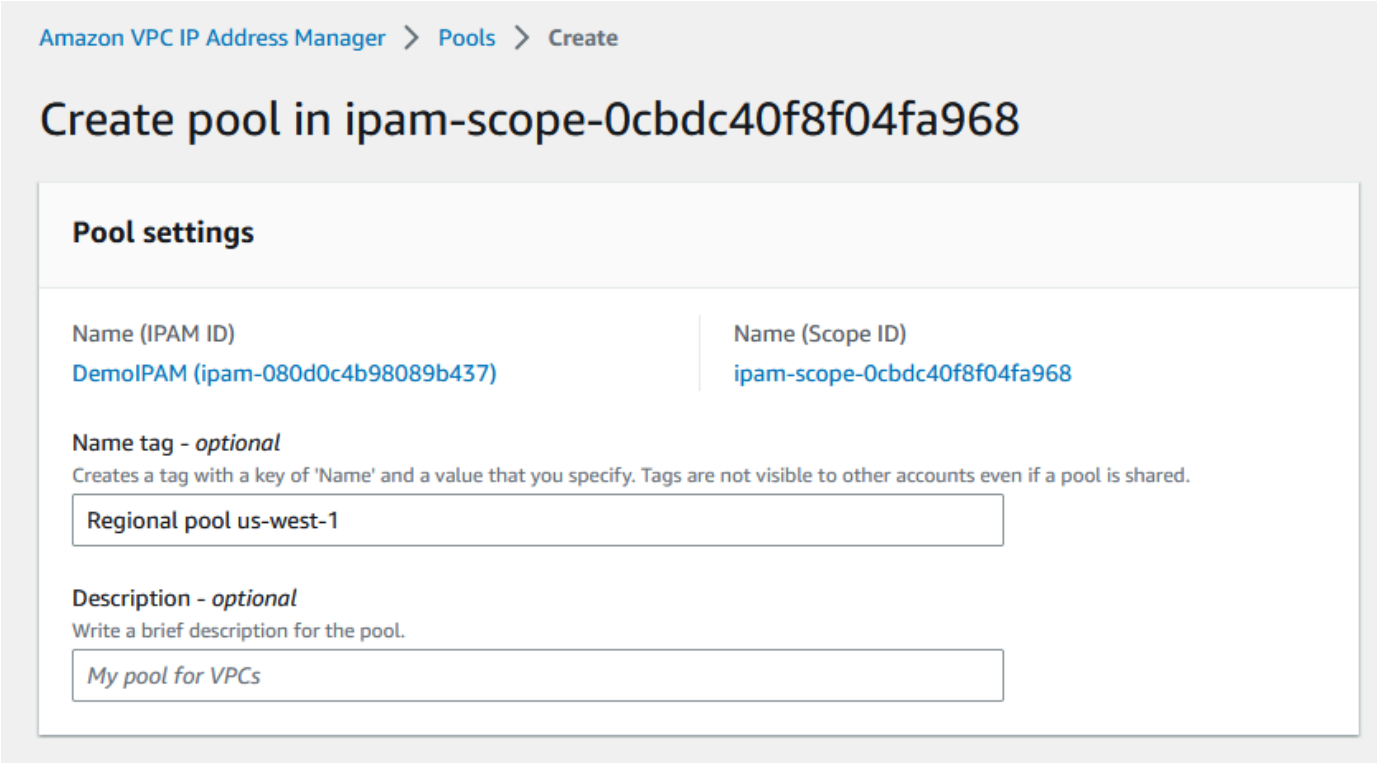
Crear un grupo regional

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).

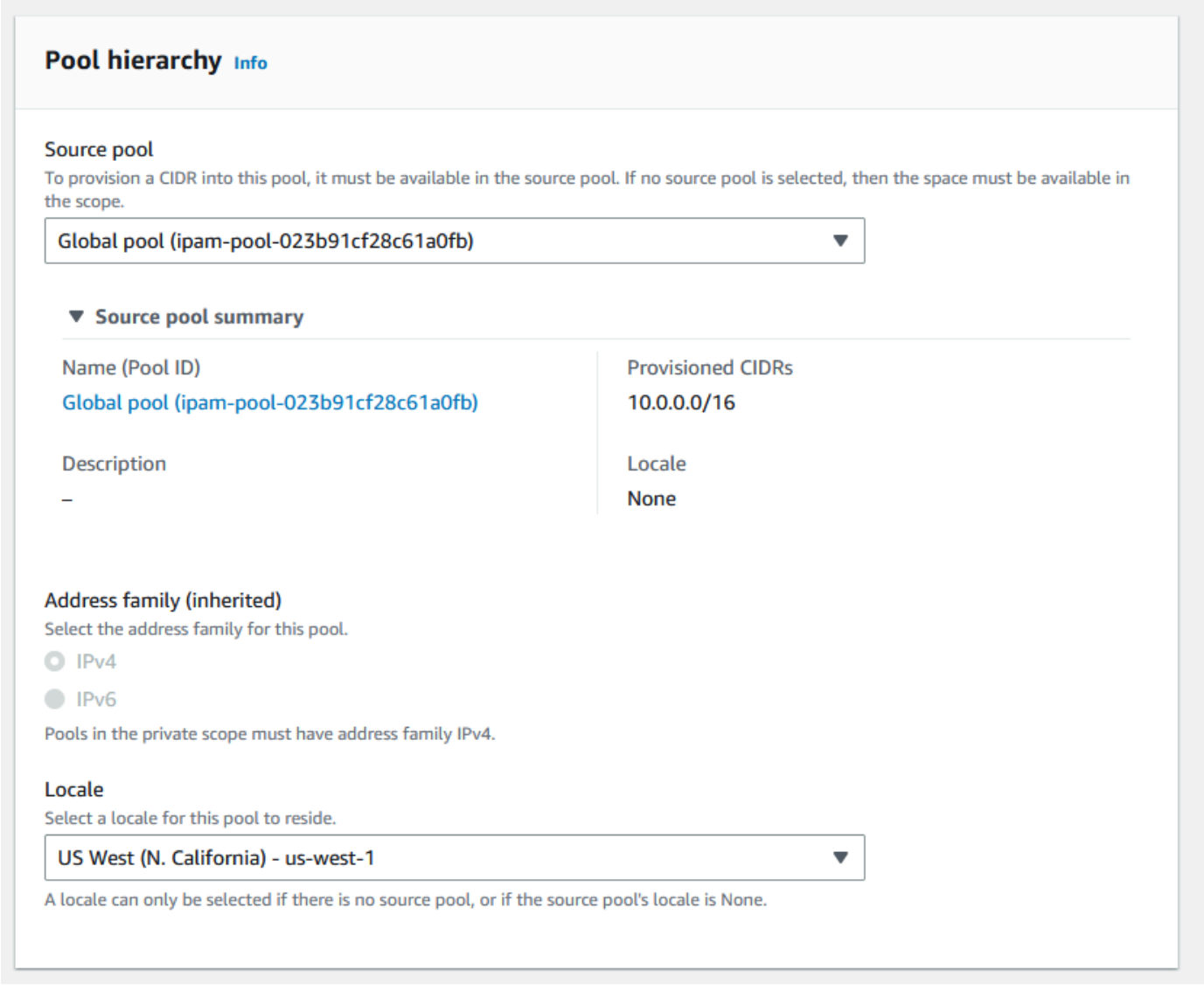
3. Seleccione el ámbito privado.



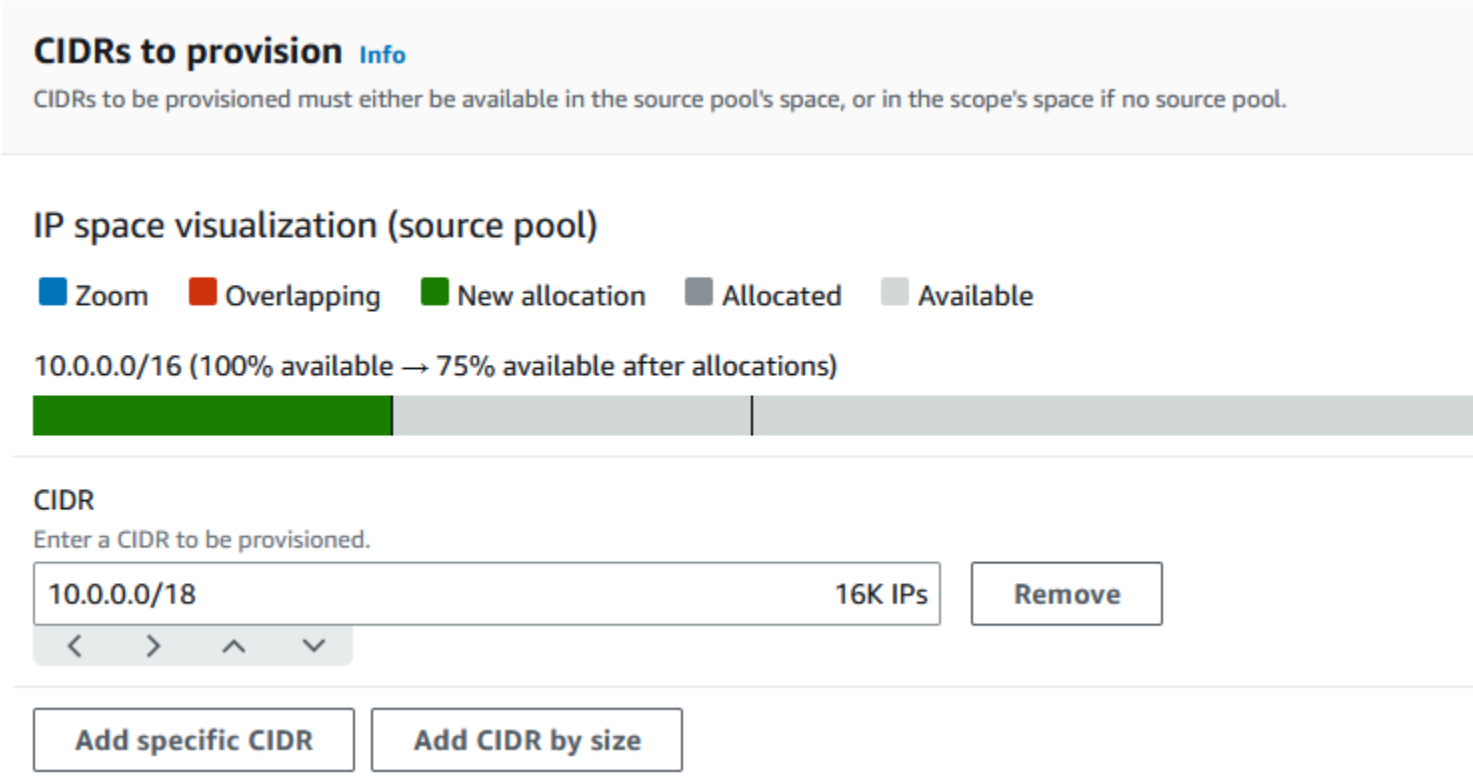
4. Elija Create pool (Crear grupo).
5. En Álcance de IPAM, deje seleccionado el alcance privado.
6. (Opcional) Añada una etiqueta de nombre y una descripción para el grupo, como Grupo regional us-west-1.



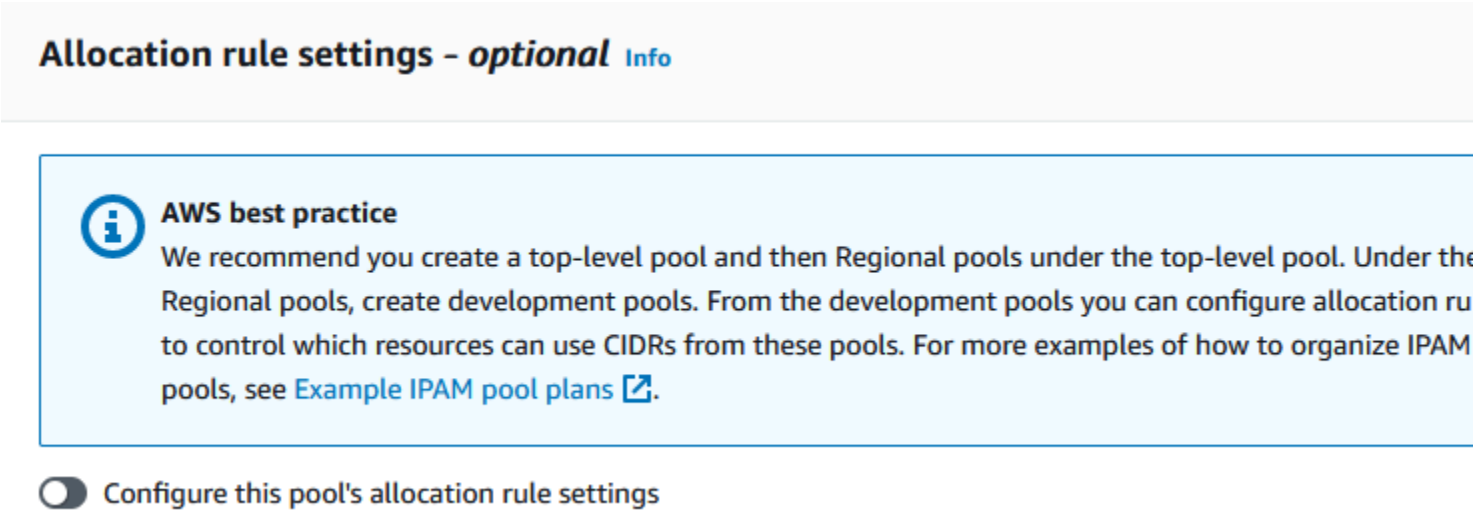
7. En Origen, seleccione Grupo de IPAM y seleccione el grupo de nivel superior (“Grupo global”) que creó en Paso 3: Cree un grupo de IPAM de nivel superior. A continuación, en Configuración regional, elija us-west-1.



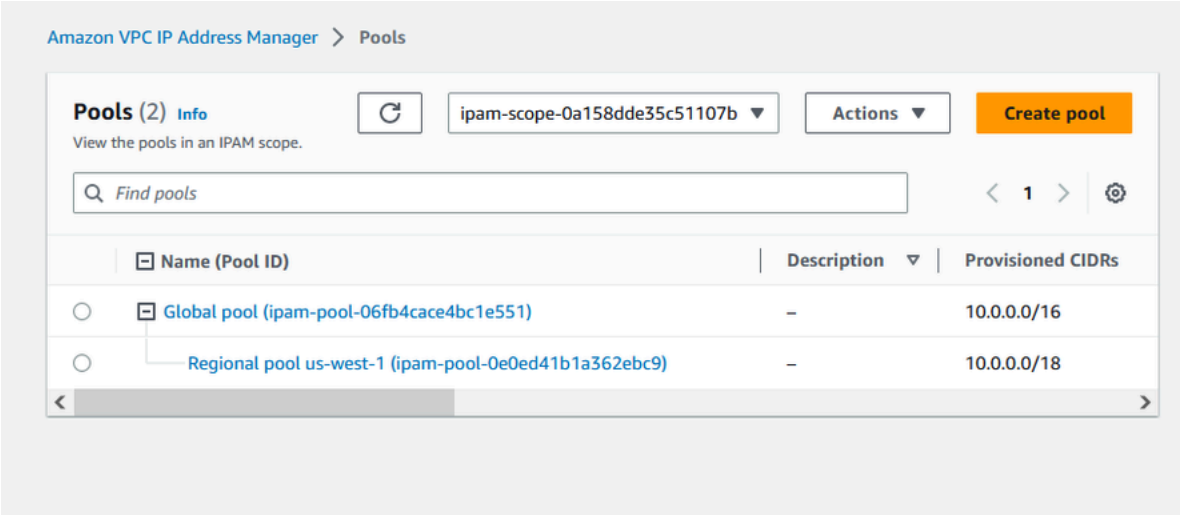
8. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
9. En CIDR a aprovisionar, introduzca 10,0.0.0/18, lo que proporcionará a este grupo unas 16 000 direcciones IP disponibles.



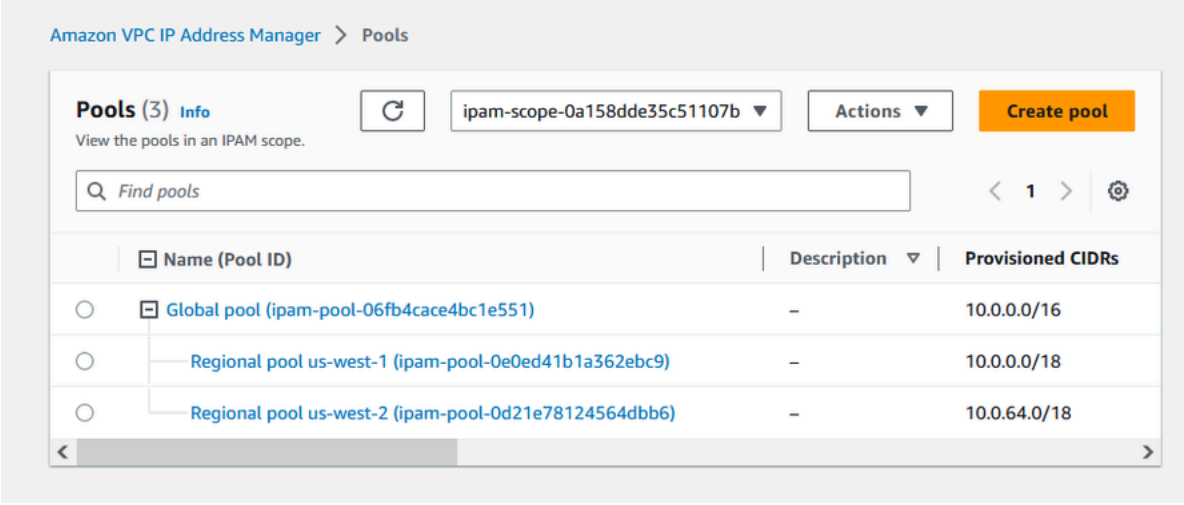
10. Deje deshabilitada la opción Configuración de las reglas de asignación de este grupo. No asignará ningún CIDR a las VPC directamente desde este grupo. En su lugar, los asignará desde un grupo secundario que creará a partir de este grupo.



11. Elija Create pool (Crear grupo).
12. Vuelva a la vista Grupos para ver la jerarquía de los grupos de IPAM que ha creado.



13. Repita los pasos de esta sección y cree un segundo grupo regional en la configuración regional de us-west-2 con el CIDR 10,0.64.0/18 asignado. Cuando complete ese proceso, tendrá tres grupos en una jerarquía similar a esta:

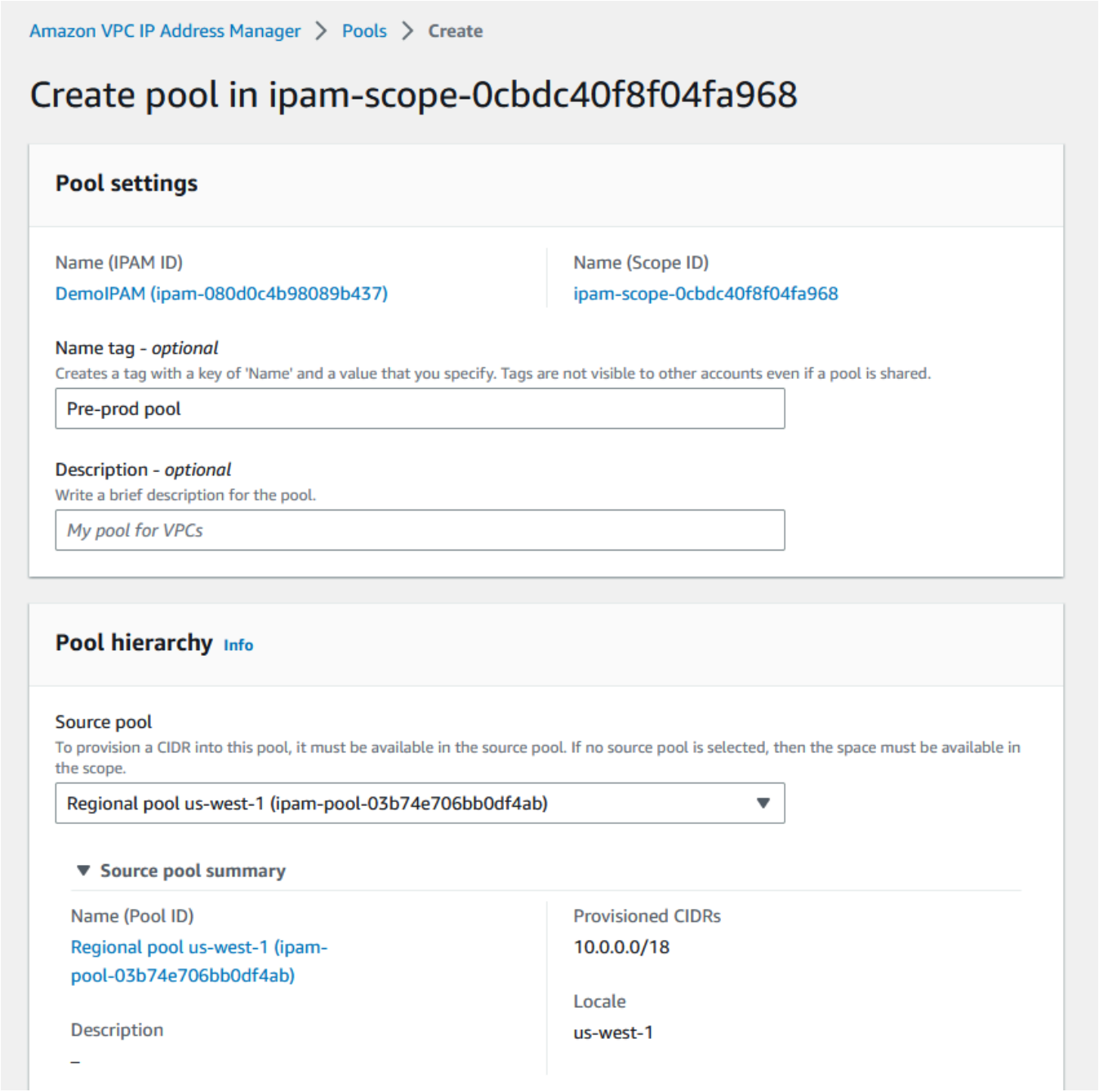


Paso 5: Cree un grupo de desarrollo para preproducción

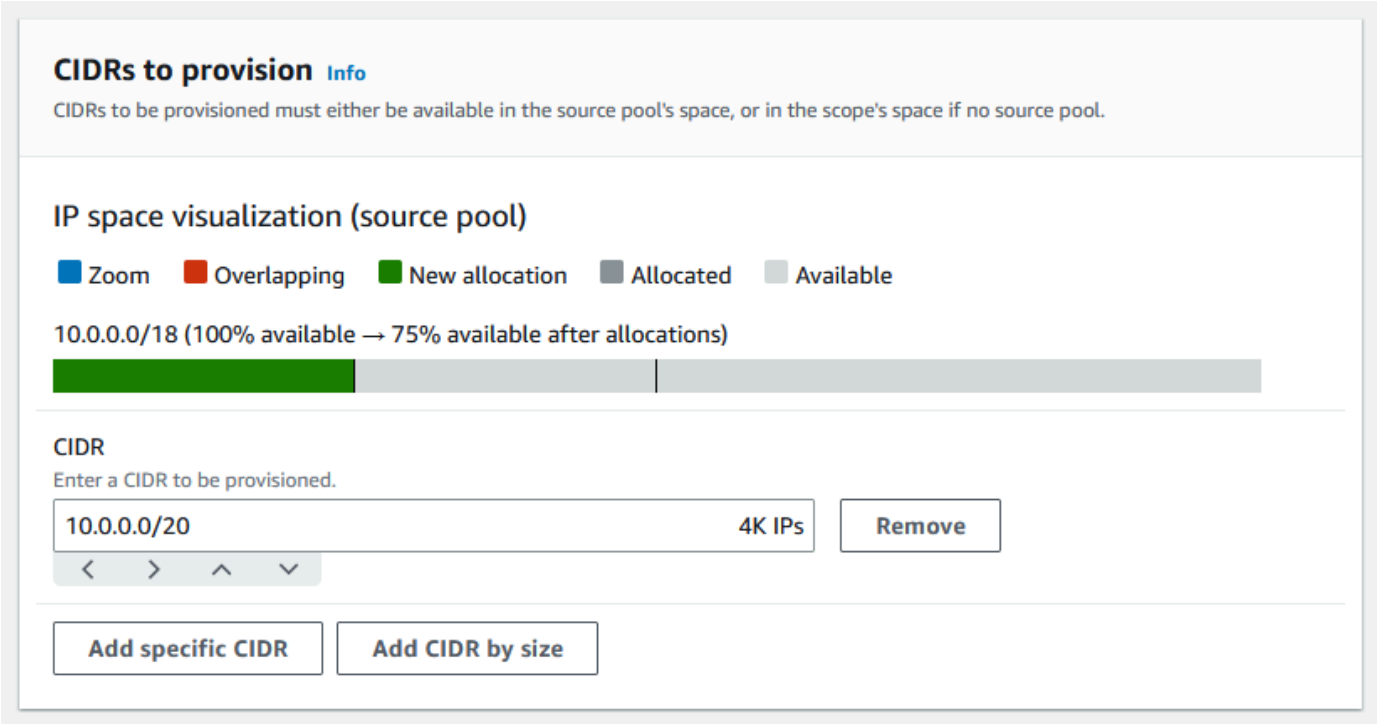
Siga los pasos de esta sección para crear un grupo de desarrollo para recursos de preproducción dentro de uno de sus grupos regionales.

Crear un grupo de desarrollo para preproducción

1. De la misma manera que en la sección anterior, usando la cuenta de administrador de IPAM, cree un grupo llamado Grupo de preproducción, pero esta vez use el Grupo regional us-west-1 como grupo de origen.

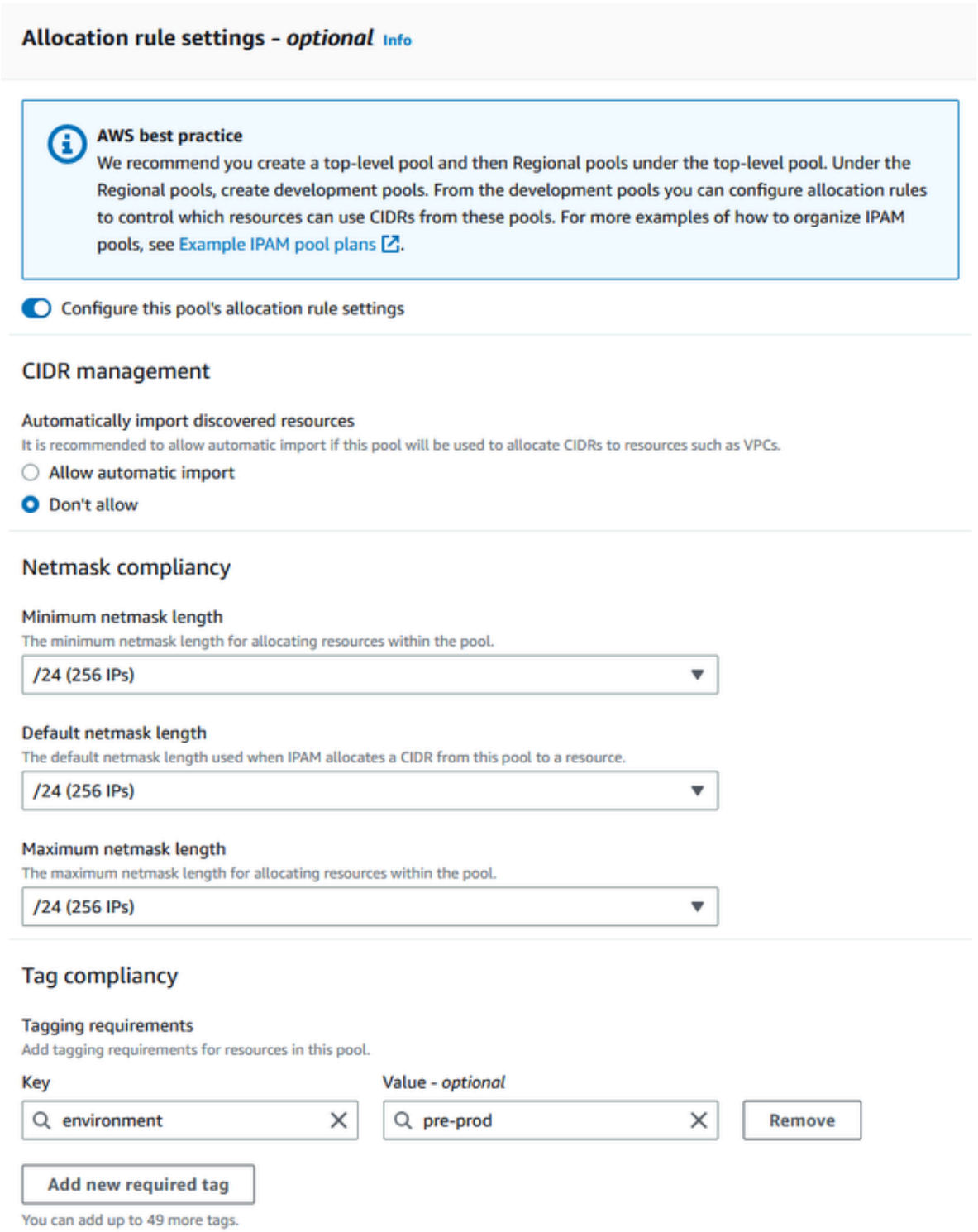


2. Especifique un CIDR de 10.0.0.0/20 para aprovisionar, lo que dará a este grupo unas 4000 direcciones IP.

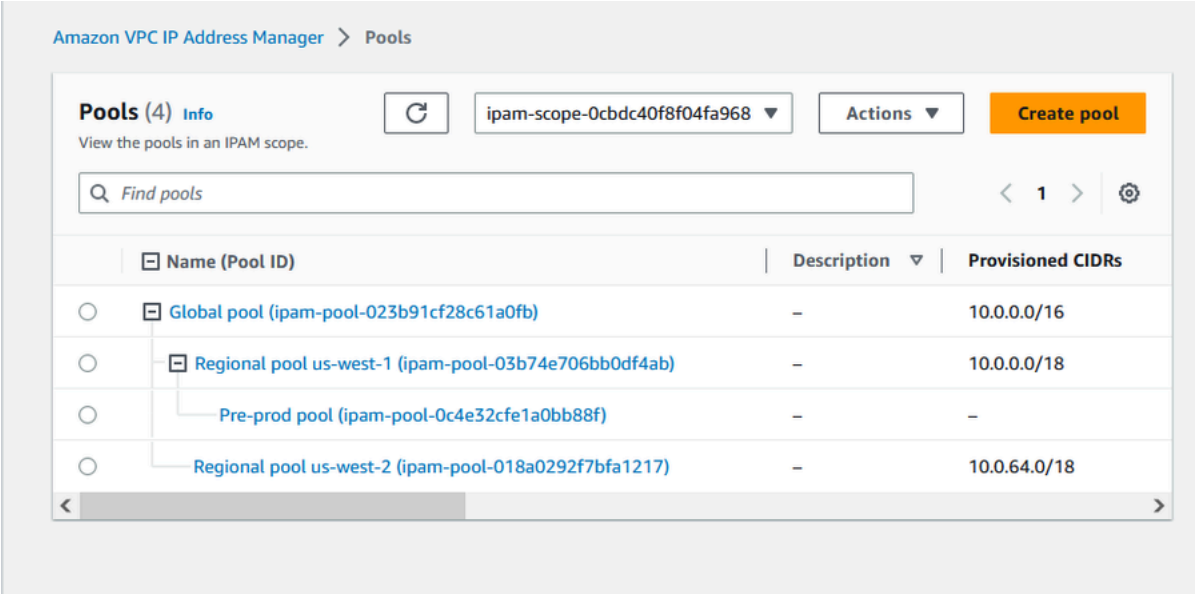


3. Habilite la opción Configurar los ajustes de las reglas de asignación de este grupo. Haga lo siguiente:

   1. En Administración de CIDR, en Importar automáticamente los recursos localizados, deje seleccionada la opción predeterminada No permitir. Esta opción permite a IPAM importar automáticamente los CIDR de recursos que identifica en la configuración regional del grupo. Una descripción detallada de esta opción está fuera del marco de este tutorial, pero puede leer más sobre ella en Creación de un grupo IPv4 de nivel superior.
   2. En Conformidad con la máscara de red, elija /24 como longitud mínima, predeterminada y máxima de la máscara de red. Una descripción detallada de esta opción está fuera del marco de este tutorial, pero puede leer más sobre ella en Creación de un grupo IPv4 de nivel superior. Es importante tener en cuenta que la VPC que cree más tarde con un CIDR de este grupo se limitará a /24 en función de lo que hayamos establecido aquí.
   3. En Conformidad de la etiqueta, introduzca entorno/preproducción. Esta etiqueta será necesaria para que las VPC asignen espacio del grupo. Más adelante veremos cómo funciona.



4. Elija Create pool (Crear grupo).
5. La jerarquía de grupos incluye ahora un grupo secundario adicional bajo el Grupo regional us-west-1:



Ahora ya puede compartir el grupo de IPAM con otra cuenta de miembro en su organización y habilitarla a fin de que asigne un CIDR del grupo y crear una VPC.

Paso 6: Comparta el grupo de IPAM

Siga los pasos de esta sección para compartir el grupo de IPAM de preproducción utilizando AWS Resource Access Manager (RAM).

Esta sección se compone de dos subsecciones:

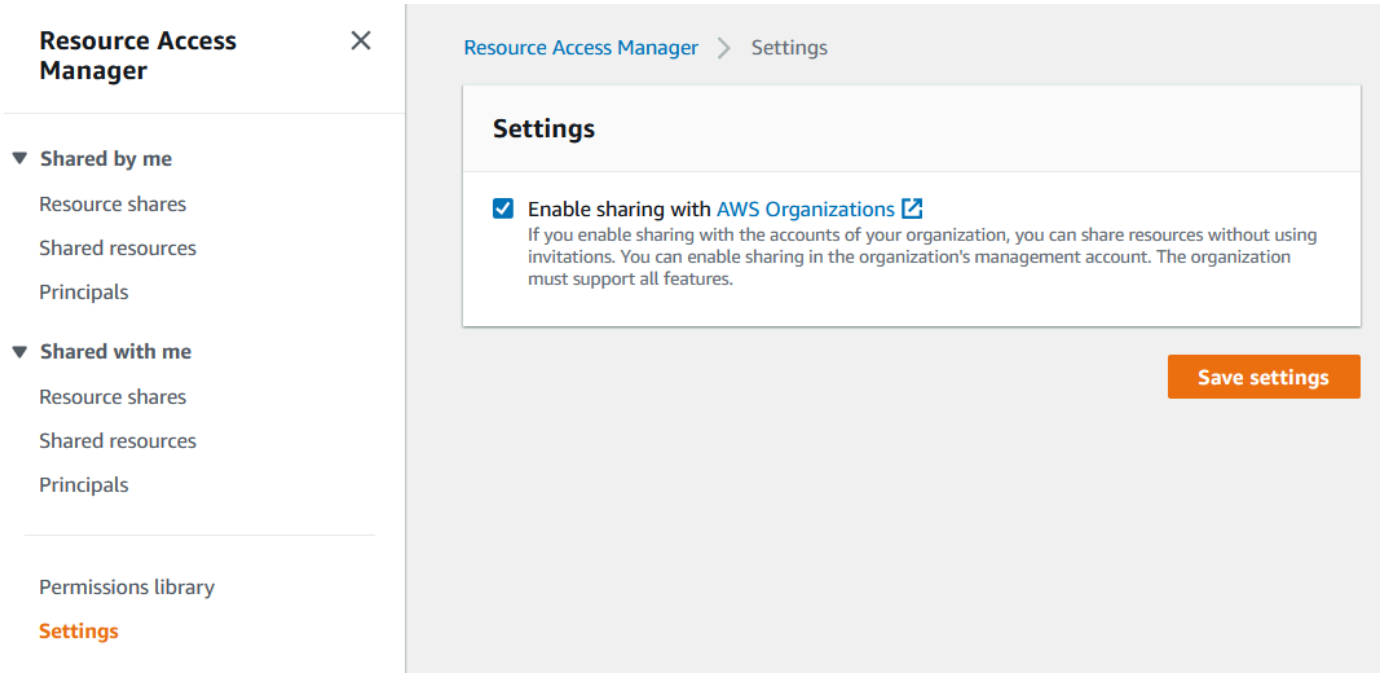
- Paso 6.1. Habilitar el uso compartido de recursos en AWS RAM: La cuenta de administración AWS Organizations debe realizar este paso.
- Paso 6.2. Compartir un grupo de IPAM mediante AWS RAM: El administrador de IPAM debe realizar este paso.

Paso 6.1. Habilitar el uso compartido de recursos en AWS RAM

Después de crear su IPAM, podrá compartir grupos de direcciones IP con otras cuentas de su organización. Antes de compartir un grupo de IPAM, complete los pasos de esta sección para habilitar el uso compartido de recursos con AWS RAM.

Habilitar el uso compartido de recursos

1. Utilizando la cuenta de administración AWS Organizations, abra la consola AWS RAM en https://console.aws.amazon.com/ram/.
2. En el panel de navegación izquierdo, seleccione Configuración, seleccione Habilitar uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.



Ahora puede compartir un grupo de IPAM con otros miembros de la organización.

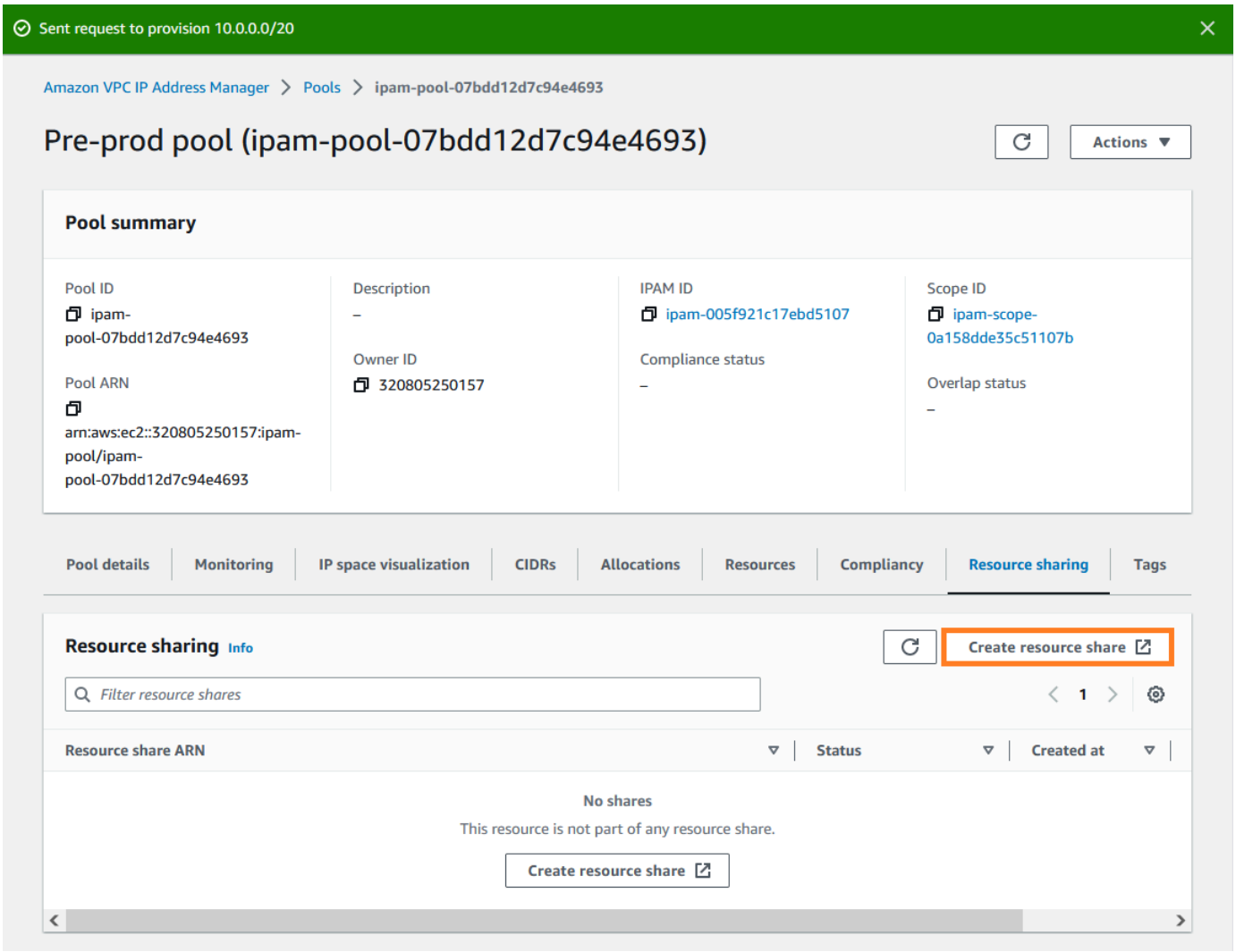
Paso 6.2. Compartir un grupo de IPAM mediante AWS RAM

En esta sección compartirá el grupo de desarrollo de preproducción con otra cuenta de miembro de AWS Organizations. Para instrucciones completas sobre cómo compartir grupos de IPAM, incluyendo información sobre los permisos de IAM requeridos, consulte Compartir un grupo de IPAM mediante AWS RAM.

Compartir un grupo de IPAM mediante AWS RAM

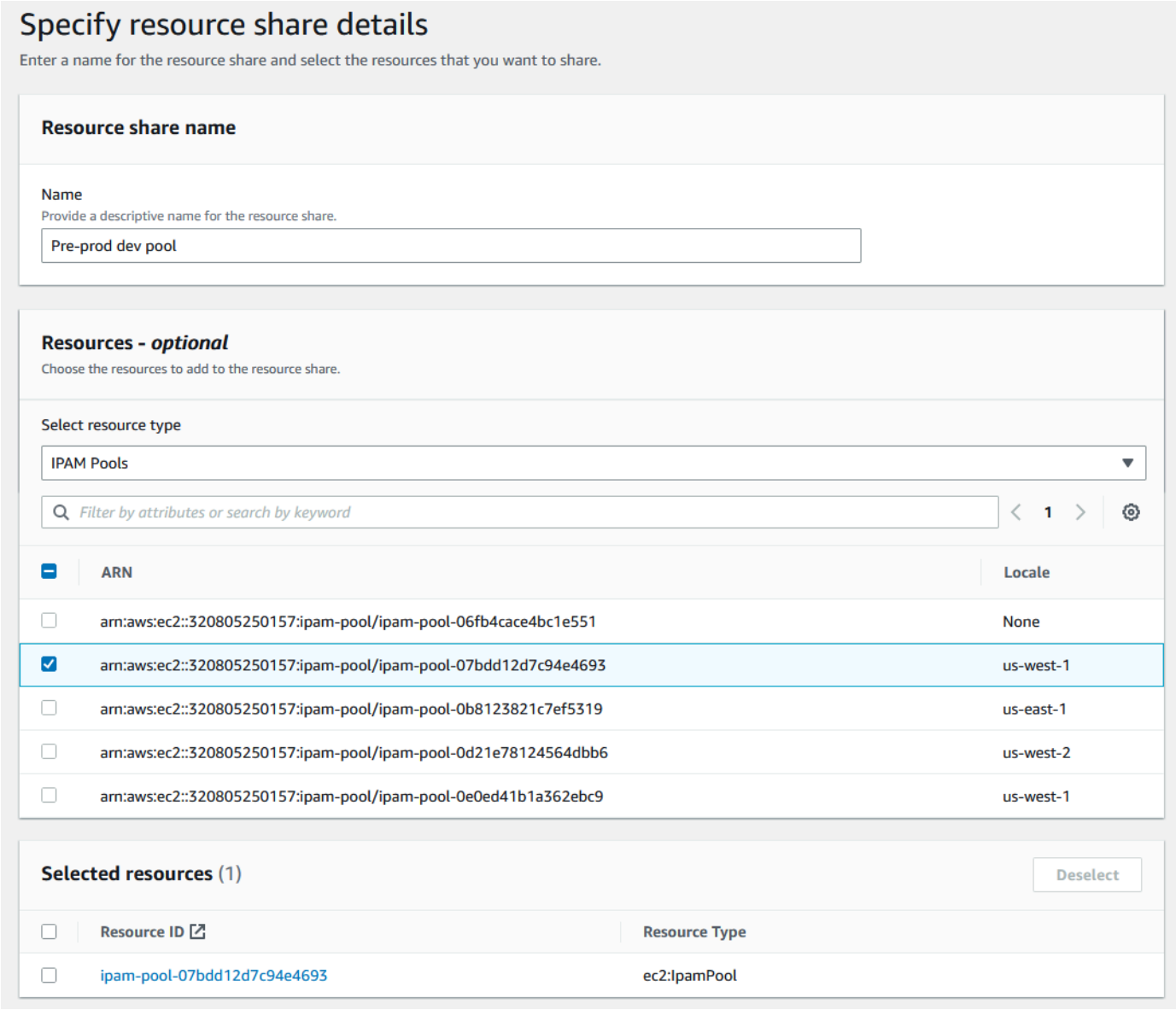
1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado, elija el grupo de IPAM de preproducción y seleccione Acciones > Ver detalles.

4. En Resource sharing (Uso compartido de recursos), elija Create resource share (Crear recursos compartidos). Se abrirá la consola de AWS RAM. Se compartirá el grupo utilizando AWS RAM.
5. Elija Create a resource share (Crear un recurso compartido).

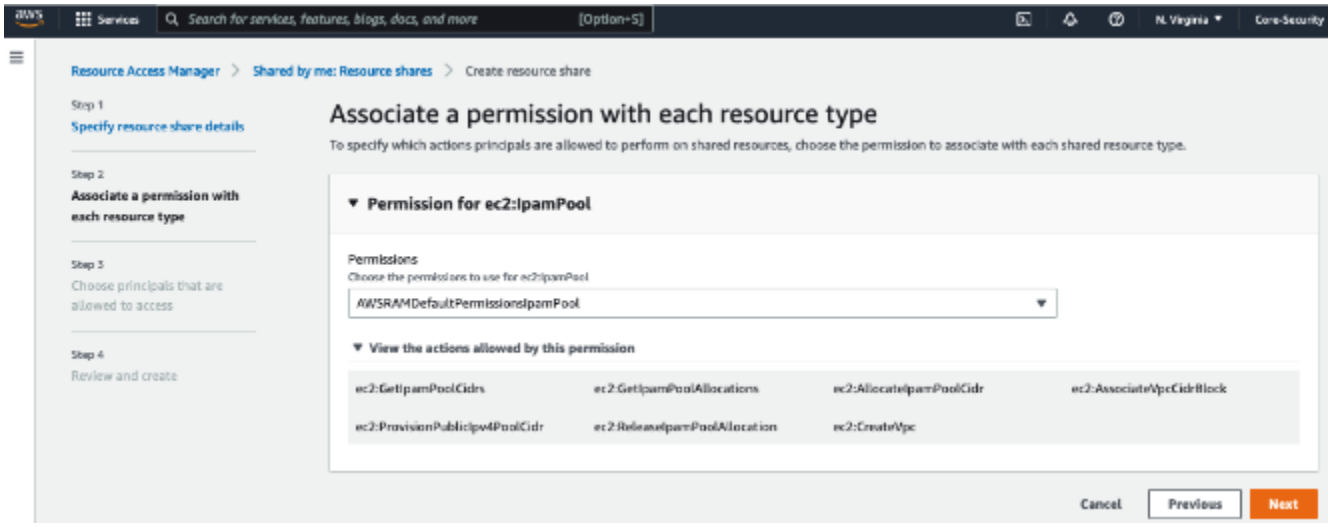


Se abrirá la consola de AWS RAM.

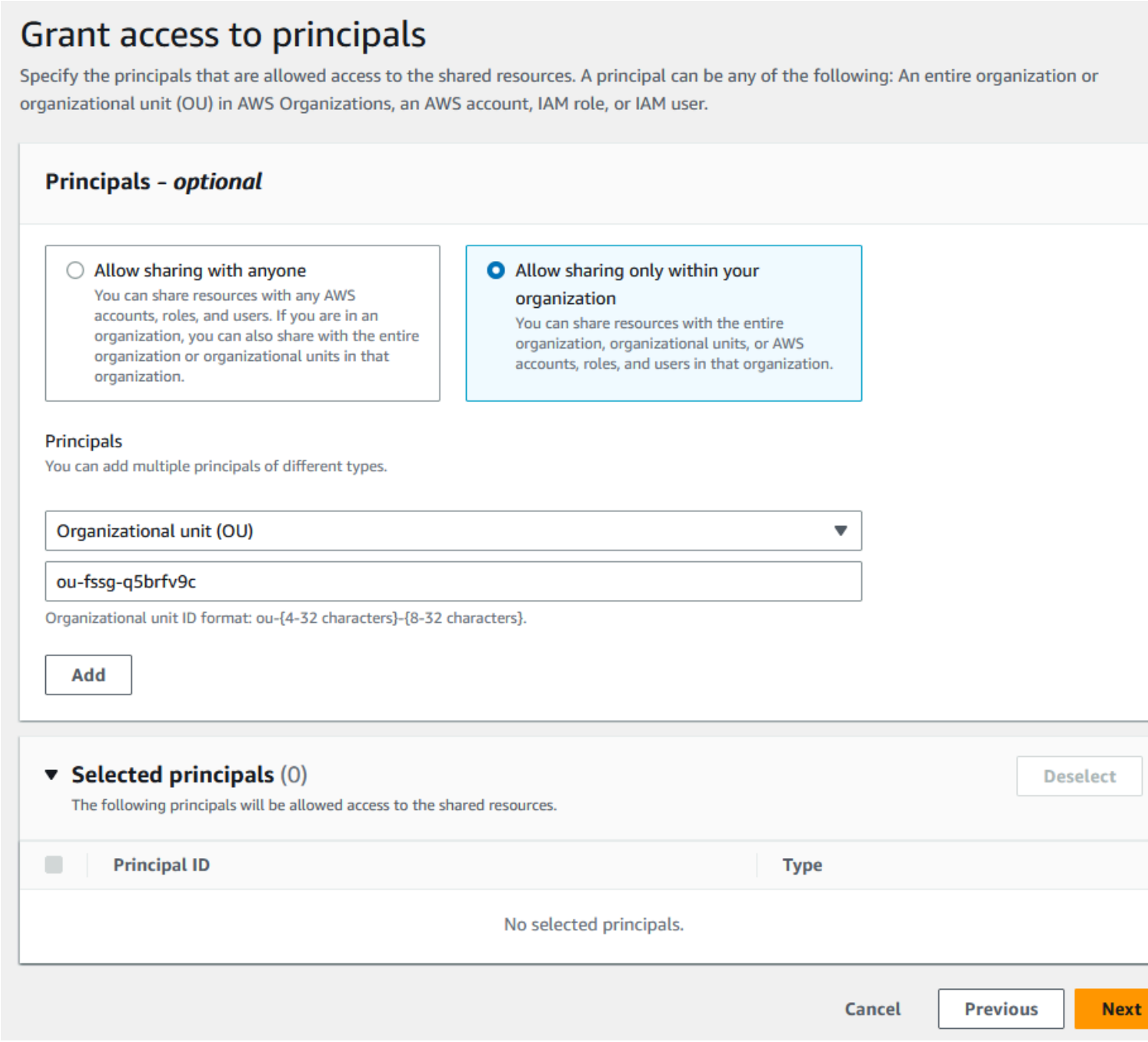
6. En la consola AWS RAM, seleccione de nuevo Crear un recurso compartido.
7. Añada un Nombre para el grupo compartido.
8. En Seleccionar tipo de recurso, elija Grupos de IPAM y, a continuación, seleccione el ARN del grupo de desarrollo de preproducción.



9. Elija Siguiente.
10. Deje seleccionado el permiso predeterminado AWSRAMDefaultPermissionsIpamPool. Los detalles de las opciones de permiso están fuera del marco de este tutorial, pero puede encontrar más información sobre estas opciones en Compartir un grupo de IPAM mediante AWS RAM.



11. Elija Siguiente.
12. En Entidades principales, seleccione Permitir compartir solo dentro de la organización. Introduzca el ID de unidad de su organización AWS Organizations (como se menciona en Cómo AWS Organizations se integra con IPAM) y luego seleccione Añadir.



13. Elija Siguiente.
14. Revise las opciones de recurso compartido y las entidades principales con las que se compartirá y seleccione Crear.

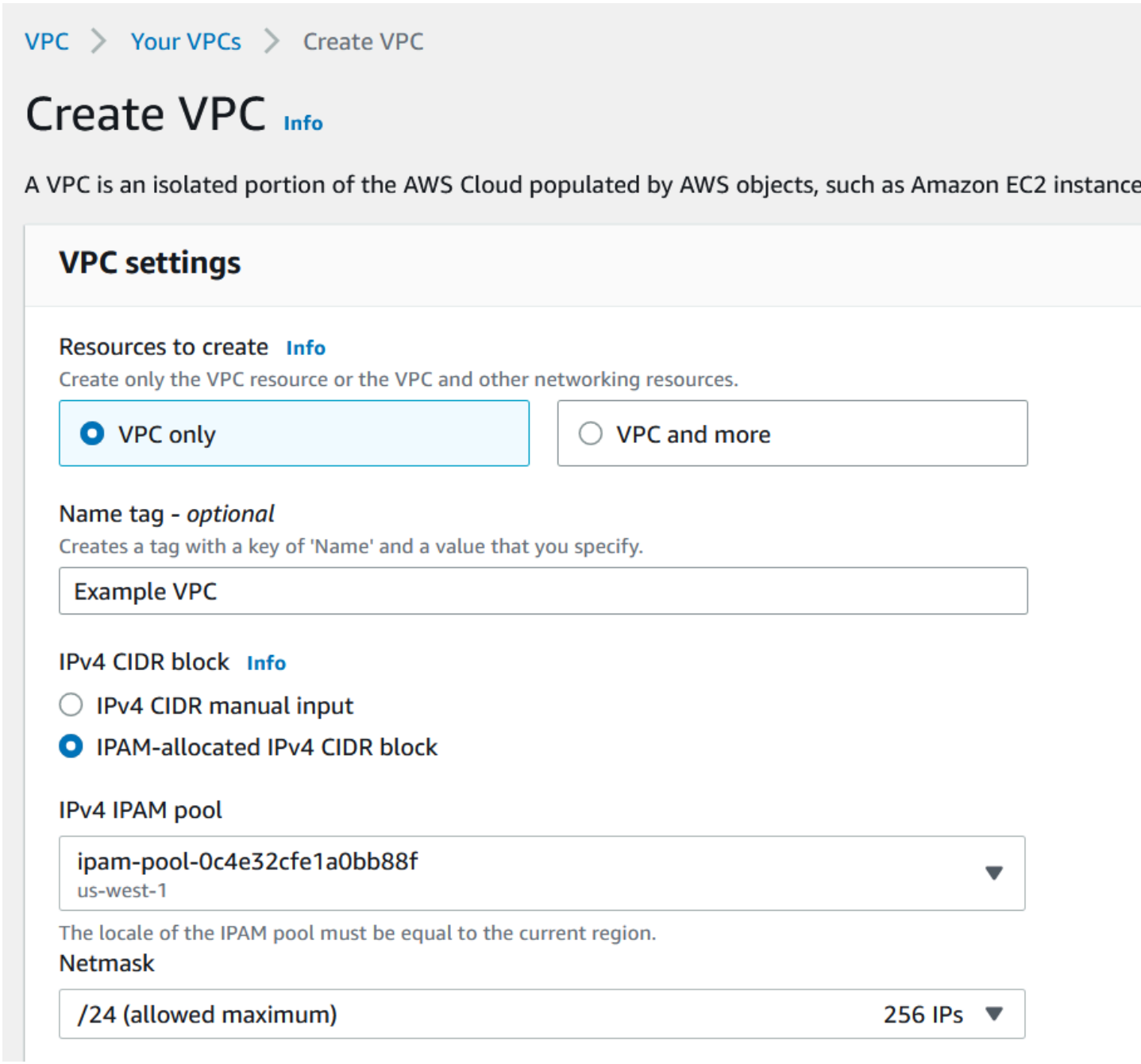
Ahora que se ha compartido el grupo, vaya al siguiente paso para crear una VPC con un CIDR asignado desde un grupo de IPAM.

Paso 7: Cree una VPC con un CIDR asignado desde un grupo de IPAM

Siga los pasos de esta sección para crear una VPC con un CIDR asignado del grupo de preproducción. Este paso debe completarse con la cuenta miembro en la OU con la que se compartió el grupo de IPAM en la sección anterior (llamada example-member-account-2 en Cómo AWS Organizations se integra con IPAM). Para más información sobre los permisos de IAM necesarios para crear VPC, consulte Ejemplos de políticas de Amazon VPC en la Guía del usuario de Amazon VPC.

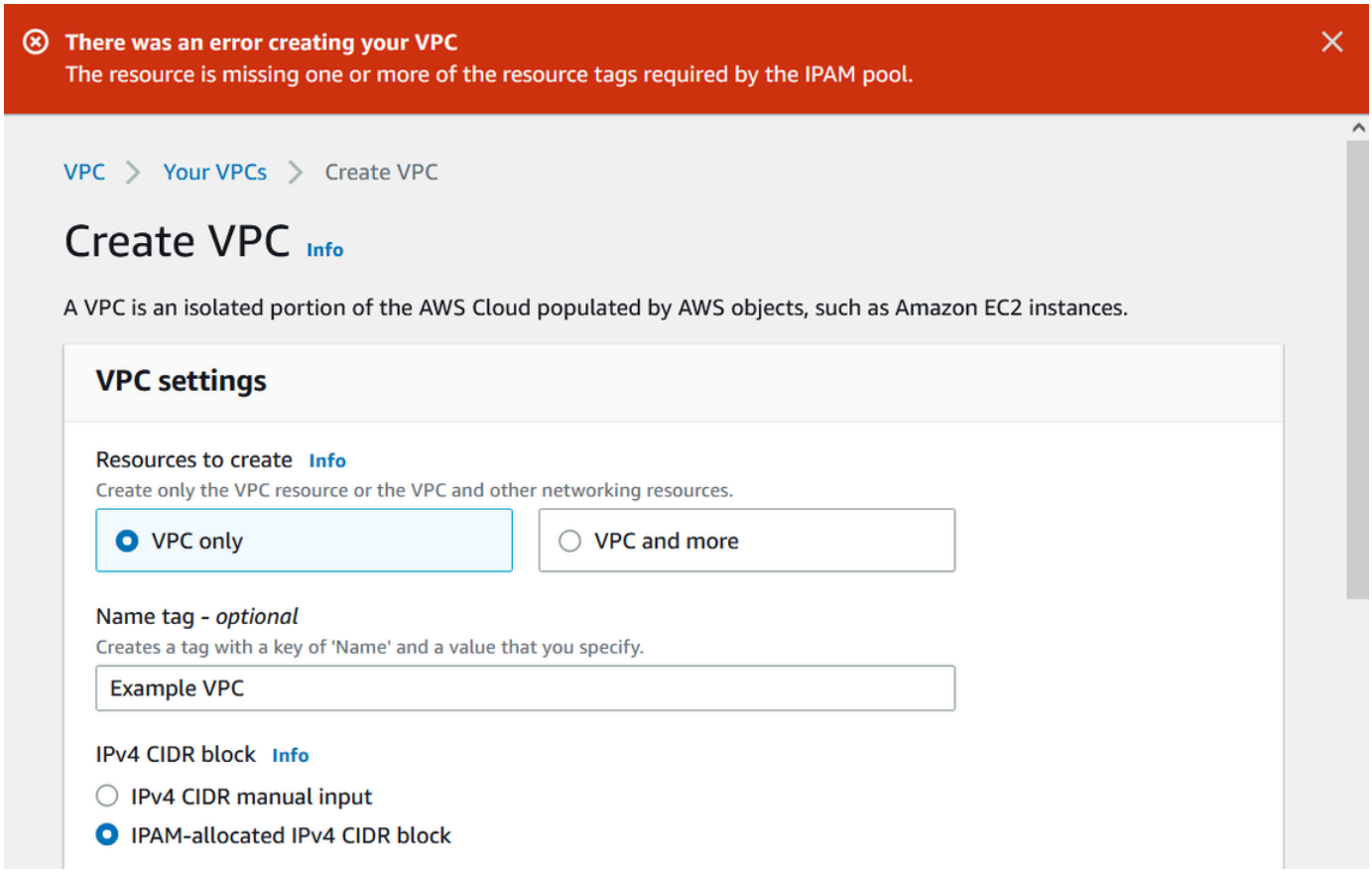
Crear una VPC con un CIDR asignado desde un grupo de IPAM

1. Abra la consola de la VPC en https://console.aws.amazon.com/vpc/ con la cuenta de miembro que utilizará como cuenta de desarrollador.
2. Seleccione Creación de VPC.
3. Haga lo siguiente:
    1. Introduzca un nombre, como VPC de ejemplo.
    2. Elija el bloque de CIDR IPv4 asignado por IPAM.
    3. En el grupo IPv4 de IPAM, seleccione el ID del grupo de preproducción.
    4. Elija una longitud de máscara de red. Como ha limitado la longitud de máscara de red disponible para este grupo a /24 (en Paso 5: Cree un grupo de desarrollo para preproducción), la única opción de máscara de red disponible es /24.

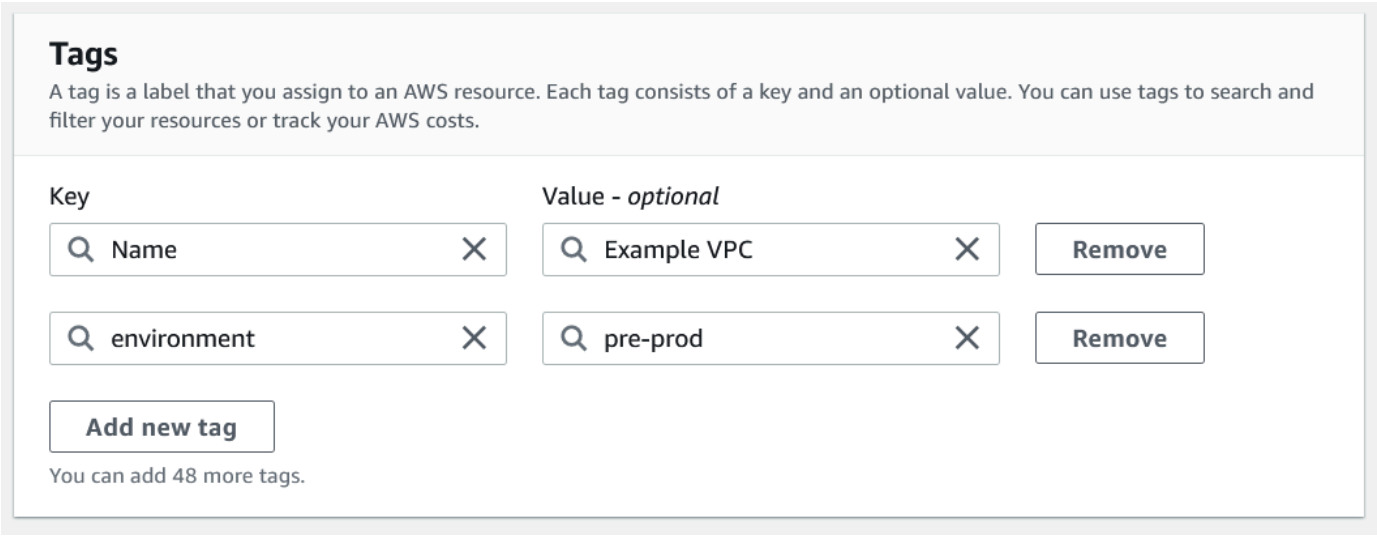


4. Para fines de demostración, en Etiquetas, no añada ninguna etiqueta adicional en este momento. Cuando creó el grupo de preproducción (en Paso 5: Cree un grupo de desarrollo para preproducción), agregó una regla de asignación que requería que cualquier VPC del grupo que se creara con CIDR tuviera la etiqueta entorno/preproducción. Deje la etiqueta entorno/preproducción desactivada por ahora para que pueda ver que aparece un error que le indica que no se ha añadido la etiqueta necesaria.
5. Seleccione Creación de VPC.

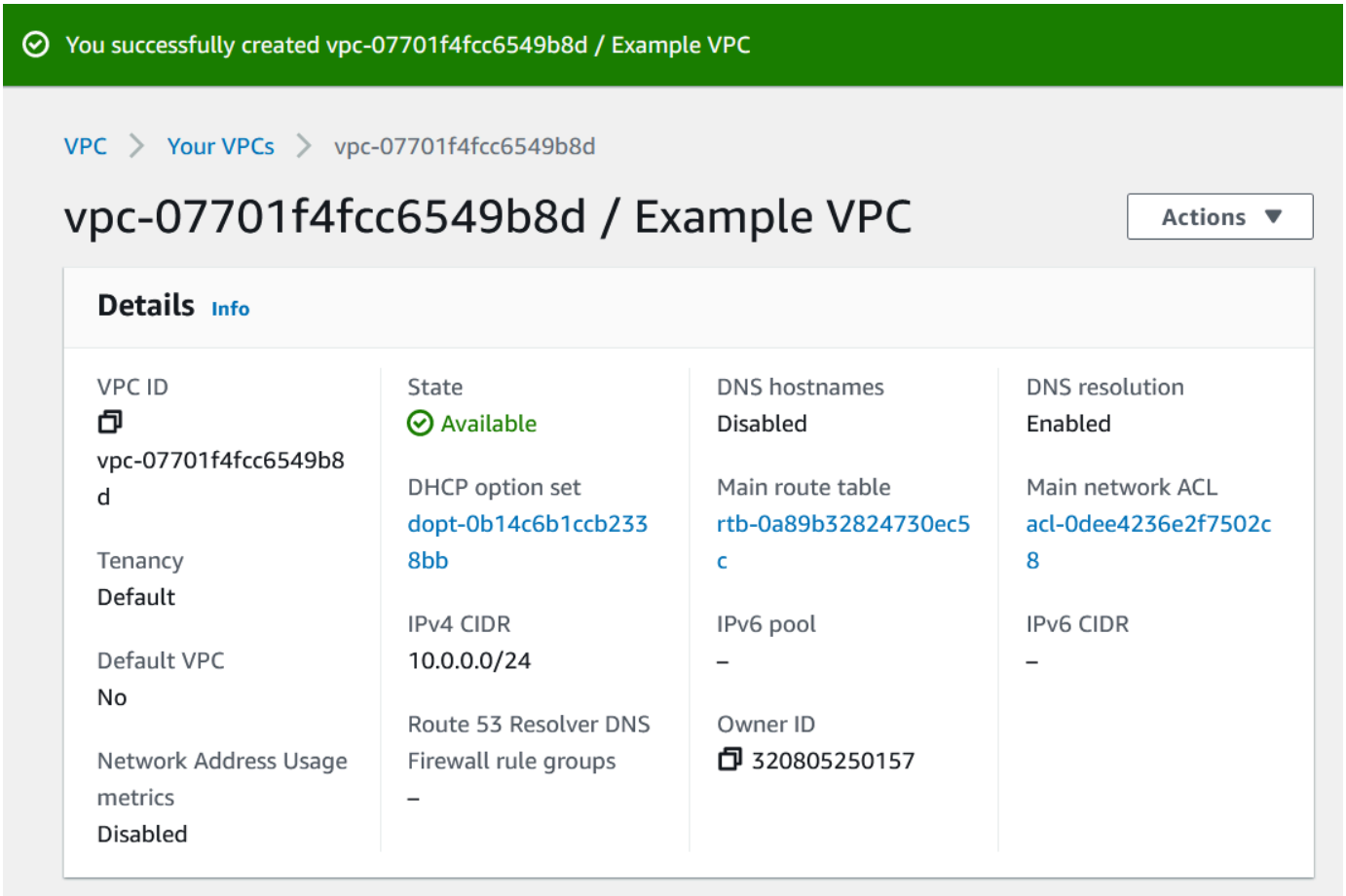
6. Aparece un error que le indica que no se ha añadido una etiqueta obligatoria. El error aparece porque ha establecido una regla de asignación al crear el grupo de preproducción (en Paso 5: Cree un grupo de desarrollo para preproducción). La regla de asignación requería que cualquier VPC creada con CIDR de este grupo tuviera una etiqueta de entorno/preproducción.



7. Ahora, en Etiquetas, añada la etiqueta entorno/preproducción y vuelva a seleccionar Crear VPC.



8. La VPC se crea correctamente y cumple con la regla de etiquetas en el grupo de preproducción:



En el panel Recursos de la consola de IPAM, el administrador de IPAM podrá ver y administrar la VPC y el CIDR asignado. Tenga en cuenta que la VPC tarda algún tiempo en aparecer en el panel Recursos.

Paso 8: Eliminar

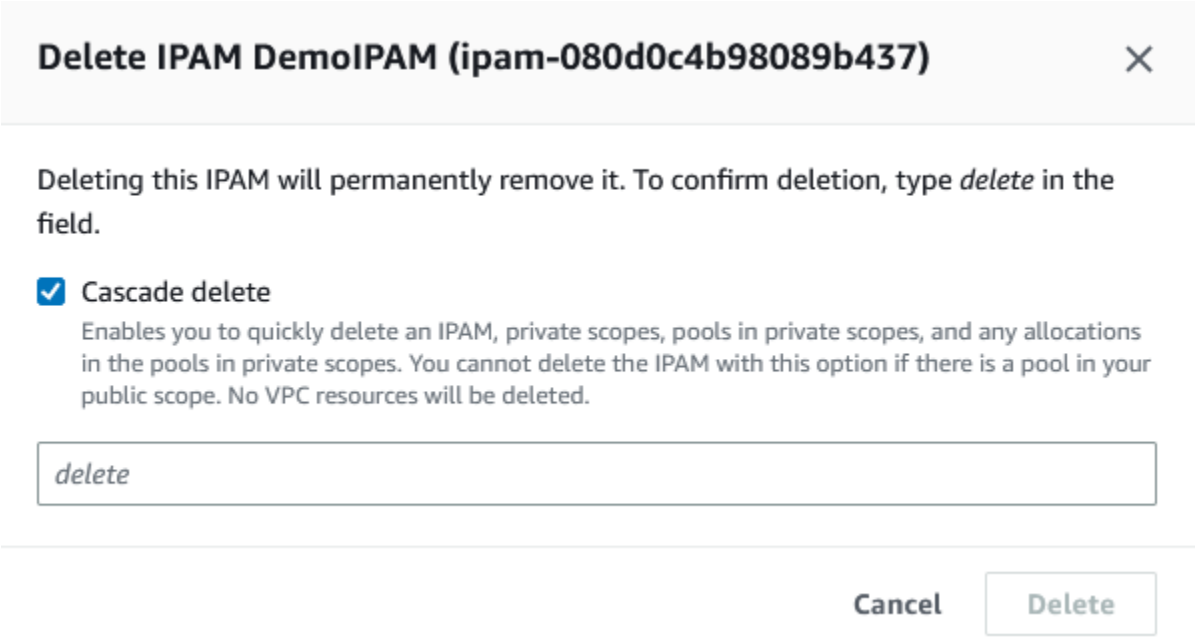
En este tutorial, ha creado un IPAM con un administrador delegado, ha creado múltiples grupos y ha habilitado una cuenta de miembro en su organización para asignar un CIDR de VPC desde un grupo.

Siga los pasos de esta sección para eliminar los recursos que ha creado en este tutorial.

Para eliminar los recursos que se han creado en este tutorial

1. Utilizando la cuenta de miembro que ha creado esta VPC de ejemplo, elimine la VPC. Para instrucciones detalladas, consulte Eliminar su VPC en la Guía del usuario de Amazon Virtual Private Cloud.

2. Utilizando la cuenta de administrador de IPAM, elimine el recurso compartido de ejemplo en la consola AWS RAM. Para instrucciones detalladas, consulte Eliminar un recurso compartido en AWSAWS RAM en la Guía del usuario de AWS Resource Access Manager.
3. Utilizando la cuenta de administrador de IPAM, inicie sesión en la consola RAM y desactive la compartición con AWS Organizations que habilitó en Paso 6.1. Habilitar el uso compartido de recursos en AWS RAM.
4. Utilizando la cuenta de administrador de IPAM, elimine el IPAM de ejemplo seleccionándolo en la consola de IPAM y eligiendo Acciones > Eliminar. Para obtener instrucciones detalladas, consulte Eliminar un IPAM.
5. Cuando aparezca la opción de borrar el IPAM, elija Borrar en cascada. Esto borrará todos los entornos y grupos dentro del IPAM antes de borrar el IPAM.



6. Escriba delete y haga clic en Eliminar.
7. Utilizando la cuenta de administrador AWS Organizations, inicie sesión en la consola de IPAM, seleccione Configuración y elimine la cuenta de administrador delegado.
8. (Opcional) Cuando se integra IPAM con AWS Organizations, IPAM crea automáticamente un rol vinculado al servicio en cada cuenta de miembro. Utilizando cada una de las cuentas de miembro de AWS Organizations, inicie sesión en IAM y elimine el rol vinculado al servicio AWSServiceRoleForIPAM en todas las cuentas de miembro.
9. Ha completado la limpieza.

Tutorial: cree un IPAM y grupos utilizando el AWS CLI

Siga los pasos de este tutorial para crear un IPAM con AWS CLI, crear grupos de direcciones IP y asignar una VPC con un CIDR desde un grupo de IPAM.

A continuación, se muestra un ejemplo de jerarquía de la estructura de grupos que creará al seguir los pasos de esta sección:

- IPAM que opera en la región de AWS 1 y la región de AWS 2
  - Alcance privado
    - Grupo de nivel superior
      - Grupo regional en la región 2 de AWS
        - Grupo de desarrollo
          - Asignación para una VPC

> **Note**
>
> En esta sección, creará un IPAM. De forma predeterminada, solo puede crear un IPAM. Para obtener más información, consulte Cuotas de IPAM. Si ya ha delegado una cuenta de IPAM y ha creado un IPAM, puede omitir los pasos 1 y 2.

Contenido

Paso 1: Habilitar IPAM en su organización

Este paso es opcional. Complete este paso para habilitar IPAM en su organización y configurar el IPAM delegado mediante AWS CLI. Para obtener más información sobre el rol de la cuenta de IPAM, consulte Integración de IPAM con cuentas en una organización de AWS.

Se debe realizar esta solicitud desde una cuenta de administración de AWS Organizations. Cuando ejecute el siguiente comando, asegúrese de que se encuentra utilizando un rol con una política de IAM que permita las siguientes acciones:

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

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

Debe ver el siguiente resultado, lo que indica que la habilitación se ha realizado correctamente.

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

Paso 2: Crear un IPAM

Siga los pasos de esta sección para crear un IPAM y conocer más información sobre los alcances que se crean. Utilizará este IPAM cuando cree grupos y aprovisione rangos de direcciones IP para esos grupos en pasos posteriores.

> **Note**
>
> La opción de regiones operativas determina para qué regiones de AWS se pueden utilizar los grupos de IPAM. Para obtener más información sobre las regiones operativas, consulte Creación de un IPAM.

Para crear un IPAM mediante la AWS CLI

1. Ejecute el siguiente comando para crear la instancia de IPAM.

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

   Al crear un IPAM, AWS realiza lo siguiente de forma automática:

   - Devuelve un ID de recurso único a nivel global (`IpamId`) para el IPAM.
   - Crea un alcance público predeterminado (`PublicDefaultScopeId`) y un alcance privado predeterminado (`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. Ejecute el siguiente comando para conocer más información relacionada con los alcances. El alcance público está destinado a direcciones IP a las que se accederá a través de Internet pública. El alcance privado está destinado a direcciones IP a las que no se accederá a través de Internet pública.

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

En la salida, verá los alcances que se encuentran disponibles. Utilizará el ID de alcance privado en el siguiente paso.

```
{
    "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
        }
    ]
}
```

Paso 3: Crear un grupo de direcciones IPv4

Siga los pasos de esta sección para crear un grupo de direcciones IPv4.

Important

No usará la opción `--locale` en este grupo de nivel superior. Establecerá la opción de configuración regional más adelante en el grupo regional. La configuración regional es la región de AWS en la que desea que un grupo esté disponible para asignaciones de CIDR.

Como resultado de no determinar la configuración regional en el grupo de nivel superior, la configuración regional se establecerá de forma predeterminada en `None`. Si un grupo tiene `None` como configuración regional, no estará disponible para los recursos de VPC en ninguna región de AWS. Solo puede asignar de manera manual el espacio de direcciones IP en el grupo para reservar espacio.

Para crear un grupo de direcciones IPv4 para todos los recursos de AWS con la AWS CLI

1. Ejecute el siguiente comando para crear un grupo de direcciones IPv4. Utilice el ID de alcance privado del IPAM que creó en el paso anterior.

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

   En la salida, verá un estado `create-in-progress` para el grupo.

```
{
    "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. Ejecute el siguiente comando hasta que vea el estado `create-complete` en la salida.

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

En la siguiente salida de ejemplo se muestra el estado correcto.

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

Paso 4: Aprovisionar un CIDR en el grupo de nivel superior

Siga los pasos de esta sección para aprovisionar un CIDR en el grupo de nivel superior y, a continuación, verificar que se aprovisiona el CIDR. Para obtener más información, consulte Aprovisionamiento de CIDR en un grupo.

Para aprovisionar un bloque de CIDR en el grupo mediante la AWS CLI

1. Ejecute el siguiente comando para aprovisionar el CIDR.

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

En la salida, puede verificar el estado del aprovisionamiento.

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

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

2. Ejecute el siguiente comando hasta que vea el estado `provisioned` en la salida.

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

En la siguiente salida de ejemplo se muestra el estado correcto.

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

Paso 5. Crear un grupo regional con el CIDR procedente del grupo de nivel superior

Cuando crea un grupo de IPAM, el grupo pertenece a la región de AWS del IPAM de forma predeterminada. Al crear una VPC, el grupo del que extrae la VPC debe encontrarse en la misma región que la VPC. Puede utilizar la opción `--locale` cuando cree un grupo a fin de que el grupo se encuentre disponible para los servicios de una región distinta de la región del IPAM. Siga los pasos de esta sección para crear un grupo regional en otra configuración regional.

Para crear un grupo con un CIDR procedente del grupo anterior mediante la AWS CLI

1. Ejecute el siguiente comando para crear el grupo e introducir espacio con un CIDR disponible conocido del grupo anterior.

```
aws ec2 create-ipam-pool --description "regional--pool" --region us-east-1 --ipam-
scope-id ipam-scope-065e7dfe880df679c --source-ipam-pool-id
ipam-pool-0008f25d7187a08d9 --locale us-west-2 --address-family ipv4
```

En la salida, verá el ID del grupo que creó. Necesitará este ID en el siguiente paso.

```
{
    "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. Ejecute el siguiente comando hasta que vea el estado `create-complete` en la salida.

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

En la salida, verá los grupos que tiene en el IPAM. En este tutorial, hemos creado un grupo de nivel superior y un grupo regional, así que verá ambos.

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

Paso 6: Aprovisionar un CIDR al grupo regional

Siga los pasos de esta sección para asignar un bloque de CIDR al grupo y validar que se ha aprovisionado correctamente.

Para asignar un bloque de CIDR al grupo regional mediante la AWS CLI

1. Ejecute el siguiente comando para aprovisionar el CIDR.

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

   En la salida, verá el estado del grupo.

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

2. Ejecute el siguiente comando hasta que vea el estado `provisioned` en la salida.

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

En la siguiente salida de ejemplo se muestra el estado correcto.

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

3. Ejecute el siguiente comando para consultar el grupo de nivel superior a fin de ver las asignaciones. El grupo regional se considera una asignación dentro del grupo de nivel superior.

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

En la salida, verá el grupo regional como una asignación en el grupo de nivel superior.

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

```
        }
    ]
}
```

Paso 7. Crear un recurso compartido de RAM para habilitar las asignaciones de IP en todas las cuentas

Este paso es opcional. Solo puede completar este paso si ha completado Integración de IPAM con cuentas en una organización de AWS.

Al crear un recurso compartido de AWS RAM de un grupo de IPAM, permite asignaciones de IP en todas las cuentas. El uso compartido de RAM solo se encuentra disponible en la región de AWS de origen. Tenga en cuenta que crea este recurso compartido en la misma región que el IPAM, no en la región local del grupo. Todas las operaciones administrativas de los recursos de IPAM se realizan a través de la región de origen del IPAM. En el ejemplo de este tutorial, se crea un único recurso compartido para un solo grupo, pero puede agregar varios grupos a un solo recurso compartido. Para obtener más información, incluida una explicación de las opciones que debe ingresar, consulte Compartir un grupo de IPAM mediante AWS RAM.

Ejecute los siguientes comandos para crear un recurso compartido:

```
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
```

La salida muestra que se ha creado el grupo.

```
{
    "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
    }
}
```

Paso 8. Creación de una VPC

Ejecute el siguiente comando para crear una VPC y asignar un bloque de CIDR a la VPC desde el grupo de IPAM que se creó recientemente.

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

La salida muestra que se ha creado la VPC.

```
{
    "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
    }
}
```

Paso 9. Eliminación

Siga los pasos de esta sección para eliminar los recursos de IPAM que ha creado en este tutorial.

1. Elimine la VPC.

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

2. Elimine el recurso compartido de RAM del grupo de IPAM.

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

3. Desaprovisione el CIDR de grupo del grupo regional.

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

4. Desaprovisione el CIDR de grupo del grupo de nivel superior.

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

5. Eliminar el IPAM

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

Tutorial: View IP address history using the AWS CLI

Los escenarios de esta sección le indican cómo analizar y auditar el uso de la dirección IP a través de la AWS CLI. Para obtener información general sobre el uso de la AWS CLI, consulte Uso de la AWS CLI en la Guía del usuario de AWS Command Line Interface.

Contenido

Descripción general

IPAM retiene de forma automática los datos del monitoreo de direcciones IP durante un máximo de tres años. Puede utilizar los datos históricos para analizar y realizar auditorías a las políticas de enrutamiento y la seguridad de red. Puede buscar información histórica sobre los siguientes tipos de recursos:

- VPC
- Subredes de la VPC

- Direcciones IP elásticas
- Instancias de EC2 que se están ejecutando
- Interfaces de red de EC2 conectadas a instancias

> **Important**
>
> Si bien IPAM no monitorea las instancias de Amazon EC2 ni las interfaces de red de EC2 que están conectadas a instancias, usted puede utilizar la característica Buscar historial de IP para buscar datos históricos en los CIDR de instancia de EC2 e interfaz de red.

> **Note**
>
> - Los comandos de este tutorial deben ejecutarse por medio de la cuenta propietaria de la IPAM y la Región de AWS que aloja el IPAM.
> - Los registros de cambios en los CIDR se recogen en instantáneas periódicas, lo que significa que los registros pueden tardar en aparecer o actualizarse, y los valores SampledStartTime y SampledEndTime pueden diferir de las horas reales en las que se produjeron.

Escenarios

Los escenarios de esta sección le indican cómo analizar y auditar el uso de la dirección IP a través de la AWS CLI. Para obtener más información sobre los valores mencionados en este tutorial, como la hora de finalización y de inicio de las muestras, consulte Ver historial de direcciones IP.

Escenario 1: ¿Qué recursos se asociaron a **`10.2.1.155/32`** entre la 1:00 h y las 21 h del 27 de diciembre de 2021 (UTC)?

1. Use el siguiente comando:

```
aws ec2 get-ipam-address-history --region us-east-1 --cidr 10.2.1.155/32 --ipam-scope-id ipam-scope-05b579a1909c5fc7a --start-time 2021-12-20T01:00:00.000Z --end-time 2021-12-27T21:00:00.000Z
```

2. Visualice los resultados del análisis. En el ejemplo siguiente, el CIDR se asignó a una interfaz de red y a una instancia de EC2 durante un periodo determinado. Tenga en cuenta que la ausencia del valor SampledEndTime significa que el registro aún está activo. Para obtener más información sobre los valores que se muestran en la siguiente salida, consulte Ver historial de direcciones 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"
        }
    ]
}
```

Si el ID de propietario de la instancia a la que está conectada una interfaz de red difiere del ID de propietario de la interfaz de red (como es el caso de las puertas de enlace NAT, las interfaces de red de Lambda en las VPC y otros servicios de AWS), el `ResourceOwnerId` es `amazon-aws` en lugar del ID de la cuenta del propietario de la interfaz de red. El siguiente ejemplo muestra el registro de un CIDR asociado a una puerta de enlace 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"
        }
    ]
}
```

Escenario 2: ¿Qué recursos se asociaron a **`10.2.1.0/24`** desde el 1.° de diciembre de 2021 hasta el 27 de diciembre de 2021 (UTC)?

1. Use el siguiente comando:

```
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. Visualice los resultados del análisis. En el ejemplo siguiente, el CIDR se asignó a una subred y una VPC durante un periodo determinado. Tenga en cuenta que la ausencia del valor SampledEndTime significa que el registro aún está activo. Para obtener más información sobre los valores que se muestran en la siguiente salida, consulte Ver historial de direcciones IP.

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

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

Escenario 3: ¿Qué recursos se asociaron a **2605:9cc0:409::/56** desde el 1.° de diciembre de 2021 hasta el 27 de diciembre de 2021 (UTC)?

1. Ejecute el siguiente comando, donde Región es la región principal de 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. Visualice los resultados del análisis. En el ejemplo siguiente, el CIDR se asignó a dos VPC diferentes durante un periodo determinado en una región fuera de la región de origen de IPAM. Tenga en cuenta que la ausencia del valor SampledEndTime significa que el registro aún está activo. Para obtener más información sobre los valores que se muestran en la siguiente salida, consulte Ver historial de direcciones 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"
        }
    ]
}
```

Escenario 4: ¿Qué recursos se asociaron a **`10.0.0.0/24`** en las últimas 24 horas (suponiendo que la hora actual es la medianoche del 27 de diciembre de 2021 [UTC])?

1. Use el siguiente comando:

```
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. Visualice los resultados del análisis. En el ejemplo siguiente, el CIDR se asignó a numerosas subredes y VPC durante un periodo determinado. Tenga en cuenta que la ausencia del valor SampledEndTime significa que el registro aún está activo. Para obtener más información sobre los valores que se muestran en la siguiente salida, consulte Ver historial de direcciones 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"
        }
    ]
}
```

Escenario 5: ¿Qué recursos están asociados actualmente a **10.2.1.155/32**?

1. Use el siguiente comando:

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

2. Visualice los resultados del análisis. En el ejemplo siguiente, el CIDR se asignó a una interfaz de red y a una instancia de EC2 durante un periodo determinado. Tenga en cuenta que la ausencia del valor SampledEndTime significa que el registro aún está activo. Para obtener más información sobre los valores que se muestran en la siguiente salida, consulte Ver historial de direcciones 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"
        }
    ]
}
```

Escenario 6: ¿Qué recursos están asociados actualmente a **10.2.1.0/24**?

1. Use el siguiente comando:

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

2. Visualice los resultados del análisis. En el ejemplo siguiente, el CIDR se asignó a una VPC y a una subred durante un periodo determinado. Solo los resultados que coinciden exactamente con este CIDR `/24` se devuelven, no todos los `/32` dentro de los CIDR `/24`. Tenga en cuenta que la ausencia del valor SampledEndTime significa que el registro aún está activo. Para obtener más información sobre los valores que se muestran en la siguiente salida, consulte Ver historial de direcciones IP.

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

Escenario 7: ¿Qué recursos están asociados actualmente a **`54.0.0.9/32`**?

En este ejemplo, a `54.0.0.9/32` se le asigna una dirección IP elástica que no forma parte de la Organización de AWS integrada con su IPAM.

1. Use el siguiente comando:

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

2. Dado que a `54.0.0.9/32` se le asigna a una dirección IP elástica que no forma parte de la Organización de AWS integrada con el IPAM en este ejemplo, no se devuelven registros.

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

Tutorial: Traer el ASN a IPAM

Si sus aplicaciones utilizan direcciones IP fiables y números de sistema autónomo (ASN) que sus socios o clientes han permitido en su red, puede ejecutar estas aplicaciones en AWS sin necesidad de que sus socios o clientes cambien sus listas de permisos.

Un número de sistema autónomo (ASN) es un número único a nivel global que permite identificar un grupo de redes a través de Internet e intercambiar datos de enrutamiento con otras redes de forma dinámica mediante el Protocolo puerta de enlace de borde. Los proveedores de servicios de Internet (ISP), por ejemplo, utilizan los ASN para identificar el origen del tráfico de red. No todas las organizaciones adquieren sus propios ASN, pero en el caso de las organizaciones que sí lo hacen, pueden traer sus ASN a AWS.

Uso de su propio número de sistema autónomo (BYOASN) le permite anunciar las direcciones IPv4 o IPv6 a las que accede AWS con su propio ASN público en lugar de hacerlo con el ASN de AWS. Cuando utiliza BYOASN, el tráfico que se origina en su dirección IP tiene su ASN en lugar del ASN de AWS, y los clientes o socios que han autorizado el tráfico listado en función de su dirección IP y ASN pueden acceder a sus cargas de trabajo.

Important

- Complete este tutorial con la cuenta de administrador de IPAM en la región de origen de su IPAM.
- En este tutorial se da por sentado que es el propietario del ASN público que desea traer a IPAM, que ya ha traído un CIDR de BYOIP a AWS y que lo ha aprovisionado a un grupo de su alcance público. Puede incorporar un ASN a IPAM en cualquier momento, pero

para utilizarlo tiene que asociarlo a un CIDR que haya traído a su cuenta de AWS. En este tutorial se asume que ya ha realizado dichas acciones. Para obtener más información, consulte Tutorial: incorpore sus direcciones IP a IPAM.

- Puede cambiar entre su propio ASN o un ASN de AWS sin demora, pero solo puede cambiar de un ASN a su propio ASN de AWS una vez por hora.
- Si su CIDR de BYOIP se encuentra anunciado actualmente, no es necesario que retire el anuncio para asociarlo a su ASN.

Requisitos previos de incorporación para su ASN

Necesitará lo siguiente para completar este tutorial:

- Su ASN público de 2 o 4 bytes.
- Si ya ha traído un rango de direcciones IP a AWS con Tutorial: incorpore sus direcciones IP a IPAM, necesitas el rango de CIDR de direcciones IP. También necesitarás una clave privada. Puede usar la clave privada que creó al cambiar el rango de CIDR de direcciones IP a AWS o puede crear una nueva clave privada como se describe en Crear una clave privada y generar un certificado X.509 en la Guía del usuario de Amazon EC2.
- Al agregar un rango de direcciones IPv4 o IPv6 a AWS con Tutorial: incorpore sus direcciones IP a IPAM, crea un certificado X.509 y lo carga en el registro de RDAP en su RIR. Debe cargar el mismo certificado que ha creado en el registro de RDAP en su RIR para el ASN. Asegúrese de incluir las cadenas `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----` antes y después de la parte codificada. Todo este contenido debe estar en una sola línea larga. El procedimiento para actualizar el RDAP depende de su RIR:
  - Para ARIN, utilice el portal del administrador de cuentas para agregar el certificado en la sección “Public Comments” del objeto “Información de la red” que representa el ASN mediante la opción “Modify ASN”. No lo añada a la sección de comentarios de su organización.
  - Para RIPE, agregue el certificado como un nuevo campo “descr” al objeto “aut-num” que representa el ASN. Por lo general, se encuentran en la sección “Mis recursos” del

    portal de bases de datos de RIPE. No lo agregue a la sección de comentarios de la organización ni al campo “Observaciones” del objeto “aut-num”.
  - Para APNIC, envíe el certificado por correo electrónico a helpdesk@apnic.net para agregarla manualmente al campo “Observaciones”. Envíe el correo electrónico con el contacto autorizado de APNIC para el ASN.

- Al incorporar un rango de direcciones IP al IPAM, crea un ROA para comprobar que controla el espacio de direcciones IP que incorpora al IPAM. Además de ese ROA, debe tener un segundo ROA en su RIR con el ASN que incorporará al IPAM. Si no tiene este segundo ROA para el ASN en su RIR, complete 3. Cree un objeto ROA en su Registro Regional de Internet (RIR). Ignore los demás pasos.

Pasos del tutorial

Complete los pasos que se indican a continuación mediante la consola de AWS o la AWS CLI.

AWS Management Console

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación izquierdo, elija IPAM.
3. Seleccione su IPAM.
4. Seleccione la pestaña BYOASN y elija Aprovisionar BYOASN.
5. Ingrese el ASN. Como resultado, el campo Mensaje se completa de forma automática con el mensaje que necesitará para iniciar sesión en el siguiente paso.

   - El formato del mensaje es el siguiente: CUENTA es su número de cuenta de AWS, ASN es el ASN que trae a IPAM y AAAAMMDD es la fecha de caducidad del mensaje (que, de forma predeterminada, es el último día del mes siguiente). Ejemplo:

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

6. Copie el mensaje y reemplace la fecha de caducidad por su propio valor si lo desea.
7. Firme el mensaje con la clave privada. Ejemplo:

   ```
   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. En Firma, introduzca la firma.
9. (Opcional) Para aprovisionar otro ASN, elija Aprovisionar otro ASN. Puede aprovisionar hasta 5 ASN. Para aumentar esta cuota, consulte Cuotas de IPAM.
10. Elija Aprovisionar.

11. Consulte el proceso de aprovisionamiento en la pestaña BYOASN. Espere a que el Estado cambie de Aprovisionamiento pendiente a Aprovisionado. Los BYOASN en estado de Aprovisionamiento fallido se eliminan de forma automática después de 7 días. Una vez que el ASN se haya aprovisionado de forma correcta, puede asociarlo a un CIDR de BYOIP.
12. En el panel de navegación izquierdo, elija Grupos.
13. Seleccione el alcance público. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
14. Elija un grupo regional que tenga un CIDR de BYOIP aprovisionado. El grupo debe tener Servicio establecido en EC2 y debe contar con una configuración regional.
15. Elija la pestaña CIDR y seleccione un CIDR de BYOIP.
16. Seleccione Acciones > Administrar asociaciones de BYOASN.
17. En los BYOASN asociados, elija el ASN que trajo a AWS. Si tiene varios ASN, puede asociar varios ASN al CIDR de BYOIP. Puede asociar tantos ASN como pueda traer a IPAM. Tenga en cuenta que, de forma predeterminada, puede traer hasta 5 ASN a IPAM. Para obtener más información, consulte Cuotas de IPAM.
18. Elija Asociar.
19. Espere a que se complete la asociación del ASN. Una vez que el ASN se haya asociado de forma correcta al CIDR de BYOIP, podrá volver a anunciar el CIDR de BYOIP.
20. Elija la pestaña CIDR agrupados.
21. Seleccione el CIDR de BYOIP y elija Actions (Acciones) > Advertise (Anunciar). Como resultado, se muestran sus opciones de ASN: el ASN de Amazon y cualquier ASN que haya traído a IPAM.
22. Seleccione el ASN que haya traído a IPAM y elija Anunciar CIDR. Como resultado, se anuncia el CIDR de BYOIP y el valor en la columna Advertising (anuncio) cambia de Withdrawn (Retirado) a Advertised (Anunciado). En la columna del Número de sistema autónomo se muestra el ASN asociado al CIDR.
23. (Opcional) Si decide volver a cambiar la asociación del ASN por el de Amazon, seleccione el CIDR de BYOIP y vuelva a elegir Acciones > Anunciar. Esta vez, elija el ASN de Amazon. Puede volver a cambiar al ASN de Amazon en cualquier momento, pero solo puede cambiar a un ASN personalizado una vez cada hora.

Se ha completado el tutorial.

Limpieza

1. Desasociar el ASN del CIDR de BYOIP

   - Para retirar el CIDR de BYOIP del anuncio, en su grupo de alcance público, elija el CIDR de BYOIP y seleccione Acciones > Retirar del anuncio.
   - Para desasociar el ASN del CIDR, seleccione Acciones > Administrar las asociaciones de BYOASN.

2. Desaprovisionar el ASN

   - Para desaprovisionar el ASN, en la pestaña BYOASN, elija el ASN y luego Desaprovisionar ASN. Como resultado, se desaprovisiona el ASN. Los BYOASN en estado Desaprovisionado se eliminan de forma automática después de 7 días.

Ha completado la limpieza.

Command line

1. Aprovisione su ASN incluyendo su ASN y su mensaje de autorización. La firma es el mensaje firmado con tu clave privada.

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

2. Describa su ASN para realizar un seguimiento del proceso de aprovisionamiento. Si la solicitud se realiza de forma correcta, debería ver ProvisionStatus establecido en Aprovisionado al cabo de unos minutos.

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

3. Asocie el ASN a su CIDR de BYOIP. Cualquier ASN personalizado desde el que desee anunciar primero debe estar asociado a su CIDR.

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

4. Describa su CIDR para realizar un seguimiento del proceso de asociación.

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

5. Anuncie el CIDR con su ASN. Si el CIDR ya se ha anunciado, se cambiará el ASN de origen del ASN de Amazon al suyo.

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

6. Describa su CIDR para ver cómo el estado del ASN cambia de asociado a anunciado.

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

Se ha completado el tutorial.

Limpieza

1. Realice una de las siguientes acciones:

   - Para retirar únicamente su anuncio de ASN y volver a utilizar los ASN de Amazon mientras se mantiene el CIDR anunciado, debe llamar a advertise-byoip-cidr con el valor especial de AWS del parámetro asn. Puede volver a cambiar al ASN de Amazon en cualquier momento, pero solo puede cambiar a un ASN personalizado una vez cada hora.

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

   - Para retirar su anuncio del CIDR y ASN de forma simultánea, puede llamar a withdraw-byoip-cidr.

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

2. Para eliminar su ASN, primero debe desasociarlo de su CIDR de BYOIP.

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

3. Una vez que su ASN se haya disociado de todos los CIDR de BYOIP a los que lo asoció, puede desaprovisionarlo.

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

4. El CIDR de BYOIP también se puede desaprovisionar una vez que se hayan eliminado todas las asociaciones de ASN.

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

5. Confirme el desaprovisionamiento.

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

Ha completado la limpieza.

Tutorial: incorpore sus direcciones IP a IPAM

Los tutoriales de esta sección lo guían a través del proceso de llevar el espacio de direcciones IP públicas a AWS y administrar el espacio con IPAM.

La administración del espacio de direcciones IP públicas con IPAM tiene los siguientes beneficios:

- Mejora la utilización de las direcciones IP públicas en toda la organización: puede utilizar IPAM para compartir espacio de direcciones IP entre cuentas de AWS. Sin utilizar IPAM, no puede compartir su espacio de IP público entre cuentas de AWS Organizations.
- Simplifica el proceso de traer el espacio de IP público a AWS: puede utilizar IPAM para incorporar un espacio de direcciones IP públicas una vez y, a continuación, utilizar IPAM a fin de distribuir sus IP públicas entre regiones para recursos como instancias de EC2 y equilibradores de carga de aplicación. Sin IPAM, debe incorporar las IP públicas para cada región de AWS.

Contenido

Verificación del control de dominio

Antes de ajustar un rango de direcciones IP a AWS, debe usar una de las opciones descritas en esta sección para comprobar que controla el espacio de direcciones IP. Esto se aplica a los rangos

de direcciones IPv4 e IPv6. Después, cuando lleve un rango de direcciones IP a AWS, AWS valida que usted controla el rango de direcciones IP. Esta validación garantiza que los clientes no puedan utilizar rangos de IP que pertenezcan a otros, lo que evita problemas de enrutamiento y seguridad.

Hay dos métodos que puede utilizar para verificar que controla el rango:

- Certificado X.509: si su rango de direcciones IP está registrado en un registro de Internet compatible con el RDAP (como ARIN, RIPE y APNIC), puede usar un certificado X.509 para verificar la propiedad de su dominio.
- Registro TXT de DNS: independientemente de si su registro de Internet admite el RDAP, puede usar un token de verificación y un registro TXT de DNS para verificar la propiedad de su dominio.

Contenido

Verificación de su dominio con un certificado X.509

En esta sección se describe cómo verificar su dominio con un certificado X.509 antes de incluir su rango de direcciones IP en IPAM.

Para verificar su dominio con un certificado X.509

1. Complete los tres pasos en Requisitos previos de BYOIP en Amazon EC2 en la Guía del usuario de Amazon EC2.

> **Note**
>
> Al crear las ROA, para los CIDR IPv4 debe establecer la longitud máxima de un prefijo de dirección IP en `/24`. Para los CIDR IPv6, si los agregará a un grupo que se puede anunciar, la longitud máxima de un prefijo de dirección IP debe ser `/48`. Esto garantiza que tenga total flexibilidad para dividir su dirección IP pública entre regiones de AWS. IPAM impone la longitud máxima que establezca. La longitud máxima es el anuncio de longitud de prefijo más pequeño que permitirá para esta ruta. Por ejemplo, si trae un bloque de CIDR `/20` a AWS, al establecer la longitud máxima en `/24`, puede dividir el bloque más grande de la forma que desee (por ejemplo, con `/21`, `/22` o `/24`) y distribuir esos bloques de CIDR más pequeños en cualquier región. Si tuviera que establecer la

longitud máxima en `/23`, no sería capaz de dividir y anunciar un `/24` del bloque más grande. Además, tenga en cuenta que `/24` es el bloque IPv4 más pequeño y `/48` es el bloque IPv6 más pequeño que puede anunciar desde una región a Internet.

2. Complete únicamente los pasos 1 y 2 en Aprovisionamiento de un intervalo de direcciones que se anuncie públicamente en AWS en la Guía del usuario de Amazon EC2 y no aprovisione el rango de direcciones (paso 3) todavía. Guarde `text_message` y `signed_message`. Las necesitará más adelante en este procedimiento.

Cuando haya completado estos pasos, continúe con Lleve su propia IP a IPAM por medio de la consola de administración de AWS y la CLI AWS o Lleve su propio CIDR IP a IPAM únicamente por medio de la CLI AWS.

Verificación de su dominio con un registro TXT de DNS

Complete los pasos de esta sección para verificar su dominio con un registro TXT de DNS antes de incluir su rango de direcciones IP en IPAM.

Puede usar los registros TXT de DNS para validar que controla un rango de direcciones IP públicas. Un registro TXT de DNS es un tipo de registro de DNS que contiene información acerca del nombre de su dominio. Esta característica le permite incluir las direcciones IP registradas en cualquier registro de Internet (como JPNIC, LACNIC y AFRINIC), no solo las que admiten validaciones basadas en registros del RDAP (Protocolo de acceso a datos de registro) (como ARIN, RIPE y APNIC).

Important

Para poder continuar, debe haber creado ya un IPAM en el nivel gratuito o avanzado. Si no tiene un IPAM, complete Creación de un IPAM primero.

Contenido

Paso 1: cree un ROA si no dispone de uno

Debe tener una autorización de origen de ruta (ROA) en su registro regional de Internet (RIR) para los rangos de direcciones IP que desee anunciar. Si no tiene un ROA en su RIR, complete 3. Cree un objeto ROA en su RIR en la Guía del usuario de Amazon EC2. Ignore los demás pasos.

El intervalo de direcciones IPv4 más específico que puede traer es /24. El intervalo de direcciones IPv6 más específico que puede utilizar es /48 para los CIDR que se anuncian públicamente y /60 para los CIDR que no se anuncian públicamente.

Paso 2. Creación de un token de verificación

Un token de verificación es un valor aleatorio generado por AWS que puede usar para demostrar que tiene el control de un recurso externo. Por ejemplo, puede usar un token de verificación para validar que controla un rango de direcciones IP públicas al ajustar un rango de direcciones IP a AWS (BYOIP).

Complete los pasos de esta sección para crear un token de verificación que necesitará en un paso posterior de este tutorial para incorporar su rango de direcciones IP a IPAM. Use las instrucciones que aparecen a continuación para la consola de AWS o para la AWS CLI.

AWS Management Console

Para crear un token de verificación

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En la consola de administración AWS, elija la región AWS en la que desea crear el IPAM.
3. En el panel de navegación izquierdo, elija IPAM.
4. Elija su IPAM y, a continuación, seleccione la pestaña de tokens de verificación.
5. Seleccione Crear token de verificación.
6. Tras crear el token, deje abierta esta pestaña del navegador. Necesitará el valor del token, el nombre del token en el siguiente paso y el ID del token en un paso posterior.

Tenga en cuenta lo siguiente:

- Una vez que haya creado un token de verificación, podrá reutilizarlo para varios CIDR de BYOIP que aprovisione desde su IPAM en un plazo de 72 horas. Si quiere aprovisionar más CIDR después de 72 horas, necesita un token nuevo.
- Puede crear hasta 100 tokens. Si alcanza el límite, elimine los tokens caducados.

Command line

- Solicite que IPAM cree un token de verificación que utilizará para la configuración del DNS con create-ipam-external-resource-verification-token:

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

Esto devolverá un IpamExternalResourceVerificationTokenID y un token con `TokenName` y `TokenValue` y el tiempo de caducidad (`NotAfter`) del token.

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

Tenga en cuenta lo siguiente:

- Una vez que haya creado un token de verificación, podrá reutilizarlo para varios CIDR de BYOIP que aprovisione desde su IPAM en un plazo de 72 horas. Si quiere aprovisionar más CIDR después de 72 horas, necesita un token nuevo.
- Puede ver sus tokens con describe-ipam-external-resource-verification-tokens.
- Puede crear hasta 100 tokens. Si llega al límite, puede eliminar los tokens caducados mediante delete-ipam-external-resource-verification-token.

Paso 3. Configuración de la zona DNS y el registro TXT

Complete los pasos descritos en esta sección para configurar la zona DNS y el registro TXT. Si no utiliza Route53 como DNS, siga la documentación proporcionada por su proveedor de DNS para configurar una zona DNS y añadir un registro TXT.

Si utiliza Route53, tenga en cuenta lo siguiente:

- Para crear una zona de búsqueda inversa en la consola de AWS, consulte Creating a public hosted zone en la Guía para desarrolladores de Amazon Route 53 o utilice el comando de AWS CLI create-hosted-zone.
- Para crear un registro en la zona de búsqueda inversa de la consola de AWS, consulte Creating records by using the Amazon Route 53 console en la Guía para desarrolladores de Amazon Route 53 o utilice el comando de AWS CLI change-resource-record-sets.
- Cuando haya terminado de crear la zona alojada, delegue la zona alojada de su RIR a los servidores de nombres proporcionados por Route53 (por ejemplo, para LACNIC o APNIC).

Ya sea que utilice otro proveedor de DNS o Route53, al configurar el registro TXT, tenga en cuenta lo siguiente:

- El nombre del registro debe ser el nombre de su token.
- El tipo de registro debe ser TXT.
- El valor ResourceRecord debe ser el valor del token.

Ejemplo:

- Nombre: `86950620.113.0.203.in-addr.arpa`
- Tipo: `TXT`
- Valor de ResourceRecords: `a34597c3-5317-4238-9ce7-50da5b6e6dc8`

Donde:

- `86950620` es el nombre del token de verificación.
- `113.0.203.in-addr.arpa` es el nombre de la zona de búsqueda inversa.
- `TXT` es el tipo de registro.
- `a34597c3-5317-4238-9ce7-50da5b6e6dc8` es el valor del token de verificación.

> **Note**
>
> Según el tamaño del prefijo que se va a llevar a IPAM con BYOIP, se deben crear uno o más registros de autenticación en el DNS. Estos registros de autenticación son del tipo de registro TXT y deben colocarse en la zona inversa del propio prefijo o de su prefijo principal.

- En el caso de IPv4, los registros de autenticación deben alinearse con los rangos situados en el límite de un octeto que componen el prefijo.
  - Ejemplos
  - Para 198.18.123.0/24, que ya está alineado en el límite de un octeto, necesitará crear un registro de autenticación único en:
    - *token-name*.123.18.198.in-addr.arpa. IN TXT "*token-value*"
  - Para 198.18.12.0/22, que en sí mismo no está alineado con el límite del octeto, necesitará crear cuatro registros de autenticación. Estos registros deben cubrir las subredes 198.18.12.0/24, 198.18.13.0/24, 198.18.14.0/24 y 198.18.15.0/24, que están alineadas en el límite de un octeto. Las entradas de DNS correspondientes deben ser:
    - *token-name*.12.18.198.in-addr.arpa. IN TXT "*token-value*"
    - *token-name*.13.18.198.in-addr.arpa. IN TXT "*token-value*"
    - *token-name*.14.18.198.in-addr.arpa. IN TXT "*token-value*"
    - *token-name*.15.18.198.in-addr.arpa. IN TXT "*token-value*"
  - Para 198.18.0.0/16, que ya está alineado en el límite de un octeto, necesita crear un registro de autenticación único:
    - *token-name*.18.198.in-addr.arpa. IN TXT "*token-value*"
- En el caso de IPv6, los registros de autenticación deben alinearse con los rangos situados en el límite de nibble que componen el prefijo. Los valores de nibble válidos son, por ejemplo, 32, 36, 40, 44, 48, 52, 56 y 60.
  - Ejemplos
  - Para 2001:0db8::/40, que ya está alineado en el límite de nibble, necesita crear un registro de autenticación único:
    - *token-name*.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
  - Para 2001:0db8:80::/42, que en sí mismo no está alineado con el límite de nibble, debe crear cuatro registros de autenticación. Estos registros deben cubrir las subredes 2001:db8:80::/44, 2001:db8:90::/44, 2001:db8:a0::/44, y 2001:db8:b0::/44, que están alineadas en un límite de nibble. Las entradas de DNS correspondientes deben ser:
    - *token-name*.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
    - *token-name*.9.0.0.8.b.d.0.1.0.0.2.ip6.arpa TXT "*token-value*"
    - *token-name*.a.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"
    - *token-name*.b.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "*token-value*"

- Para el rango no anunciado 2001:db8:0:1000::/54, que en sí mismo no está alineado con un límite fijo, debe crear cuatro registros de autenticación. Estos registros deben cubrir las subredes 2001:db8:0:1000::/56, 2001:db8:0:1100::/56, 2001:db8:0:1200::/56 y 2001:db8:0:1300::/56, que están alineadas en un límite de nibble. Las entradas de DNS correspondientes deben ser:
  - `token-name.0.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
  - `token-name.1.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
  - `token-name.2.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
  - `token-name.3.1.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN TXT "token-value"`
- Para validar el número correcto de números hexadecimales entre el nombre del token y la cadena "ip6.arpa", multiplique el número por cuatro. El resultado debe coincidir con la longitud del prefijo. Por ejemplo, para un prefijo /56, debe tener 14 dígitos hexadecimales.

Cuando haya completado estos pasos, continúe con Lleve su propia IP a IPAM por medio de la consola de administración de AWS y la CLI AWS o Lleve su propio CIDR IP a IPAM únicamente por medio de la CLI AWS.

Lleve su propia IP a IPAM por medio de la consola de administración de AWS y la CLI AWS

Traiga su propia IP (BYOIP) al IPAM le permite utilizar los rangos de direcciones IPv4 e IPv6 existentes de su organización en AWS. Esto le permite mantener una imagen de marca coherente, mejorar el rendimiento de la red, mejorar la seguridad y simplificar la administración al unificar los entornos en las instalaciones y en la nube en su propio espacio de direcciones IP.

Siga estos pasos para llevar un CIDR IPv4 o IPv6 a IPAM por medio de la consola de administración de AWS y la AWS CLI.

> **Note**
>
> Antes de comenzar, debe tener un control de dominio verificado.

Una vez que hayas llevado un rango de direcciones IPv4 a AWS, podrás usar todas las direcciones IP del rango, incluidas la primera dirección (la dirección de red) y la última dirección (la dirección de transmisión).

Contenido

Lleve su propio CIDR IPv4 a IPAM por medio de la consola de administración de AWS y la AWS CLI

Siga estos pasos para llevar un CIDR IPv4 a IPAM y asignar una dirección IP elástica (EIP) mediante la consola de administración de AWS y la AWS CLI.

> **Important**
>
> - En este tutorial, se presupone que ya ha completado los pasos que se detallan en las siguientes secciones:
>   - Integración de IPAM con cuentas en una organización de AWS.
>   - Creación de un IPAM.
> - Cada paso de este tutorial debe realizarse con una de tres cuentas de AWS Organizations:
>   - La cuenta de administración.
>   - La cuenta de miembro configurada para ser su administrador de IPAM en Integración de IPAM con cuentas en una organización de AWS. En este tutorial, esta cuenta se llamará cuenta de IPAM.
>   - La cuenta de miembro de su organización es la que asignará CIDR de un grupo de IPAM. En este tutorial, esta cuenta se llamará cuenta de miembro.

Contenido

Paso 1: Crear perfiles con nombre y roles de IAM de la AWS CLI

Para completar este tutorial como un usuario de AWS único, puede utilizar perfiles con nombre de AWS CLI para cambiar de un rol de IAM a otro. Los perfiles con nombre son conjuntos de configuraciones y credenciales a los que se hace referencia cuando se utiliza la opción `--profile` con la AWS CLI. Para obtener más información sobre cómo crear roles de IAM y perfiles con nombre para las cuentas de AWS, consulte Uso de un rol de IAM en la AWS CLI.

Cree un rol y un perfil con nombre para cada una de las tres cuentas de AWS que utilizará en este tutorial:

- Un perfil llamado `management-account` para la cuenta de administración de AWS Organizations.
- Un perfil llamado `ipam-account` para la cuenta de miembro de AWS Organizations que está configurada para ser su administrador de IPAM.
- Un perfil llamado `member-account` para la cuenta de miembro de AWS Organizations en su organización que asignará CIDR de un grupo de IPAM.

Después de crear los roles de IAM y los perfiles con nombre, regrese a esta página y vaya al paso siguiente. En el resto de este tutorial, observará que los comandos AWS CLI de ejemplo utilizan la opción `--profile` con uno de los perfiles con nombre para indicar qué cuenta debe ejecutar el comando.

Paso 2: Cree un grupo de IPAM de nivel superior

Complete los pasos de esta sección para crear un grupo de IPAM de nivel superior.

La cuenta de IPAM debe realizar este paso.

Para crear un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Seleccione el alcance público. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. Elija Create pool (Crear grupo).
5. (Opcional) Agregue una Name tag (Etiqueta de nombre) y una Description (Descripción) para el grupo.
6. En Origen, elija Alcance del IPAM.
7. En Address family (Familia de direcciones), elija IPv4.
8. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
9. En Locale (Configuración regional), elija None (Ninguna).

   La integración de IPAM con BYOIP requiere que la configuración regional se establezca en el grupo que se utilizará para el CIDR de BYOIP. Dado que va a crear un grupo de IPAM de nivel superior con un grupo regional dentro de él y vamos a asignar espacio a una dirección IP elástica desde el grupo regional, establecerá la configuración regional en el grupo regional y no en el grupo de nivel superior. Agregará la configuración regional al grupo regional cuando cree dicho grupo en un paso posterior.

   > **Note**
   >
   > Si está creando un solo grupo y no un grupo de nivel superior con grupos regionales dentro de él, podría querer elegir una configuración regional para este grupo de modo que esté disponible para asignaciones.

10. En Fuente de IP pública, seleccione BYOIP.
11. En la sección CIDR que desee aprovisionar, realice una de las siguientes acciones:

- Si verificó el control de su dominio con un certificado X.509, debe incluir el CIDR y el mensaje BYOIP y la firma del certificado que creó en ese paso para que podamos verificar que controla el espacio público.
- Si verificó el control de su dominio con un registro TXT de DNS, debe incluir el CIDR y el token de verificación CIDR e IPAM que creó en ese paso para que podamos verificar que controla el espacio público.

Tenga en cuenta que cuando aprovisione un CIDR IPv4 en un grupo dentro del grupo de nivel superior, el CIDR IPv4 mínimo que puede aprovisionar es `/24`; no se permiten CIDR más específicos (como `/25`).

> **Important**
>
> Si bien la mayoría del aprovisionamiento se completará en dos horas, el proceso de aprovisionamiento de los intervalos que se pueden anunciar públicamente puede tardar hasta una semana en completarse.

12. Deje sin seleccionar la opción Configure this pool's allocation rule settings.
13. (Opcional) Elija Tags (Etiquetas) para el grupo.
14. Elija Create pool (Crear grupo).

Antes de continuar, asegúrese de que este CIDR se haya aprovisionado. Puede ver el estado del aprovisionamiento en la pestaña CIDR en la página de detalles del grupo.

Paso 3. Crear un grupo regional dentro del grupo de nivel superior

Crear un grupo regional dentro del grupo de nivel superior La integración de IPAM con BYOIP requiere que la configuración regional se establezca en el grupo que se utilizará para el CIDR de BYOIP. Agregará la configuración regional al grupo regional cuando cree dicho grupo en esta sección. La `Locale` debe ser parte de una de las regiones operativas que configuró cuando creó el IPAM. Por ejemplo, una configuración regional de us-east-1 significa que us-east-1 debe ser una región operativa para IPAM. Una configuración regional us-east-1-scl-1 (un grupo de borde de red que se utiliza para las zonas locales) significa que IPAM debe tener una región operativa de us-east-1.

La cuenta de IPAM debe realizar este paso.

Para crear un grupo regional dentro de un grupo de nivel superior

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Si no desea utilizar el alcance privado predeterminado, en el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. Elija Create pool (Crear grupo).
5. (Opcional) Agregue una Name tag (Etiqueta de nombre) y una Description (Descripción) para el grupo.
6. En Origen, elija el grupo de nivel superior que ha creado en la sección anterior.
7. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
8. En Locale (Configuración regional), elija la configuración regional para el grupo. En este tutorial, utilizaremos `us-east-2` como escenario para el grupo regional. Las opciones disponibles proceden de las regiones operativas que eligió al crear su IPAM.

   En su lugar, realice una de las siguientes acciones:

   - Una región de AWS en las que desea que este grupo de IPAM esté disponible para asignaciones.
   - El grupo de límites de red de una zona AWS local en la que desea que este grupo de IPAM esté disponible para asignaciones (zonas locales compatibles). Esta opción solo está disponible para los grupos IPv4 de IPAM de ámbito público.
   - Una zona AWS local dedicada. Para crear un grupo dentro de una zona AWS local dedicada, ingrese la zona AWS local dedicada en la entrada del selector.
   - `Global` cuando desee utilizar direcciones IP de forma global en todas las regiones de AWS, como las ubicaciones de CloudFront. La configuración local `Global` solo está disponible para los grupos IPv4 públicos.

   Por ejemplo, solo puede asignar un CIDR para una VPC desde un grupo de IPAM que comparte una configuración regional con la región de la VPC. Tenga en cuenta que, una vez elegida la

configuración regional para un grupo, no puede modificarla. Si la región de origen de IPAM no está disponible debido a una interrupción y el grupo tiene una configuración regional diferente a la región de origen de IPAM, el grupo aún se puede usar para asignar direcciones IP.

Elegir una configuración regional garantiza que no haya dependencias entre regiones entre su grupo y los recursos que se asignan desde él.

9. En Service (Servicio), elija EC2 (EIP/VPC). El servicio que seleccione determina el servicio AWS en el que el CIDR será anunciado. Actualmente, la única opción es EC2 (EIP/VPC), lo que significa que los CIDR asignados desde este grupo podrán ser anunciados por el servicio Amazon EC2 (para direcciones IP elásticas) y el servicio Amazon VPC (para CIDR asociados a VPC).
10. En CIDRs to provision (CIDR para aprovisionar), elija un CIDR para aprovisionar el grupo.

> **Note**
>
> Al aprovisionar un CIDR en un grupo regional dentro del grupo de nivel superior, el CIDR IPv4 más específico que puede aprovisionar es `/24`; no se permiten CIDR más específicos (como `/25`). Después de crear el grupo regional, podrá crear grupos más reducidos (como `/25`) dentro del mismo grupo regional. Tenga en cuenta que, si comparte el grupo o los grupos regionales dentro de este, estos grupos solo se podrán utilizar en la configuración regional establecida en el mismo grupo regional.

11. Habilite Configure this pool's allocation rule settings. Aquí tiene las mismas opciones de reglas de asignación que cuando creó el grupo de nivel superior. Consulte Creación de un grupo IPv4 de nivel superior para obtener una explicación de las opciones disponibles al crear grupos. Las reglas de asignación del grupo regional no se heredan del grupo de nivel superior. Si no aplica ninguna regla aquí, no se establecerán reglas de asignación para el grupo.
12. (Opcional) Elija Tags (Etiquetas) para el grupo.
13. Cuando haya terminado de configurar el grupo, elija Create pool (Crear grupo).

Antes de continuar, asegúrese de que este CIDR se haya aprovisionado. Puede ver el estado del aprovisionamiento en la pestaña CIDR en la página de detalles del grupo.

Paso 4: anuncio del CIDR

La cuenta de IPAM debe realizar los pasos de esta sección. Una vez que asocie la dirección IP elástica (EIP) a una instancia o un Elastic Load Balancer, podrá comenzar a anunciar el CIDR que

llevó a AWS y se encuentra en el grupo con Service EC2 (EIP/VPC) (Servicio EC2 [EIP/VPC]) configurado. En este tutorial, ese es su grupo regional. De forma predeterminada, el CIDR no se anuncia, lo que significa que no es accesible de manera pública a través de Internet.

La cuenta de IPAM debe realizar este paso.

> **Note**
>
> El estado del anuncio no restringe su capacidad de asignar direcciones IP elásticas. Incluso si su CIDR de BYOIPv4 no está anunciado, puede crear EIP a partir del grupo del IPAM.

Para anunciar el CIDR

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Seleccione el alcance público. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. Elija el grupo regional que creó en este tutorial.
5. Elija la pestaña CIDR.
6. Seleccione el CIDR de BYOIP y elija Actions (Acciones) > Advertise (Anunciar).
7. Elija Advertise CIDR (Anunciar CIDR).

Como resultado, se anuncia el CIDR de BYOIP y el valor en la columna Advertising (Anuncio) cambia de Withdrawn (Retirado) a Advertised (Anunciado).

Paso 5. Comparta el grupo regional

Siga los pasos de esta sección para compartir el grupo de IPAM utilizando AWS Resource Access Manager (RAM).

Habilitar el uso compartido de recursos en AWS RAM

Después de crear su IPAM, podrá compartir el grupo regional con otras cuentas de su organización. Antes de compartir un grupo de IPAM, complete los pasos de esta sección para habilitar el uso compartido de recursos con AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`management-account`**.

Habilitar el uso compartido de recursos

1. Utilizando la cuenta de administración AWS Organizations, abra la consola AWS RAM en https://console.aws.amazon.com/ram/.
2. En el panel de navegación izquierdo, seleccione Configuración, seleccione Habilitar uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.

Ahora puede compartir un grupo de IPAM con otros miembros de la organización.

Compartir un grupo de IPAM mediante AWS RAM

En esta sección compartirá el grupo regional con otra cuenta de miembro de AWS Organizations. Para instrucciones completas sobre cómo compartir grupos de IPAM, incluyendo información sobre los permisos de IAM requeridos, consulte Compartir un grupo de IPAM mediante AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`ipam-account`**.

Compartir un grupo de IPAM mediante AWS RAM

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado, elija el grupo de IPAM y seleccione Acciones > Ver detalles.
4. En Resource sharing (Uso compartido de recursos), elija Create resource share (Crear recursos compartidos). Se abrirá la consola de AWS RAM. Se compartirá el grupo utilizando AWS RAM.
5. Elija Create a resource share (Crear un recurso compartido).
6. En la consola AWS RAM, seleccione de nuevo Crear un recurso compartido.
7. Añada un Nombre para el grupo compartido.
8. En Seleccionar tipo de recurso, elija Grupos de IPAM y, a continuación, seleccione el ARN del grupo que quieres compartir.
9. Elija Siguiente.
10. Elija el permiso AWSRAMPermissionIpamPoolByoipCidrImport. Los detalles de las opciones de permiso están fuera del marco de este tutorial, pero puede encontrar más información sobre estas opciones en Compartir un grupo de IPAM mediante AWS RAM.
11. Elija Siguiente.

12. En Entidades principales > Seleccionar tipo de entidad principal, elige Cuenta de AWS e ingresa el ID de la cuenta que proporcionará un rango de direcciones IP a IPAM y, a continuación, elige Agregar .
13. Elija Siguiente.
14. Revise las opciones de recurso compartido y las entidades principales con las que se compartirá y seleccione Crear.
15. Para permitir que la cuenta de **`member-account`** asigne CIDRS de direcciones IP desde el grupo de IPAM, cree un segundo recurso compartido con `AWSRAMDefaultPermissionsIpamPool`. El valor para `--resource-arns` es el ARN del grupo de IPAM que creó en la sección anterior. El valor para `--principals` es el ID de cuenta del **`member-account`**. El valor para `--permission-arns` es el ARN del permiso `AWSRAMDefaultPermissionsIpamPool`.

Paso 6: asignación de una dirección IP elástica desde el grupo

Complete los pasos de esta sección para asignar una dirección IP elástica desde el grupo. Tenga en cuenta que si utiliza grupos de IPv4 públicos para asignar direcciones IP elásticas, puede seguir los pasos alternativos de Alternativa al paso 6 en lugar de los pasos de esta sección.

> **Important**
>
> Si aparece un error relacionado con la falta de permisos para llamar a ec2:AllocateAddress, se debe actualizar el permiso administrado actualmente asignado al grupo de IPAM que se le compartió. Póngase en contacto con la persona que creó el recurso compartido y pídale que actualice el permiso administrado `AWSRAMPermissionIpamResourceDiscovery` a la versión predeterminada. Para obtener más información, consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM.

AWS Management Console

Siga los pasos de Allocate an Elastic IP address en la Guía del usuario de Amazon EC2 para asignar la dirección, pero tenga en cuenta lo siguiente:

- La cuenta de miembro debe realizar este paso.
- Asegúrese de que la región de AWS en la que se encuentra en la consola de EC2 coincida con la opción de configuración regional que eligió al crear el grupo regional.

- Al elegir el grupo de direcciones, seleccione la opción Asignar mediante un grupo de IPAM IPv4 y elija el grupo regional que creó.

Command line

Asigne una dirección del grupo con el comando allocate-address. El valor de `--region` que utilice debe coincidir con la opción `-locale` que eligió al crear el grupo en el paso 2. Incluya el ID del grupo del IPAM que creó en el paso 2 en `--ipam-pool-id`. Si lo desea, también puede elegir un `/32` específico de su grupo de IPAM mediante la opción `--address`.

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

Respuesta de ejemplo:

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

Para obtener más información, consulte Allocate an Elastic IP address en la Guía del usuario de Amazon EC2.

Paso 7: asociación de la dirección IP elástica a una instancia de EC2

Complete los pasos de esta sección a fin de asociar la dirección IP elástica a una instancia de EC2.

AWS Management Console

Siga los pasos de Associate an Elastic IP address en la Guía del usuario de Amazon EC2 para asignar una dirección IP elástica del grupo del IPAM, pero tenga en cuenta lo siguiente: cuando utilice la opción de la Consola de administración de AWS, la región de AWS a la que asocie la dirección IP elástica debe coincidir con la opción de configuración regional que eligió al crear el grupo regional.

La cuenta de miembro debe realizar este paso.

Command line

La cuenta de miembro debe realizar este paso. Use la opción `--profile` **`member-account`**.

Asocie la dirección IP elástica a una instancia con el comando associate-address. El valor de `--region` al que asocia la dirección IP elástica debe coincidir con la opción `--locale` que eligió cuando creó el grupo regional.

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

Respuesta de ejemplo:

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

Para obtener más información, consulte Asociación de una dirección IP elástica a una instancia o una interfaz de red en la Guía del usuario de Amazon EC2.

Paso 8: Eliminar

Siga los pasos de esta sección para eliminar los recursos que ha aprovisionado y creado en este tutorial.

Paso 1: Retire el CIDR del estado de anuncio

La cuenta de IPAM debe realizar este paso.

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Seleccione el alcance público.
4. Elija el grupo regional que creó en este tutorial.
5. Elija la pestaña CIDR.
6. Seleccione el CIDR de BYOIP y elija Actions (Acciones) > Withdraw from advertising (Retirar del estado de anuncio).

7. Elija Withdraw CIDR (Retirar CIDR).

Como resultado, el CIDR de BYOIP ya no se anuncia y el valor en la columna Advertising (Anuncio) cambia de Advertised (Anunciado) a Withdrawn (Retirado).

Paso 2: Anule la asociación de una dirección IP elástica

La cuenta de miembro debe realizar este paso. Si utiliza la AWS CLI, utilice la opción `--profile` **`member-account`**.

- Realice los pasos de Anular la asociación de una dirección IP elástica en la Guía del usuario de Amazon EC2 con el objetivo de anular la asociación de la EIP. Cuando abre EC2 en la consola de administración de AWS, la Región de AWS en la que crea la EIP debe coincidir con la opción `Locale` que eligió cuando creó el grupo que se utilizará para el CIDR de BYOIP. En este tutorial, ese grupo es su grupo regional.

Paso 3: Lance la dirección IP elástica

La cuenta de miembro debe realizar este paso. Si utiliza la AWS CLI, utilice la opción `--profile` **`member-account`**.

- Realice los pasos de Lanzar una dirección IP elástica en la Guía del usuario de Amazon EC2 con el objetivo de lanzar una dirección IP elástica (EIP) desde el grupo IPv4 público. Cuando abre EC2 en la consola de administración de AWS, la Región de AWS en la que crea la EIP debe coincidir con la opción `Locale` que eligió cuando creó el grupo que se utilizará para el CIDR de BYOIP.

Paso 4: eliminación de los recursos compartidos de RAM y deshabilitación de la integración de RAM con AWS Organizations

Este paso deben realizarlo las cuentas IPAM y de administración, respectivamente. Si utiliza AWS CLI para eliminar los recursos compartidos de RAM y desactivar la integración de RAM, utilice las opciones `--profile` **`ipam-account`** y `--profile` **`management-account`**.

- Complete los pasos descritos en Eliminación de un recurso compartido en AWS RAM y, a continuación, en Desactivación del uso compartido de recursos con AWS Organizations, en la Guía del usuario de AWS RAM, en ese orden, para eliminar los recursos compartidos de RAM y desactivar la integración de RAM con AWS Organizations.

Paso 5: anulación del aprovisionamiento de los CIDR del grupo regional y del grupo de nivel superior

La cuenta de IPAM debe realizar este paso. Si utiliza la AWS CLI para compartir el grupo, utilice la opción `--profile` **`ipam-account`**.

- Siga los pasos en Anular el aprovisionamiento del CIDR de un grupo para anular el aprovisionamiento de los CIDR del grupo regional y, a continuación, del grupo de nivel superior, en ese orden.

Paso 6: eliminación del grupo regional y el grupo de nivel superior

La cuenta de IPAM debe realizar este paso. Si utiliza la AWS CLI para compartir el grupo, utilice la opción `--profile` **`ipam-account`**.

- Siga los pasos de Eliminar un grupo para eliminar el grupo regional y, a continuación, el grupo de nivel superior, en ese orden.

Alternativa al paso 6

Si utiliza grupos de IPv4 públicos para asignar direcciones IP elásticas, puede seguir los pasos de esta sección en lugar de los pasos de Paso 6: asignación de una dirección IP elástica desde el grupo.

Contenido

Paso 1: creación de un grupo de IPv4 público

Este paso lo debe realizar la cuenta de miembro que aprovisionará una dirección IP elástica.

> **Note**
>
> - La cuenta de miembro debe realizar este paso por medio de la AWS CLI.

- Los grupos IPv4 públicos y los grupos de IPAM se administran mediante distintos recursos en AWS. Los grupos IPv4 públicos son recursos de una sola cuenta que le permiten convertir sus CIDR de propiedad pública en direcciones IP elásticas. Los grupos de IPAM se pueden utilizar para asignar el espacio público a grupos IPv4 públicos.

Para crear un grupo IPv4 público mediante la AWS CLI

- Ejecute el siguiente comando para aprovisionar el CIDR. Cuando ejecute el comando en esta sección, el valor de `--region` debe coincidir con la opción `Locale` que eligió cuando creó el grupo que se utilizará para el CIDR de BYOIP.

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

En la salida aparecerá el ID del grupo IPv4 público. Necesitará este ID en el siguiente paso.

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

Paso 2: aprovisionamiento del CIDR de IPv4 público en el grupo de IPv4 público

Aprovisione el CIDR IPv4 público en su grupo IPv4 público. El valor de `--region` debe coincidir con el valor de `Locale` que eligió cuando creó el grupo que se utilizará para el CIDR de BYOIP. `--netmask-length` es la cantidad de espacio del grupo de IPAM que quiere llevar a su grupo público. El valor no puede ser mayor que la longitud de la máscara de red del grupo de IPAM. El `--netmask-length` menos específico que puede definir es `24`.

Note

- Si va a incorporar un rango de CIDR `/24` a IPAM para compartirlo en una organización de AWS, puede aprovisionar prefijos más pequeños a varios grupos de IPAM, por ejemplo, `/27` (usando `-- netmask-length 27`), en lugar de aprovisionar todo el CIDR `/24` (usando `-- netmask-length 24`), como se muestra en este tutorial.
- La cuenta de miembro debe realizar este paso por medio de la AWS CLI.

Para crear un grupo IPv4 público mediante la AWS CLI

1. Ejecute el siguiente comando para aprovisionar el 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
```

   En la salida aparecerá el CIDR aprovisionado.

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

2. Ejecute el siguiente comando para ver el CIDR aprovisionado en el grupo IPv4 público.

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

   En la salida aparecerá el CIDR aprovisionado. De forma predeterminada, el CIDR no se anuncia, lo que significa que no es accesible de manera pública a través de Internet. Tendrá la oportunidad de configurar este CIDR como anunciado en el último paso de este 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 vez creado el grupo IPv4 público, para ver el grupo IPv4 público asignado en el grupo regional de IPAM, abra la consola de IPAM y vea la asignación en el grupo regional en Allocations (Asignaciones) o Resources (Recursos).

Paso 3: asignación de una dirección IP elástica desde el grupo de IPv4 público

Siga los pasos de Allocate an Elastic IP address en la Guía del usuario de Amazon EC2 para crear una EIP desde el grupo de IPv4 público. Cuando abre EC2 en la consola de administración de AWS, la Región de AWS en la que crea la EIP debe coincidir con la opción `Locale` que eligió cuando creó el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de miembro debe realizar este paso. Si utiliza la AWS CLI, utilice la opción `--profile` **`member-account`**.

Una vez que haya completado estos tres pasos, regrese a Paso 7: asociación de la dirección IP elástica a una instancia de EC2 y continúe hasta completar el tutorial.

Alternativa a la limpieza del paso 6

Complete estos pasos para limpiar los grupos de IPv4 públicos creados con la alternativa al paso 9. Debe completar estos pasos después de liberar la dirección IP elástica durante el proceso de limpieza estándar en Paso 8: Eliminar.

Paso 1: anulación del aprovisionamiento del CIDR de IPv4 público del grupo de IPv4 público

> **Important**
>
> La cuenta de miembro debe realizar este paso por medio de la AWS CLI.

1. Vea los CIDR de BYOIP.

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

En la salida aparecerán las direcciones IP de su CIDR de 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. Ejecute el siguiente comando para lanzar el CIDR del grupo IPv4 público.

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

3. Vuelva a ver sus CIDR de BYOIP y asegúrese de que no haya más direcciones aprovisionadas. Al ejecutar el comando en esta sección, el valor de `--region` debe coincidir con la región de su IPAM.

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

En la salida aparecerá el recuento de direcciones IP en el grupo IPv4 público.

```
{
    "PublicIpv4Pools": [
```

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

> **Note**
>
> IPAM puede tardar en descubrir que se han eliminado las asignaciones de grupos IPv4 públicos. No puede continuar con la eliminación y anulación de aprovisionamiento del CIDR en el grupo de IPAM hasta que vea que la asignación se ha eliminado de IPAM.

Paso 2: eliminación del grupo de IPv4 público

La cuenta de miembro debe realizar este paso.

- Ejecute el siguiente comando para eliminar el CIDR del grupo IPv4 público. Cuando ejecute el comando en esta sección, el valor de `--region` debe coincidir con la opción `Locale` que eligió cuando creó el grupo que se utilizará para el CIDR de BYOIP. En este tutorial, ese grupo es su grupo regional. Este paso debe realizarse por medio de la AWS CLI.

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

  En la salida, verá que se devolvió el valor true (verdadero).

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

  Una vez eliminado el grupo, para ver la asignación que no ha sido administrada por IPAM, abra la consola de IPAM y vea los detalles del grupo regional en Allocations (Asignaciones).

Lleve su propio CIDR IPv6 a IPAM mediante la consola de administración de AWS

Siga los pasos de este tutorial para llevar un CIDR IPv6 a IPAM y asignar una VPC al CIDR mediante la consola de administración de AWS y la AWS CLI.

Si no necesita anunciar sus direcciones IPv6 a través de Internet, puede aprovisionar una dirección IPv6 GUA privada a un IPAM. Para obtener más información, consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados.

Important

- En este tutorial, se presupone que ya ha completado los pasos que se detallan en las siguientes secciones:
  - Integración de IPAM con cuentas en una organización de AWS.
  - Creación de un IPAM.
- Cada paso de este tutorial debe realizarse con una de tres cuentas de AWS Organizations:
  - La cuenta de administración.
  - La cuenta de miembro configurada para ser su administrador de IPAM en Integración de IPAM con cuentas en una organización de AWS. En este tutorial, esta cuenta se llamará cuenta de IPAM.
  - La cuenta de miembro de su organización es la que asignará CIDR de un grupo de IPAM. En este tutorial, esta cuenta se llamará cuenta de miembro.

Contenido

Paso 1: Cree un grupo de IPAM de nivel superior

Dado que creará un grupo de IPAM de nivel superior que incluirá un grupo regional y que se asignará espacio a un recurso desde el grupo regional, debe establecer la configuración regional en el grupo regional y no en el grupo de nivel superior. Agregará la configuración regional al grupo regional cuando cree dicho grupo en un paso posterior. La integración de IPAM con BYOIP requiere que la configuración regional se establezca en el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de IPAM debe realizar este paso.

Para crear un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Seleccione el alcance público. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. Elija Create pool (Crear grupo).
5. (Opcional) Agregue una Name tag (Etiqueta de nombre) y una Description (Descripción) para el grupo.
6. En Origen, elija Alcance del IPAM.
7. En Address family (Familia de direcciones), elija IPv6.
8. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
9. En Locale (Configuración regional), elija None (Ninguna). Establecerá la configuración regional en el grupo regional.

   La configuración regional es la región de AWS en la que desea que este grupo de IPAM esté disponible para asignaciones. Por ejemplo, solo puede asignar un CIDR para una VPC desde un grupo de IPAM que comparte una configuración regional con la región de la VPC. Tenga en cuenta que, una vez elegida la configuración regional para un grupo, no puede modificarla. Si la región de origen de IPAM no está disponible debido a una interrupción y el grupo tiene una configuración regional diferente a la región de origen de IPAM, el grupo aún se puede usar para asignar direcciones IP.

> **Note**
>
> Si está creando un solo grupo y no un grupo de nivel superior con grupos regionales dentro de él, podría querer elegir una configuración regional para este grupo de modo que esté disponible para asignaciones.

10. En Origen de IP pública, la opción BYOIP está seleccionada de forma predeterminada.
11. En la sección CIDR que desee aprovisionar, realice una de las siguientes acciones:

    - Si verificó el control de su dominio con un certificado X.509, debe incluir el CIDR y el mensaje BYOIP y la firma del certificado que creó en ese paso para que podamos verificar que controla el espacio público.
    - Si verificó el control de su dominio con un registro TXT de DNS, debe incluir el CIDR y el token de verificación CIDR e IPAM que creó en ese paso para que podamos verificar que controla el espacio público.

    Tenga en cuenta que al aprovisionar un IPv6 CIDR a un grupo dentro del grupo de nivel superior, el intervalo de direcciones IPv6 más específico que puede traer es /48 para los CIDR que se anuncian públicamente y /60 para los CIDR que no se anuncian públicamente.

    > **Important**
    >
    > Si bien la mayoría del aprovisionamiento se completará en dos horas, el proceso de aprovisionamiento de los intervalos que se pueden anunciar públicamente puede tardar hasta una semana en completarse.

12. Deje sin seleccionar la opción Configure this pool's allocation rule settings.
13. (Opcional) Elija Tags (Etiquetas) para el grupo.
14. Elija Create pool (Crear grupo).

Antes de continuar, asegúrese de que este CIDR se haya aprovisionado. Puede ver el estado del aprovisionamiento en la pestaña CIDR en la página de detalles del grupo.

Paso 2. Crear un grupo regional dentro del grupo de nivel superior

Cree un grupo regional dentro del grupo de nivel superior. La configuración regional es obligatoria en el grupo y debe ser una de las regiones operativas que configuró cuando creó la IPAM.

La cuenta de IPAM debe realizar este paso.

Para crear un grupo regional dentro de un grupo de nivel superior

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Si no desea utilizar el alcance privado predeterminado, en el menú desplegable de la parte superior del panel de contenido, elija el alcance que desea utilizar. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. Elija Create pool (Crear grupo).
5. (Opcional) Agregue una etiqueta de nombre y una descripción para el grupo.
6. En Origen, elija el grupo de nivel superior que ha creado en la sección anterior.
7. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance. Para obtener más información sobre el uso de esta opción a fin de planificar el espacio de IP de subred en una VPC, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred.
8. Elija la configuración regional del grupo. La elección de una configuración regional garantiza que no haya dependencias entre regiones entre su grupo y los recursos que se asignan desde él. Las opciones disponibles proceden de las regiones operativas que eligió al crear su IPAM. En este tutorial, utilizaremos `us-east-2` como configuración regional para el grupo regional.

   La configuración regional es la Región AWS en la que desea que este grupo de IPAM esté disponible para asignaciones. Por ejemplo, solo puede asignar un CIDR para una VPC desde un grupo de IPAM que comparte una configuración regional con la región de la VPC. Tenga en cuenta que, una vez elegida la configuración regional para un grupo, no puede modificarla. Si la región de origen de IPAM no está disponible debido a una interrupción y el grupo tiene una configuración regional diferente a la región de origen de IPAM, el grupo aún se puede usar para asignar direcciones IP.
9. En Service (Servicio), elija EC2 (EIP/VPC). El servicio que seleccione determina el servicio AWS en el que el CIDR será anunciado. En la actualidad, la única opción es EC2 (EIP/VPC), lo que

significa que los CIDR asignados desde este grupo pueden ser anunciados en los servicios Amazon EC2 y Amazon VPC (para los CIDR asociados a VPC).

10. En CIDRs to provision (CIDR para aprovisionar), elija un CIDR para aprovisionar el grupo. Tenga en cuenta que al aprovisionar un IPv6 CIDR a un grupo dentro del grupo de nivel superior, el intervalo de direcciones IPv6 más específico que puede traer es /48 para los CIDR que se anuncian públicamente y /60 para los CIDR que no se anuncian públicamente.
11. Habilite Configure this pool's allocation rule settings y elija las reglas de asignación opcionales para este grupo:

    - Automatically import discovered resources (Importar automáticamente recursos detectados): esta opción no está disponible si Locale (Configuración regional) tiene el valor None (Ninguna). Si se selecciona, IPAM buscará continuamente recursos dentro del rango de CIDR de este grupo y los importará automáticamente como asignaciones al IPAM. Tenga en cuenta lo siguiente:
      - Los CIDR que se asignarán a estos recursos no se deben haber asignado previamente a otros recursos para que la importación se realice correctamente.
      - IPAM importará un CIDR independientemente de si cumple o no con las reglas de asignación del grupo, de modo que un recurso podría importarse y marcarse posteriormente como no conforme.
      - Si IPAM detecta varios CIDR que se superponen, importará únicamente el CIDR más grande.
      - Si IPAM detecta varios CIDR con CIDR que coinciden, IPAM importará solo uno de ellos aleatoriamente.
    - Minimum netmask length (Longitud mínima de la máscara de red): la longitud mínima de la máscara de red requerida para que las asignaciones de CIDR en este grupo de IPAM sean conformes y para el bloque de CIDR de mayor tamaño que se puede asignar desde el grupo. La longitud mínima de la máscara de red debe ser inferior a su longitud máxima. Las longitudes de máscara de red posibles para las direcciones IPv4 van de `0` a `32`. Las longitudes de máscara de red posibles para las direcciones IPv6 van de `0` a `128`.
    - Default netmask length (Longitud predeterminada de la máscara de red): longitud predeterminada de la máscara de red para las asignaciones agregadas a este grupo.
    - Maximum netmask length (Longitud máxima de la máscara de red): longitud máxima de la máscara de red que se requerirá para las asignaciones de CIDR en este grupo. Este valor determina el bloque de CIDR de menor tamaño que se puede asignar desde el grupo. Asegúrese de que este valor sea mínimo **`/48`**.

- Tagging requirements (Requisitos de etiquetado): las etiquetas necesarias para que los recursos asignen espacio del grupo. Si los recursos cambian sus etiquetas después de haber asignado espacio o si se modifican las reglas de etiquetado de asignación en el grupo, el recurso puede marcarse como no conforme.
- Locale (Configuración regional): la configuración regional que se requerirá para los recursos que utilizan CIDR de este grupo. Los recursos importados automáticamente que no tengan esta configuración regional se marcarán como no conformes. Los recursos que no se importan automáticamente al grupo no podrán asignar espacio desde el grupo a menos que se encuentren en esta configuración regional.

12. (Opcional) Elija Tags (Etiquetas) para el grupo.
13. Cuando haya terminado de configurar el grupo, elija Create pool (Crear grupo).

Antes de continuar, asegúrese de que este CIDR se haya aprovisionado. Puede ver el estado del aprovisionamiento en la pestaña CIDR en la página de detalles del grupo.

Paso 3. Comparta el grupo regional

Siga los pasos de esta sección para compartir el grupo de IPAM utilizando AWS Resource Access Manager (RAM).

Habilitar el uso compartido de recursos en AWS RAM

Después de crear su IPAM, podrá compartir el grupo regional con otras cuentas de su organización. Antes de compartir un grupo de IPAM, complete los pasos de esta sección para habilitar el uso compartido de recursos con AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`management-account`**.

Habilitar el uso compartido de recursos

1. Utilizando la cuenta de administración AWS Organizations, abra la consola AWS RAM en https://console.aws.amazon.com/ram/.
2. En el panel de navegación izquierdo, seleccione Configuración, seleccione Habilitar uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.

Ahora puede compartir un grupo de IPAM con otros miembros de la organización.

Compartir un grupo de IPAM mediante AWS RAM

En esta sección compartirá el grupo regional con otra cuenta de miembro de AWS Organizations. Para instrucciones completas sobre cómo compartir grupos de IPAM, incluyendo información sobre los permisos de IAM requeridos, consulte Compartir un grupo de IPAM mediante AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`ipam-account`**.

Compartir un grupo de IPAM mediante AWS RAM

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado, elija el grupo de IPAM y seleccione Acciones > Ver detalles.
4. En Resource sharing (Uso compartido de recursos), elija Create resource share (Crear recursos compartidos). Se abrirá la consola de AWS RAM. Se compartirá el grupo utilizando AWS RAM.
5. Elija Create a resource share (Crear un recurso compartido).
6. En la consola AWS RAM, seleccione de nuevo Crear un recurso compartido.
7. Añada un Nombre para el grupo compartido.
8. En Seleccionar tipo de recurso, elija Grupos de IPAM y, a continuación, seleccione el ARN del grupo que quieres compartir.
9. Elija Siguiente.
10. Elija el permiso AWSRAMPermissionIpamPoolByoipCidrImport. Los detalles de las opciones de permiso están fuera del marco de este tutorial, pero puede encontrar más información sobre estas opciones en Compartir un grupo de IPAM mediante AWS RAM.
11. Elija Siguiente.
12. En Entidades principales > Seleccionar tipo de entidad principal, elige Cuenta de AWS e ingresa el ID de la cuenta que proporcionará un rango de direcciones IP a IPAM y, a continuación, elige Agregar .
13. Elija Siguiente.
14. Revise las opciones de recurso compartido y las entidades principales con las que se compartirá y seleccione Crear.
15. Para permitir que la cuenta de **`member-account`** asigne CIDRS de direcciones IP desde el grupo de IPAM, cree un segundo recurso compartido con

`AWSRAMDefaultPermissionsIpamPool`. El valor para `--resource-arns` es el ARN del grupo de IPAM que creó en la sección anterior. El valor para `--principals` es el ID de cuenta del **`member-account`**. El valor para `--permission-arns` es el ARN del permiso `AWSRAMDefaultPermissionsIpamPool`.

Paso 4: Cree una VPC

Siga los pasos que aparecen en Creación de una VPC en la Guía del usuario de Amazon VPC.

La cuenta de miembro debe realizar este paso.

> **Note**
>
> - Cuando abre la VPC en la consola de administración de AWS, la Región de AWS en la que crea la VPC debe coincidir con la opción `Locale` que eligió cuando creó el grupo que se utilizará para el CIDR de BYOIP.
> - Cuando llegue al paso donde debe elegir un CIDR para la VPC, tendrá la opción de utilizar un CIDR de un grupo de IPAM. Elija el grupo regional que creó en este tutorial.

Cuando crea la VPC, AWS asigna un CIDR en el grupo de IPAM a la VPC. Podrá ver la asignación en IPAM cuando elija un grupo en el panel de contenido de la consola de IPAM y visualice la pestaña Allocations (Asignaciones) del grupo.

Paso 5: Anuncie el CIDR

La cuenta de IPAM debe realizar los pasos de esta sección. Una vez creada la VPC, puede comenzar a anunciar el CIDR que ha traído a AWS y se encuentra en el grupo con Service EC2 (EIP/VPC) (Servicio EC2 ([EIP/VPC]) configurado. En este tutorial, ese es su grupo regional. De forma predeterminada, el CIDR no se anuncia, lo que significa que no es accesible de manera pública a través de Internet.

La cuenta de IPAM debe realizar este paso.

Para anunciar el CIDR

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).

3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Seleccione el alcance público. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. Elija el grupo regional que creó en este tutorial.
5. Elija la pestaña CIDR.
6. Seleccione el CIDR de BYOIP y elija Actions (Acciones) > Advertise (Anunciar).
7. Elija Advertise CIDR (Anunciar CIDR).

Como resultado, se anuncia el CIDR de BYOIP y el valor en la columna Advertising (Anuncio) cambia de Withdrawn (Retirado) a Advertised (Anunciado).

Paso 6: Efectúe una limpieza

Siga los pasos de esta sección para eliminar los recursos que ha aprovisionado y creado en este tutorial.

Paso 1: Retire el CIDR del estado de anuncio

La cuenta de IPAM debe realizar este paso.

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. De forma predeterminada, al crear un grupo, se selecciona el alcance privado predeterminado. Seleccione el alcance público.
4. Elija el grupo regional que creó en este tutorial.
5. Elija la pestaña CIDR.
6. Seleccione el CIDR de BYOIP y elija Actions (Acciones) > Withdraw from advertising (Retirar del estado de anuncio).
7. Elija Withdraw CIDR (Retirar CIDR).

Como resultado, el CIDR de BYOIP ya no se anuncia y el valor en la columna Advertising (Anuncio) cambia de Advertised (Anunciado) a Withdrawn (Retirado).

Paso 2: Elimine la VPC

La cuenta de miembro debe realizar este paso.

- Siga los pasos que aparecen en Eliminación de una VPC en la Guía del usuario de Amazon VPC para eliminar la VPC. Cuando abre la VPC en la consola de administración de AWS, la Región de AWS en la que eliminó la VPC debe coincidir con la opción `Locale` que eligió cuando creó el grupo que utilizará para el CIDR de BYOIP. En este tutorial, ese grupo es su grupo regional.

  Cuando elimina la VPC, IPAM tarda en detectar que el recurso se ha eliminado, así como también en anular la asignación del CIDR que se había asignado a la VPC. No puede continuar con el siguiente paso de la limpieza hasta que la IPAM no haya eliminado la asignación del grupo en la pestaña Allocations (Asignaciones) en los detalles del grupo.

Paso 3: Elimine los recursos compartidos de RAM y desactive la integración de RAM con AWS Organizations

Este paso deben realizarlo las cuentas IPAM y de administración, respectivamente.

- Realice los pasos de la Eliminación de un recurso compartido en AWS RAM y Desactivación del uso compartido de recursos con AWS Organizaciones en la Guía del usuario de AWS RAM, en ese orden, para poder eliminar el recurso compartido de RAM y desactivar la integración de RAM con AWS Organizations.

Paso 4: Anule el aprovisionamiento de los CIDR del grupo regional y del grupo de nivel superior

La cuenta de IPAM debe realizar este paso.

- Siga los pasos en Anular el aprovisionamiento del CIDR de un grupo para anular el aprovisionamiento de los CIDR del grupo regional y, a continuación, del grupo de nivel superior, en ese orden.

Paso 5: Elimine el grupo regional y el grupo de nivel superior

La cuenta de IPAM debe realizar este paso.

- Siga los pasos de Eliminar un grupo para eliminar el grupo regional y, a continuación, el grupo de nivel superior, en ese orden.

Lleve su propio CIDR IP a IPAM únicamente por medio de la CLI AWS

Traiga su propia IP (BYOIP) al IPAM le permite utilizar los rangos de direcciones IPv4 e IPv6 existentes de su organización en AWS. Esto le permite mantener una imagen de marca coherente, mejorar el rendimiento de la red, mejorar la seguridad y simplificar la administración al unificar los entornos en las instalaciones y en la nube en su propio espacio de direcciones IP.

Siga estos pasos para llevar un CIDR IPv4 o IPv6 a IPAM únicamente por medio de la AWS CLI.

> **Note**
>
> Antes de comenzar, debe tener un control de dominio verificado.

Una vez que hayas llevado un rango de direcciones IPv4 a AWS, podrás usar todas las direcciones IP del rango, incluidas la primera dirección (la dirección de red) y la última dirección (la dirección de transmisión).

Contenido

Lleve su propio CIDR IPv4 público a IPAM únicamente por medio de la AWS CLI

Siga estos pasos para llevar un CIDR IPv4 a IPAM y asignar una dirección IP elástica (EIP) con el CIDR únicamente mediante el uso de AWS CLI.

> **Important**
>
> - En este tutorial, se presupone que ya ha completado los pasos que se detallan en las siguientes secciones:
>   - Integración de IPAM con cuentas en una organización de AWS.
>   - Creación de un IPAM.
> - Cada paso de este tutorial debe realizarse con una de tres cuentas de AWS Organizations:
>   - La cuenta de administración.

- La cuenta de miembro configurada para ser su administrador de IPAM en Integración de IPAM con cuentas en una organización de AWS. En este tutorial, esta cuenta se llamará cuenta de IPAM.
- La cuenta de miembro de su organización es la que asignará CIDR de un grupo de IPAM. En este tutorial, esta cuenta se llamará cuenta de miembro.

Contenido

Paso 1: Crear perfiles con nombre y roles de IAM de la AWS CLI

Para completar este tutorial como un usuario de AWS único, puede utilizar perfiles con nombre de AWS CLI para cambiar de un rol de IAM a otro. Los perfiles con nombre son conjuntos de configuraciones y credenciales a los que se hace referencia cuando se utiliza la opción `--profile` con la AWS CLI. Para obtener más información sobre cómo crear roles de IAM y perfiles con nombre para las cuentas de AWS, consulte Uso de un rol de IAM en la AWS CLI.

Cree un rol y un perfil con nombre para cada una de las tres cuentas de AWS que utilizará en este tutorial:

- Un perfil llamado `management-account` para la cuenta de administración de AWS Organizations.

- Un perfil llamado `ipam-account` para la cuenta de miembro de AWS Organizations que está configurada para ser su administrador de IPAM.
- Un perfil llamado `member-account` para la cuenta de miembro de AWS Organizations en su organización que asignará CIDR de un grupo de IPAM.

Después de crear los roles de IAM y los perfiles con nombre, regrese a esta página y vaya al paso siguiente. En el resto de este tutorial, observará que los comandos AWS CLI de ejemplo utilizan la opción `--profile` con uno de los perfiles con nombre para indicar qué cuenta debe ejecutar el comando.

Paso 2: Cree un IPAM

Este paso es opcional. Si ya tiene un IPAM creado con regiones operativas de `us-east-1` y `us-west-2` creadas, puede omitir este paso. Cree un IPAM y especifique una región operativa de `us-east-1` y `us-west-2`. Debe seleccionar una región operativa para poder utilizar la opción de configuración regional al crear su grupo de IPAM. La integración de IPAM con BYOIP requiere que la configuración regional se establezca en el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de IPAM debe realizar este paso.

Use el siguiente comando:

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

En la salida, verá el IPAM que creó. Anote el valor para `PublicDefaultScopeId`. Necesitará su ID de alcance público en el siguiente paso. Está utilizando el alcance público porque los CIDR de BYOIP son direcciones IP públicas, que es para lo que está destinado el alcance público.

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

Paso 3: Cree un grupo de IPAM de nivel superior

Complete los pasos de esta sección para crear un grupo de IPAM de nivel superior.

La cuenta de IPAM debe realizar este paso.

Para crear un grupo de direcciones IPv4 para todos los recursos de AWS con la AWS CLI

1. Ejecute el siguiente comando para crear un grupo de IPAM. Utilice el ID de alcance público del IPAM que creó en el paso anterior.

   La cuenta de IPAM debe realizar este paso.

   ```
   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
   ```

   En la salida, verá `create-in-progress`, lo que indica que la creación del grupo se encuentra en curso.

   ```
   {
       "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. Ejecute el siguiente comando hasta que vea el estado `create-complete` en la salida.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

La siguiente salida de ejemplo muestra el estado del grupo.

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

Paso 4: Aprovisione un CIDR en el grupo de nivel superior

Aprovisione un bloque de CIDR en el grupo de nivel superior. Tenga en cuenta que cuando aprovisione un CIDR IPv4 en un grupo dentro del grupo de nivel superior, el CIDR IPv4 mínimo que puede aprovisionar es `/24`; no se permiten CIDR más específicos (como `/25`).

> **Note**
>
> - Si verificó el control de su dominio con un certificado X.509, debe incluir el CIDR y el mensaje BYOIP y la firma del certificado que creó en ese paso para que podamos verificar que controla el espacio público.
> - Si verificó el control de su dominio con un registro TXT de DNS, debe incluir el CIDR y el token de verificación CIDR e IPAM que creó en ese paso para que podamos verificar que controla el espacio público.

Solo tiene que verificar el control del dominio cuando aprovisiona el CIDR de BYOIP en el grupo de nivel superior. En el grupo regional dentro del grupo de nivel superior, puede omitir la opción de verificación de propiedad del dominio.

La cuenta de IPAM debe realizar este paso.

> **Important**
>
> Solo tiene que verificar el control del dominio cuando aprovisiona el CIDR de BYOIP en el grupo de nivel superior. En el grupo regional dentro del grupo de nivel superior, puede omitir la opción de control del dominio. Una vez que haya incorporado su BYOIP a IPAM, no está obligado a realizar la validación de la propiedad cuando divide el BYOIP entre regiones y cuentas.

Para aprovisionar un bloque de CIDR en el grupo mediante la AWS CLI

1. Para proporcionar al CIDR la información del certificado, utilice el siguiente ejemplo de comando. Además de reemplazar los valores según sea necesario en el ejemplo, asegúrese de reemplazar los valores `Message` y `Signature` por los valores `text_message` y `signed_message` que ingresó en Verificación de su dominio con un certificado X.509.

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

```
du9pnEHBOX6WhoGYjWszPw0iV4cmaAX9DuMs8ASR83K127VvcBcRXElT5URr3gWEB1CQe3rmuyQk~gAdbXiDN-94-
oS9AZlafBbrFxRjFWRCTJhc7Cg3ASbRO-VWNci-
C~bWAPczbX3wPQSjtWGV3k1bGuD26ohUc02o8oJZQyYXRpgqcWGVJdQ__" --profile ipam-account
```

Para proporcionar al CIDR la información del token de verificación, utilice el siguiente ejemplo de comando. Además de reemplazar los valores según sea necesario en el ejemplo, asegúrese de reemplazar `ipam-ext-res-ver-token-0309ce7f67a768cf0` por el ID del token `IpamExternalResourceVerificationTokenId` que ingresó en Verificación de su dominio con un registro TXT de DNS.

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

En la salida, verá el CIDR pendiente de aprovisionamiento.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Antes de continuar, asegúrese de que este CIDR se haya aprovisionado.

> **Important**
>
> Si bien la mayoría del aprovisionamiento se completará en dos horas, el proceso de aprovisionamiento de los intervalos que se pueden anunciar públicamente puede tardar hasta una semana en completarse.

Ejecute el siguiente comando hasta que vea el estado `provisioned` en la salida.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

En la siguiente salida de ejemplo se muestra el estado.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

Paso 5: Cree un grupo regional dentro del grupo de nivel superior

Cree un grupo regional dentro del grupo de nivel superior.

En su lugar, realice una de las siguientes acciones:

- Una región de AWS en las que desea que este grupo de IPAM esté disponible para asignaciones.
- El grupo de límites de red de una zona AWS local en la que desea que este grupo de IPAM esté disponible para asignaciones (zonas locales compatibles). Esta opción solo está disponible para los grupos IPv4 de IPAM de ámbito público.
- Una zona AWS local dedicada. Para crear un grupo dentro de una zona AWS local dedicada, ingrese la zona AWS local dedicada en la entrada del selector.
- `Global` cuando desee utilizar direcciones IP de forma global en todas las regiones de AWS, como las ubicaciones de CloudFront. La configuración local `Global` solo está disponible para los grupos IPv4 públicos.

Por ejemplo, solo puede asignar un CIDR para una VPC desde un grupo de IPAM que comparte una configuración regional con la región de la VPC. Tenga en cuenta que, una vez elegida la configuración regional para un grupo, no puede modificarla. Si la región de origen de IPAM no está disponible debido a una interrupción y el grupo tiene una configuración regional diferente a la región de origen de IPAM, el grupo aún se puede usar para asignar direcciones IP.

Cuando ejecute los comandos de esta sección, el valor de `--region` debe coincidir con la opción `--locale` que ingresó cuando creó el grupo que se utilizará para el CIDR de BYOIP. Por ejemplo, si creó el grupo BYOIP con la configuración regional us-east-1, la `--region` debería ser us-east-1. Si creó el grupo BYOIP con la configuración regional us-east-1-scl-1 (un grupo de borde de red que se utiliza para las zonas locales), la `--region` debería ser us-east-1 porque esa región administra la configuración regional us-east-1-scl-1.

La cuenta de IPAM debe realizar este paso.

Elegir una configuración regional garantiza que no haya dependencias entre regiones entre su grupo y los recursos que se asignan desde él. Las opciones disponibles proceden de las regiones operativas que eligió al crear su IPAM. En este tutorial, utilizaremos `us-west-2` como escenario para el grupo regional.

> **Important**
>
> Al crear el grupo, debe incluir `--aws-service ec2`. El servicio que seleccione determina el servicio AWS donde el CIDR puede ser anunciado. Actualmente, la única opción es `ec2`, lo que significa que los CIDR asignados desde este grupo pueden ser anunciados en el servicio Amazon EC2 (para direcciones IP elásticas) y el servicio Amazon VPC (para CIDR asociados a VPC).

Para crear un grupo regional mediante la AWS CLI

1. Ejecute el siguiente comando para crear el grupo.

```
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
```

   En la salida, verá el IPAM que crea el grupo.

```
{
     "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. Ejecute el siguiente comando hasta que vea el estado `create-complete` en la salida.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

En la salida, verá los grupos que tiene en el IPAM. En este tutorial, hemos creado un grupo de nivel superior y un grupo regional, así que verá ambos.

Paso 6: Aprovisione un CIDR al grupo regional

Aprovisione un bloque de CIDR al grupo regional.

> **Note**
>
> Al aprovisionar un CIDR en un grupo regional dentro del grupo de nivel superior, el CIDR IPv4 más específico que puede aprovisionar es `/24`; no se permiten CIDR más específicos (como `/25`). Después de crear el grupo regional, podrá crear grupos más reducidos (como `/25`) dentro del mismo grupo regional. Tenga en cuenta que, si comparte el grupo o los grupos regionales dentro de este, estos grupos solo se podrán utilizar en la configuración regional establecida en el mismo grupo regional.

La cuenta de IPAM debe realizar este paso.

Para asignar un bloque de CIDR al grupo regional mediante la AWS CLI

1. Ejecute el siguiente comando para aprovisionar el 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
```

   En la salida, verá el CIDR pendiente de aprovisionamiento.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-provision"

    }

}
```

2. Ejecute el siguiente comando hasta que vea el estado `provisioned` en la salida.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   La siguiente salida de ejemplo muestra el estado correcto.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "State": "provisioned"
        }
    ]
}
```

Paso 7: Anunciar el CIDR

La cuenta de IPAM debe realizar los pasos de esta sección. Una vez que asocie la dirección IP elástica (EIP) a una instancia o un Elastic Load Balancer, podrá comenzar a anunciar el CIDR que

ha traído a AWS que está en el grupo y tiene `--aws-service ec2` definido. En este tutorial, ese es su grupo regional. De forma predeterminada, el CIDR no se anuncia, lo que significa que no es accesible de manera pública a través de Internet. Cuando ejecute el comando en esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de IPAM debe realizar este paso.

> **Note**
>
> El estado del anuncio no restringe su capacidad de asignar direcciones IP elásticas. Incluso si su CIDR de BYOIPv4 no está anunciado, puede crear EIP a partir del grupo del IPAM.

Comenzar a anunciar el CIDR mediante la AWS CLI

- Ejecute el siguiente comando para anunciar el CIDR.

  ```
  aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
  profile ipam-account
  ```

  En la salida, verá que se anuncia el CIDR.

  ```
  {
      "ByoipCidr": {
          "Cidr": "130.137.245.0/24",
          "State": "advertised"
      }
  }
  ```

Paso 8: uso compartido del grupo regional

Siga los pasos de esta sección para compartir el grupo de IPAM utilizando AWS Resource Access Manager (RAM).

Habilitar el uso compartido de recursos en AWS RAM

Después de crear su IPAM, podrá compartir el grupo regional con otras cuentas de su organización. Antes de compartir un grupo de IPAM, complete los pasos de esta sección para habilitar el uso

compartido de recursos con AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`management-account`**.

Habilitar el uso compartido de recursos

1. Utilizando la cuenta de administración AWS Organizations, abra la consola AWS RAM en https://console.aws.amazon.com/ram/.
2. En el panel de navegación izquierdo, seleccione Configuración, seleccione Habilitar uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.

Ahora puede compartir un grupo de IPAM con otros miembros de la organización.

Compartir un grupo de IPAM mediante AWS RAM

En esta sección compartirá el grupo regional con otra cuenta de miembro de AWS Organizations. Para instrucciones completas sobre cómo compartir grupos de IPAM, incluyendo información sobre los permisos de IAM requeridos, consulte Compartir un grupo de IPAM mediante AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`ipam-account`**.

Compartir un grupo de IPAM mediante AWS RAM

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado, elija el grupo de IPAM y seleccione Acciones > Ver detalles.
4. En Resource sharing (Uso compartido de recursos), elija Create resource share (Crear recursos compartidos). Se abrirá la consola de AWS RAM. Se compartirá el grupo utilizando AWS RAM.
5. Elija Create a resource share (Crear un recurso compartido).
6. En la consola AWS RAM, seleccione de nuevo Crear un recurso compartido.
7. Añada un Nombre para el grupo compartido.
8. En Seleccionar tipo de recurso, elija Grupos de IPAM y, a continuación, seleccione el ARN del grupo que quieres compartir.
9. Elija Siguiente.

10. Elija el permiso AWSRAMPermissionIpamPoolByoipCidrImport. Los detalles de las opciones de permiso están fuera del marco de este tutorial, pero puede encontrar más información sobre estas opciones en Compartir un grupo de IPAM mediante AWS RAM.
11. Elija Siguiente.
12. En Entidades principales > Seleccionar tipo de entidad principal, elige Cuenta de AWS e ingresa el ID de la cuenta que proporcionará un rango de direcciones IP a IPAM y, a continuación, elige Agregar .
13. Elija Siguiente.
14. Revise las opciones de recurso compartido y las entidades principales con las que se compartirá y seleccione Crear.
15. Para permitir que la cuenta de **`member-account`** asigne CIDRS de direcciones IP desde el grupo de IPAM, cree un segundo recurso compartido con `AWSRAMDefaultPermissionsIpamPool`. El valor para `--resource-arns` es el ARN del grupo de IPAM que creó en la sección anterior. El valor para `--principals` es el ID de cuenta del **`member-account`**. El valor para `--permission-arns` es el ARN del permiso `AWSRAMDefaultPermissionsIpamPool`.

Paso 9: asignación de una dirección IP elástica desde el grupo

Complete los pasos de esta sección para asignar una dirección IP elástica desde el grupo. Tenga en cuenta que si utiliza grupos de IPv4 públicos para asignar direcciones IP elásticas, puede seguir los pasos alternativos de Alternativa al paso 9 en lugar de los pasos de esta sección.

> **Important**
>
> Si aparece un error relacionado con la falta de permisos para llamar a ec2:AllocateAddress, se debe actualizar el permiso administrado actualmente asignado al grupo de IPAM que se le compartió. Póngase en contacto con la persona que creó el recurso compartido y pídale que actualice el permiso administrado `AWSRAMPermissionIpamResourceDiscovery` a la versión predeterminada. Para obtener más información, consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM.

AWS Management Console

Siga los pasos de Allocate an Elastic IP address en la Guía del usuario de Amazon EC2 para asignar la dirección, pero tenga en cuenta lo siguiente:

- La cuenta de miembro debe realizar este paso.
- Asegúrese de que la región de AWS en la que se encuentra en la consola de EC2 coincida con la opción de configuración regional que eligió al crear el grupo regional.
- Al elegir el grupo de direcciones, seleccione la opción Asignar mediante un grupo de IPAM IPv4 y elija el grupo regional que creó.

Command line

Asigne una dirección del grupo con el comando allocate-address. El valor de `--region` que utilice debe coincidir con la opción `-locale` que eligió al crear el grupo en el paso 2. Incluya el ID del grupo del IPAM que creó en el paso 2 en `--ipam-pool-id`. Si lo desea, también puede elegir un `/32` específico de su grupo de IPAM mediante la opción `--address`.

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

Respuesta de ejemplo:

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

Para obtener más información, consulte Allocate an Elastic IP address en la Guía del usuario de Amazon EC2.

Paso 10: asociación de la dirección IP elástica a una instancia de EC2

Complete los pasos de esta sección a fin de asociar la dirección IP elástica a una instancia de EC2.

AWS Management Console

Siga los pasos de Associate an Elastic IP address en la Guía del usuario de Amazon EC2 para asignar una dirección IP elástica del grupo del IPAM, pero tenga en cuenta lo siguiente: cuando utilice la opción de la Consola de administración de AWS, la región de AWS a la que asocie la

dirección IP elástica debe coincidir con la opción de configuración regional que eligió al crear el grupo regional.

La cuenta de miembro debe realizar este paso.

Command line

La cuenta de miembro debe realizar este paso. Use la opción `--profile` **`member-account`**.

Asocie la dirección IP elástica a una instancia con el comando associate-address. El valor de `--region` al que asocia la dirección IP elástica debe coincidir con la opción `--locale` que eligió cuando creó el grupo regional.

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

Respuesta de ejemplo:

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

Para obtener más información, consulte Asociación de una dirección IP elástica a una instancia o una interfaz de red en la Guía del usuario de Amazon EC2.

Paso 11: Efectúe una limpieza

Siga los pasos de esta sección para eliminar los recursos que ha aprovisionado y creado en este tutorial. Cuando ejecute los comandos de esta sección, el valor de `--region` debe coincidir con la opción `--locale` que ingresó cuando creó el grupo que se utilizará para el CIDR de BYOIP.

Eliminar recursos mediante AWS CLI

1. Vea la asignación EIP administrada en IPAM.

   La cuenta de IPAM debe realizar este paso.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

La salida muestra la asignación en 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. No anuncie el CIDR IPv4.

   La cuenta de IPAM debe realizar este paso.

   ```
   aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 130.137.245.0/24 --
   profile ipam-account
   ```

   En la salida, verá que el estado CIDR ha cambiado de advertised (anunciado) a provisioned (aprovisionado).

   ```
   {
       "ByoipCidr": {
           "Cidr": "130.137.245.0/24",
           "State": "provisioned"
       }
   }
   ```

3. Lance la dirección IP elástica.

   La cuenta de miembro debe realizar este paso.

   ```
   aws ec2 release-address --region us-west-2 --allocation-
   id eipalloc-0db3405026756dbf6 --profile member-account
   ```

   Cuando ejecute este comando no verá resultados.

4. Vea la asignación EIP que ya no se administra en IPAM. IPAM puede tardar un poco en determinar que la dirección IP elástica se haya eliminado. No puede continuar con la eliminación y anulación de aprovisionamiento del CIDR en el grupo de IPAM hasta que vea que la asignación se ha eliminado de IPAM. Cuando ejecute el comando en esta sección, el valor de la `--region` debe incluir la opción `--locale` que ingresó cuando creó el grupo que se utilizará para el CIDR de BYOIP.

   La cuenta de IPAM debe realizar este paso.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0d8f3646b61ca5987 --profile ipam-account
   ```

   La salida muestra la asignación en IPAM.

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

5. Anule el aprovisionamiento del CIDR de grupo regional. Cuando ejecute los comandos de este paso, el valor de `--region` debe coincidir con la región de su IPAM.

   La cuenta de IPAM debe realizar este paso.

   ```
   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
   ```

   En la salida verá la anulación del aprovisionamiento pendiente de CIDR.

   ```
   {
       "IpamPoolCidr": {

           "Cidr": "130.137.245.0/24",

           "State": "pending-deprovision"

       }

   }
   ```

La anulación del aprovisionamiento tarda un tiempo en completarse. Compruebe el estado de la anulación del aprovisionamiento.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

Espere a que el estado sea Deprovisioned (Aprovisionamiento anulado) antes de continuar con el siguiente paso.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

6. Elimine los recursos compartidos de RAM y desactive la integración de RAM con AWS Organizations. Complete los pasos descritos en Eliminación de un recurso compartido en AWS RAM y, a continuación, en Desactivación del uso compartido de recursos con AWS Organizations, en la Guía del usuario de AWS RAM, en ese orden, para eliminar los recursos compartidos de RAM y desactivar la integración de RAM con AWS Organizations.

   Este paso deben realizarlo las cuentas IPAM y de administración, respectivamente. Si utiliza AWS CLI para eliminar los recursos compartidos de RAM y desactivar la integración de RAM, utilice las opciones `--profile` **`ipam-account`** y `--profile` **`management-account`**.

7. Elimine el grupo regional. Cuando ejecute el comando en este paso, el valor de `--region` debe coincidir con la región de su IPAM.

   La cuenta de IPAM debe realizar este paso.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

   En la salida, puede ver el estado de eliminación.

```
{
   "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0d8f3646b61ca5987",
        "SourceIpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0d8f3646b61ca5987",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "reg-ipv4-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

8. Anule el aprovisionamiento del CIDR del grupo de nivel superior. Cuando ejecute los comandos de este paso, el valor de `--region` debe coincidir con la región de su IPAM.

   La cuenta de IPAM debe realizar este paso.

```
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
```

   En la salida verá la anulación del aprovisionamiento pendiente de CIDR.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "pending-deprovision"

    }

}
```

La anulación del aprovisionamiento tarda un tiempo en completarse. Ejecute el siguiente comando para verificar el estado del desaprovisionamiento.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

Espere a que el estado sea deprovisioned (con el aprovisionamiento anulado) antes de continuar con el siguiente paso.

```
{
    "IpamPoolCidr": {

        "Cidr": "130.137.245.0/24",

        "State": "deprovisioned"

    }

}
```

9. Elimine el grupo de nivel superior. Cuando ejecute el comando en este paso, el valor de `--region` debe coincidir con la región de su IPAM.

   La cuenta de IPAM debe realizar este paso.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0a03d430ca3f5c035 --profile ipam-account
```

   En la salida, puede ver el estado de eliminación.

```
{
  "IpamPool": {
        "OwnerId": "123456789012",
        "IpamPoolId": "ipam-pool-0a03d430ca3f5c035",
        "IpamPoolArn": "arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-0a03d430ca3f5c035",
        "IpamScopeArn": "arn:aws:ec2::123456789012:ipam-scope/ipam-
scope-0087d83896280b594",
        "IpamScopeType": "public",
```

```
        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "Locale": "us-east-1",
        "PoolDepth": 2,
        "State": "delete-in-progress",
        "Description": "top-level-pool",
        "AutoImport": false,
        "Advertisable": true,
        "AddressFamily": "ipv4"
    }
}
```

10. Elimine el IPAM. Cuando ejecute el comando en este paso, el valor de `--region` debe coincidir con la región de su IPAM.

    La cuenta de IPAM debe realizar este paso.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    En la salida verá la respuesta de IPAM. Esto significa que se ha eliminado el IPAM.

```
{
    "Ipam": {
        "OwnerId": "123456789012",
        "IpamId": "ipam-090e48e75758de279",

        "IpamArn": "arn:aws:ec2::123456789012:ipam/ipam-090e48e75758de279",
        "PublicDefaultScopeId": "ipam-scope-0087d83896280b594",

        "PrivateDefaultScopeId": "ipam-scope-08b70b04fbd524f8d",

        "ScopeCount": 2,

        "OperatingRegions": [

            {

                "RegionName": "us-east-1"

            },
            {
                "RegionName": "us-west-2"
            }
```

```
        ],
    }
}
```

Alternativa al paso 9

Si utiliza grupos de IPv4 públicos para asignar direcciones IP elásticas, puede seguir los pasos de esta sección en lugar de los pasos de Paso 9: asignación de una dirección IP elástica desde el grupo.

Contenido

Paso 1: creación de un grupo de IPv4 público

Por lo general, este paso lo lleva a cabo otra cuenta de AWS que desea aprovisionar una dirección IP elástica, como la cuenta de miembro.

> **Important**
>
> Los grupos IPv4 públicos y los grupos de IPAM se administran mediante distintos recursos en AWS. Los grupos IPv4 públicos son recursos de una sola cuenta que le permiten convertir sus CIDR de propiedad pública en direcciones IP elásticas. Los grupos de IPAM se pueden utilizar para asignar el espacio público a grupos IPv4 públicos.

Para crear un grupo IPv4 público mediante la AWS CLI

- Ejecute el siguiente comando para aprovisionar el CIDR. Al ejecutar el comando en esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo que se utilizará para el CIDR de BYOIP.

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

En la salida aparecerá el ID del grupo IPv4 público. Necesitará este ID en el siguiente paso.

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

Paso 2: aprovisionamiento del CIDR de IPv4 público en el grupo de IPv4 público

Aprovisione el CIDR IPv4 público en su grupo IPv4 público. El valor de `--region` debe coincidir con el valor de `--locale` que introdujo al crear el grupo que se utilizará para el CIDR de BYOIP. El `--netmask-length` menos específico que puede definir es `24`.

La cuenta de miembro debe realizar este paso.

Para crear un grupo IPv4 público mediante la AWS CLI

1. Ejecute el siguiente comando para aprovisionar el 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
```

   En la salida aparecerá el CIDR aprovisionado.

```
{
    "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
    "PoolAddressRange": {
        "FirstAddress": "130.137.245.0",
        "LastAddress": "130.137.245.255",
        "AddressCount": 256,
        "AvailableAddressCount": 256
    }
}
```

2. Ejecute el siguiente comando para ver el CIDR aprovisionado en el grupo IPv4 público.

```
aws ec2 describe-byoip-cidrs --region us-west-2 --max-results 10 --profile member-
account
```

En la salida aparecerá el CIDR aprovisionado. De forma predeterminada, el CIDR no se anuncia, lo que significa que no es accesible de manera pública a través de Internet. Tendrá la oportunidad de configurar este CIDR como anunciado en el último paso de este tutorial.

```
{
    "ByoipCidrs": [
        {
            "Cidr": "130.137.245.0/24",
            "StatusMessage": "Cidr successfully provisioned",
            "State": "provisioned"
        }
    ]
}
```

Paso 3: creación de una dirección IP elástica desde el grupo de IPv4 público

Cree una dirección IP elástica (EIP) desde el grupo IPv4 público. Cuando ejecute los comandos de esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de miembro debe realizar este paso.

Para crear una EIP desde el grupo IPv4 público mediante la AWS CLI

1. Ejecute el siguiente comando para crear la EIP.

```
aws ec2 allocate-address  --region us-west-2 --public-ipv4-pool ipv4pool-
ec2-0019eed22a684e0b2 --profile member-account
```

   En la salida aparecerá la asignación.

```
{
    "PublicIp": "130.137.245.100",
    "AllocationId": "eipalloc-0db3405026756dbf6",
    "PublicIpv4Pool": "ipv4pool-ec2-0019eed22a684e0b2",
    "NetworkBorderGroup": "us-east-1",
    "Domain": "vpc"
}
```

2. Ejecute el siguiente comando para ver la asignación de EIP administrada en IPAM.

La cuenta de IPAM debe realizar este paso.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0d8f3646b61ca5987 --profile ipam-account
```

La salida muestra la asignación en IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.245.0/24",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc45",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b2",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Alternativa a la limpieza del paso 9

Complete estos pasos para limpiar los grupos de IPv4 públicos creados con la alternativa al paso 9. Debe completar estos pasos después de liberar la dirección IP elástica durante el proceso de limpieza estándar en Paso 10: Eliminar.

1. Vea los CIDR de BYOIP.

   La cuenta de miembro debe realizar este paso.

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

   En la salida aparecerán las direcciones IP de su CIDR de BYOIP.

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
               "Description": "",
   ```

```
            "PoolAddressRanges": [
                {
                    "FirstAddress": "130.137.245.0",
                    "LastAddress": "130.137.245.255",
                    "AddressCount": 256,
                    "AvailableAddressCount": 256
                }
            ],
            "TotalAddressCount": 256,
            "TotalAvailableAddressCount": 256,
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

2. Lance el CIDR del grupo IPv4 público. Cuando ejecute el comando en esta sección, el valor de `--region` debe coincidir con la región de su IPAM.

   La cuenta de miembro debe realizar este paso.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1 --pool-id ipv4pool-
ec2-0019eed22a684e0b2 --cidr 130.137.245.0/24 --profile member-account
```

3. Vuelva a ver sus CIDR de BYOIP y asegúrese de que no haya más direcciones aprovisionadas. Cuando ejecute el comando en esta sección, el valor de `--region` debe coincidir con la región de su IPAM.

   La cuenta de miembro debe realizar este paso.

```
aws ec2 describe-public-ipv4-pools --region us-east-1 --profile member-account
```

   En la salida aparecerá el recuento de direcciones IP en el grupo IPv4 público.

```
{
    "PublicIpv4Pools": [
        {
            "PoolId": "ipv4pool-ec2-0019eed22a684e0b2",
            "Description": "",
            "PoolAddressRanges": [],
            "TotalAddressCount": 0,
            "TotalAvailableAddressCount": 0,
```

```
            "NetworkBorderGroup": "us-east-1",
            "Tags": []
        }
    ]
}
```

Lleve su propio CIDR IPv6 a IPAM únicamente por medio de la AWS CLI

Siga estos pasos para llevar un CIDR IPv6 a IPAM y asignar una VPC únicamente mediante el uso de AWS CLI.

Si no necesita anunciar sus direcciones IPv6 a través de Internet, puede aprovisionar una dirección IPv6 GUA privada a un IPAM. Para obtener más información, consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados.

Important

- En este tutorial, se presupone que ya ha completado los pasos que se detallan en las siguientes secciones:
  - Integración de IPAM con cuentas en una organización de AWS.
  - Creación de un IPAM.
- Cada paso de este tutorial debe realizarse con una de tres cuentas de AWS Organizations:
  - La cuenta de administración.
  - La cuenta de miembro configurada para ser su administrador de IPAM en Integración de IPAM con cuentas en una organización de AWS. En este tutorial, esta cuenta se llamará cuenta de IPAM.
  - La cuenta de miembro de su organización es la que asignará CIDR de un grupo de IPAM. En este tutorial, esta cuenta se llamará cuenta de miembro.

Contenido

Paso 1: Crear perfiles con nombre y roles de IAM de la AWS CLI

Para completar este tutorial como un usuario de AWS único, puede utilizar perfiles con nombre de AWS CLI para cambiar de un rol de IAM a otro. Los perfiles con nombre son conjuntos de configuraciones y credenciales a los que se hace referencia cuando se utiliza la opción `--profile` con la AWS CLI. Para obtener más información sobre cómo crear roles de IAM y perfiles con nombre para las cuentas de AWS, consulte Uso de un rol de IAM en la AWS CLI.

Cree un rol y un perfil con nombre para cada una de las tres cuentas de AWS que utilizará en este tutorial:

- Un perfil llamado `management-account` para la cuenta de administración de AWS Organizations.
- Un perfil llamado `ipam-account` para la cuenta de miembro de AWS Organizations que está configurada para ser su administrador de IPAM.
- Un perfil llamado `member-account` para la cuenta de miembro de AWS Organizations en su organización que asignará CIDR de un grupo de IPAM.

Después de crear los roles de IAM y los perfiles con nombre, regrese a esta página y vaya al paso siguiente. En el resto de este tutorial, observará que los comandos AWS CLI de ejemplo utilizan la opción `--profile` con uno de los perfiles con nombre para indicar qué cuenta debe ejecutar el comando.

Paso 2: Cree un IPAM

Este paso es opcional. Si ya tiene un IPAM creado con regiones operativas de `us-east-1` y `us-west-2` creadas, puede omitir este paso. Cree un IPAM y especifique una región operativa de `us-east-1` y `us-west-2`. Debe seleccionar una región operativa para poder utilizar la opción de configuración regional al crear su grupo de IPAM. La integración de IPAM con BYOIP requiere que la configuración regional se establezca en el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de IPAM debe realizar este paso.

Use el siguiente comando:

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

En la salida, verá el IPAM que creó. Anote el valor para `PublicDefaultScopeId`. Necesitará su ID de alcance público en el siguiente paso.

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

Paso 3: Cree un grupo de IPAM

Dado que creará un grupo de IPAM de nivel superior que incluirá un grupo regional, y que asignaremos espacio a un recurso (una VPC) desde el grupo regional, debe establecer la configuración regional en el grupo regional y no en el grupo de nivel superior. Agregará la configuración regional al grupo regional cuando cree dicho grupo en un paso posterior. La integración de IPAM con BYOIP requiere que la configuración regional se establezca en el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de IPAM debe realizar este paso.

Elija si desea que AWS pueda anunciar este CIDR del grupo de IPAM a través de la Internet pública (`--publicly-advertisable` o `--no-publicly-advertisable`).

> **Note**
>
> Tenga en cuenta que el ID de alcance debe ser el ID de alcance público y la familia de direcciones debe ser `ipv6`.

Para crear un grupo de direcciones IPv6 para todos los recursos de AWS con la AWS CLI

1. Ejecute el siguiente comando para crear un grupo de IPAM. Utilice el ID de alcance público del IPAM que creó en el paso anterior.

   ```
   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
   ```

   En la salida, verá `create-in-progress`, lo que indica que la creación del grupo se encuentra en curso.

   ```
   {
       "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. Ejecute el siguiente comando hasta que vea el estado `create-complete` en la salida.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

La siguiente salida de ejemplo muestra el estado del grupo.

```
{
    "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": []

    }

}
```

Paso 4: Aprovisione un CIDR en el grupo de nivel superior

Aprovisione un bloque de CIDR en el grupo de nivel superior. Tenga en cuenta que al aprovisionar un IPv6 CIDR a un grupo dentro del grupo de nivel superior, el intervalo de direcciones IPv6 más específico que puede traer es /48 para los CIDR que se anuncian públicamente y /60 para los CIDR que no se anuncian públicamente.

> **Note**
>
> - Si verificó el control de su dominio con un certificado X.509, debe incluir el CIDR y el mensaje BYOIP y la firma del certificado que creó en ese paso para que podamos verificar que controla el espacio público.
> - Si verificó el control de su dominio con un registro TXT de DNS, debe incluir el CIDR y el token de verificación CIDR e IPAM que creó en ese paso para que podamos verificar que controla el espacio público.

Solo tiene que verificar el control del dominio cuando aprovisiona el CIDR de BYOIP en el grupo de nivel superior. En el grupo regional dentro del grupo de nivel superior, puede omitir la opción de dominio.

La cuenta de IPAM debe realizar este paso.

Para aprovisionar un bloque de CIDR en el grupo mediante la AWS CLI

1. Para proporcionar al CIDR la información del certificado, utilice el siguiente ejemplo de comando. Además de reemplazar los valores según sea necesario en el ejemplo, asegúrese

de reemplazar los valores `Message` y `Signature` por los valores `text_message` y `signed_message` que ingresó en Verificación de su dominio con un certificado X.509.

```
aws ec2 provision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --verification-method remarks-
x509 --cidr-authorization-context Message="1|aws|470889052444|2605:9cc0:409::/48|
20250101|SHA256|RSAPSS",Signature="FU26~vRG~NUGXa~akxd6dvdcCfvL88g8d~YAuai-
CR7HqMwzcgdS9RlpBGtfIdsRGyr77LmWyWqU9Xp1g2R1kSkfD00NiLKLcv9F63k6wdEkyFxNp7RAJDvF1mBwxmSgH~C
Vp6LON3yOOXMp4JENB9uM7sMlu6oeoutGyyhXFeYPzlGSRdcdfKNKaimvPCqVsxGN5AwSilKQ8byNqoa~G3dvs8ueSa
wispI~r69fq515UR19TA~fmmxBDh1huQ8DkM1rqcwveWow__" --profile ipam-account
```

Para proporcionar al CIDR la información del token de verificación, utilice el siguiente ejemplo de comando. Además de reemplazar los valores según sea necesario en el ejemplo, asegúrese de reemplazar `ipam-ext-res-ver-token-0309ce7f67a768cf0` por el ID del token `IpamExternalResourceVerificationTokenId` que ingresó en Verificación de su dominio con un registro TXT de DNS.

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

En la salida, verá el CIDR pendiente de aprovisionamiento.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "pending-provision"

    }

}
```

2. Antes de continuar, asegúrese de que este CIDR se haya aprovisionado.

> **Important**
>
> Si bien la mayoría del aprovisionamiento se completará en dos horas, el proceso de aprovisionamiento de los intervalos que se pueden anunciar públicamente puede tardar hasta una semana en completarse.

Ejecute el siguiente comando hasta que vea el estado `provisioned` en la salida.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

En la siguiente salida de ejemplo se muestra el estado.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Paso 5: Cree un grupo regional dentro del grupo de nivel superior

Cree un grupo regional dentro del grupo de nivel superior. El campo `--locale` es obligatorio en el grupo y debe ser una de las regiones operativas que configuró al crear el IPAM.

La cuenta de IPAM debe realizar este paso.

> **Important**
>
> Al crear el grupo, debe incluir `--aws-service ec2`. El servicio que seleccione determina el servicio AWS donde el CIDR puede ser anunciado. En la actualidad, la única opción es `ec2`, lo que significa que los CIDR asignados desde este grupo pueden ser anunciados en los servicios Amazon EC2 y Amazon VPC (para los CIDR asociados a VPC).

Para crear un grupo regional mediante la AWS CLI

1. Ejecute el siguiente comando para crear el grupo.

```
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
```

   En la salida, verá el IPAM que crea el grupo.

```
{
    "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. Ejecute el siguiente comando hasta que vea el estado `create-complete` en la salida.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

   En la salida, verá los grupos que tiene en el IPAM. En este tutorial, hemos creado un grupo de nivel superior y un grupo regional, así que verá ambos.

Paso 6: Aprovisione un CIDR al grupo regional

Aprovisione un bloque de CIDR al grupo regional. Tenga en cuenta que al aprovisionar el CIDR a un grupo dentro del grupo de nivel superior, el intervalo de direcciones IPv6 más específico que puede traer es /48 para los CIDR que se anuncian públicamente y /60 para los CIDR que no se anuncian públicamente.

La cuenta de IPAM debe realizar este paso.

Para asignar un bloque de CIDR al grupo regional mediante la AWS CLI

1. Ejecute el siguiente comando para aprovisionar el 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
```

   En la salida, verá el CIDR pendiente de aprovisionamiento.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-provision"
    }
}
```

2. Ejecute el siguiente comando hasta que vea el estado `provisioned` en la salida.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   La siguiente salida de ejemplo muestra el estado correcto.

```
{
    "IpamPoolCidrs": [
        {
            "Cidr": "2605:9cc0:409::/48",
            "State": "provisioned"
        }
    ]
}
```

Paso 7. Comparta el grupo regional

Siga los pasos de esta sección para compartir el grupo de IPAM utilizando AWS Resource Access Manager (RAM).

Habilitar el uso compartido de recursos en AWS RAM

Después de crear su IPAM, podrá compartir el grupo regional con otras cuentas de su organización. Antes de compartir un grupo de IPAM, complete los pasos de esta sección para habilitar el uso compartido de recursos con AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`management-account`**.

Habilitar el uso compartido de recursos

1. Utilizando la cuenta de administración AWS Organizations, abra la consola AWS RAM en https://console.aws.amazon.com/ram/.
2. En el panel de navegación izquierdo, seleccione Configuración, seleccione Habilitar uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.

Ahora puede compartir un grupo de IPAM con otros miembros de la organización.

Compartir un grupo de IPAM mediante AWS RAM

En esta sección compartirá el grupo regional con otra cuenta de miembro de AWS Organizations. Para instrucciones completas sobre cómo compartir grupos de IPAM, incluyendo información sobre los permisos de IAM requeridos, consulte Compartir un grupo de IPAM mediante AWS RAM. Si utiliza la AWS CLI para habilitar el uso compartido de recursos, utilice la opción `--profile` **`ipam-account`**.

Compartir un grupo de IPAM mediante AWS RAM

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado, elija el grupo de IPAM y seleccione Acciones > Ver detalles.
4. En Resource sharing (Uso compartido de recursos), elija Create resource share (Crear recursos compartidos). Se abrirá la consola de AWS RAM. Se compartirá el grupo utilizando AWS RAM.
5. Elija Create a resource share (Crear un recurso compartido).

6. En la consola AWS RAM, seleccione de nuevo Crear un recurso compartido.
7. Añada un Nombre para el grupo compartido.
8. En Seleccionar tipo de recurso, elija Grupos de IPAM y, a continuación, seleccione el ARN del grupo que quieres compartir.
9. Elija Siguiente.
10. Elija el permiso AWSRAMPermissionIpamPoolByoipCidrImport. Los detalles de las opciones de permiso están fuera del marco de este tutorial, pero puede encontrar más información sobre estas opciones en Compartir un grupo de IPAM mediante AWS RAM.
11. Elija Siguiente.
12. En Entidades principales > Seleccionar tipo de entidad principal, elige Cuenta de AWS e ingresa el ID de la cuenta que proporcionará un rango de direcciones IP a IPAM y, a continuación, elige Agregar .
13. Elija Siguiente.
14. Revise las opciones de recurso compartido y las entidades principales con las que se compartirá y seleccione Crear.
15. Para permitir que la cuenta de **`member-account`** asigne CIDRS de direcciones IP desde el grupo de IPAM, cree un segundo recurso compartido con `AWSRAMDefaultPermissionsIpamPool`. El valor para `--resource-arns` es el ARN del grupo de IPAM que creó en la sección anterior. El valor para `--principals` es el ID de cuenta del **`member-account`**. El valor para `--permission-arns` es el ARN del permiso `AWSRAMDefaultPermissionsIpamPool`.

Paso 8: Cree una VPC mediante el CIDR IPv6

Cree una VPC mediante el ID de grupo de IPAM. Debe asociar un bloque de CIDR IPv4 a la VPC mediante el `--cidr-block` o fallará la solicitud. Al ejecutar el comando en esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo que se utilizará para el CIDR de BYOIP.

La cuenta de miembro debe realizar este paso.

Para crear una VPC con el CIDR IPv6 mediante la AWS CLI

1. Ejecute el siguiente comando para aprovisionar el 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
```

En la salida, verá que se está creando la VPC.

```
{
    "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. Vea la asignación de VPC en IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

En la salida, verá la asignación en IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "2605:9cc0:409::/56",
            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",
            "ResourceType": "vpc",
            "ResourceOwner": "123456789012"
        }
    ]
}
```

Paso 9: Anunciar el CIDR

Una vez que se haya creado la VPC con el CIDR asignado en IPAM, puede comenzar a anunciar el CIDR que ha traído a AWS, que se encuentra en el grupo que tiene definido `--aws-service ec2`. En este tutorial, ese es su grupo regional. De forma predeterminada, el CIDR no se anuncia, lo que significa que no es accesible de manera pública a través de Internet. Al ejecutar el comando en esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo regional que se utilizará para el CIDR de BYOIP.

La cuenta de IPAM debe realizar este paso.

Comenzar a anunciar el CIDR mediante la AWS CLI

- Ejecute el siguiente comando para anunciar el CIDR.

```
aws ec2 advertise-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

En la salida, verá que se anuncia el CIDR.

```
{
```

```
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "advertised"
    }
}
```

Paso 10: Eliminar

Siga los pasos de esta sección para eliminar los recursos que ha aprovisionado y creado en este tutorial. Al ejecutar los comandos en esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo regional que se utilizará para el CIDR de BYOIP.

Eliminar recursos mediante la AWS CLI

1. Ejecute el siguiente comando para ver la asignación de VPC administrada en IPAM.

   La cuenta de IPAM debe realizar este paso.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   La salida muestra la asignación en IPAM.

   ```
   {
       "IpamPoolAllocations": [
           {
               "Cidr": "2605:9cc0:409::/56",
               "IpamPoolAllocationId": "ipam-pool-
   alloc-5f8db726fb9e4ff0a33836e649283a52",
               "ResourceId": "vpc-00b5573ffc3b31a29",
               "ResourceType": "vpc",
               "ResourceOwner": "123456789012"
           }
       ]
   }
   ```

2. Ejecute el siguiente comando para dejar de anunciar el CIDR. Al ejecutar el comando en este paso, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo regional que se utilizará para el CIDR de BYOIP.

   La cuenta de IPAM debe realizar este paso.

```
aws ec2 withdraw-byoip-cidr --region us-west-2 --cidr 2605:9cc0:409::/48 --
profile ipam-account
```

En la salida, verá que el estado CIDR ha cambiado de advertised (anunciado) a provisioned (aprovisionado).

```
{
    "ByoipCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "provisioned"
    }
}
```

3. Ejecute el siguiente comando para eliminar la VPC. Al ejecutar el comando en esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo regional que se utilizará para el CIDR de BYOIP.

   La cuenta de miembro debe realizar este paso.

   ```
   aws ec2 delete-vpc --region us-west-2 --vpc-id vpc-00b5573ffc3b31a29 --
   profile member-account
   ```

   Cuando ejecute este comando no verá resultados.

4. Ejecute el siguiente comando para ver la asignación de VPC en IPAM. IPAM puede tardar en descubrir que se ha eliminado la VPC y quitado esta asignación. Al ejecutar los comandos en esta sección, el valor de `--region` debe coincidir con la opción `--locale` que introdujo cuando creó el grupo regional que se utilizará para el CIDR de BYOIP.

   La cuenta de IPAM debe realizar este paso.

   ```
   aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
   pool-0053b7d2b4fc3f730 --profile ipam-account
   ```

   La salida muestra la asignación en IPAM.

   ```
   {
      "IpamPoolAllocations": [
   ```

```
        {

            "Cidr": "2605:9cc0:409::/56",

            "IpamPoolAllocationId": "ipam-pool-
alloc-5f8db726fb9e4ff0a33836e649283a52",
            "ResourceId": "vpc-00b5573ffc3b31a29",

            "ResourceType": "vpc",

            "ResourceOwner": "123456789012"

        }

    ]

}
```

Vuelva a ejecutar el comando y busque la asignación que se eliminará. No puede continuar con la eliminación y anulación de aprovisionamiento del CIDR en el grupo de IPAM hasta que vea que la asignación se ha eliminado de IPAM.

```
aws ec2 get-ipam-pool-allocations --region us-west-2 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

La salida muestra la asignación que se ha eliminado de IPAM.

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

5. Elimine los recursos compartidos de RAM y desactive la integración de RAM con AWS Organizations. Realice los pasos de la Eliminación de un recurso compartido en AWS RAM y Desactivación del uso compartido de recursos con AWS Organizaciones en la Guía del usuario de AWS RAM, en ese orden, para poder eliminar el recurso compartido de RAM y desactivar la integración de RAM con AWS Organizations.

   Este paso deben realizarlo las cuentas IPAM y de administración, respectivamente. Si utiliza AWS CLI para eliminar los recursos compartidos de RAM y desactivar la integración de RAM, utilice las opciones `--profile ipam-account` y `--profile management-account`.

6. Ejecute el siguiente comando para anular el aprovisionamiento del grupo regional de CIDR.

   La cuenta de IPAM debe realizar este paso.

```
aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   En la salida verá la anulación del aprovisionamiento pendiente de CIDR.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "pending-deprovision"
    }
}
```

   La anulación del aprovisionamiento tarda un tiempo en completarse. Continúe con la ejecución del comando hasta que vea el estado de CIDR deprovisioned (desaprovisionado).

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --cidr 2605:9cc0:409::/48 --profile ipam-account
```

   En la salida verá la anulación del aprovisionamiento pendiente de CIDR.

```
{
    "IpamPoolCidr": {
        "Cidr": "2605:9cc0:409::/48",
        "State": "deprovisioned"
    }
}
```

7. Ejecute el siguiente comando para eliminar el grupo regional.

   La cuenta de IPAM debe realizar este paso.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-0053b7d2b4fc3f730 --profile ipam-account
```

   En la salida, puede ver el estado de eliminación.

```
{
    "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. Ejecute el siguiente comando para anular el aprovisionamiento el grupo de nivel superior de CIDR.

   La cuenta de IPAM debe realizar este paso.

   ```
   aws ec2 deprovision-ipam-pool-cidr --region us-east-1 --ipam-pool-id ipam-
   pool-07f2466c7158b50c4 --cidr 2605:9cc0:409::/48 --profile ipam-account
   ```

   En la salida verá la anulación del aprovisionamiento pendiente de CIDR.

   ```
   {
       "IpamPoolCidr": {
           "Cidr": "2605:9cc0:409::/48",
           "State": "pending-deprovision"
       }
   }
   ```

   La anulación del aprovisionamiento tarda un tiempo en completarse. Ejecute el siguiente comando para verificar el estado del desaprovisionamiento.

```
aws ec2 get-ipam-pool-cidrs --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

Espere a que el estado sea deprovisioned (con el aprovisionamiento anulado) antes de continuar con el siguiente paso.

```
{
    "IpamPoolCidr": {

        "Cidr": "2605:9cc0:409::/48",

        "State": "deprovisioned"

    }

}
```

9. Ejecute el siguiente comando para eliminar el grupo de nivel superior.

   La cuenta de IPAM debe realizar este paso.

```
aws ec2 delete-ipam-pool --region us-east-1 --ipam-pool-id ipam-
pool-07f2466c7158b50c4 --profile ipam-account
```

   En la salida, puede ver el estado de eliminación.

```
{
    "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. Ejecute el siguiente comando para eliminar el IPAM.

    La cuenta de IPAM debe realizar este paso.

```
aws ec2 delete-ipam --region us-east-1 --ipam-id ipam-090e48e75758de279 --
profile ipam-account
```

    En la salida verá la respuesta de IPAM. Esto significa que se ha eliminado el IPAM.

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

Incorporación de su propia IP a CloudFront mediante IPAM (admite IPv4 e IPv6)

La funcionalidad BYOIP de IPAM para servicios globales permite usar direcciones IPv4 e IPv6 propias con servicios globales de AWS, como CloudFront. A diferencia del BYOIP regional, las direcciones IP se anuncian de forma simultánea desde múltiples ubicaciones periféricas mediante enrutamiento anycast.

Este tutorial cubre:

- Creación de grupos de IPAM globales para rangos de direcciones IPv4 (/24) y/o IPv6 (/48)
- Aprovisionamiento de listas de IP estáticas de Anycast con sus propias direcciones IP
- Anuncie sus CIDR en todo el mundo a través de las ubicaciones periféricas de CloudFront
- Configuraciones de doble pila mediante grupos de IPAM de direcciones IPv4 e IPv6 independientes

¿Por qué usar esta característica?

- Mantenga listas de permitidos de direcciones IP: utilice direcciones IP ya aprobadas en lugar de modificar las configuraciones del firewall
- Simplifique las migraciones: migre desde otros CDN sin necesidad de cambiar la infraestructura de direcciones IP
- Marca coherente: conserve su espacio de direcciones IP existente al migrar a AWS
- Preparación IPv6: admite arquitecturas de pila dual modernas con IPv4 e IPv6

¿Quién debería usar esta característica?

Organizaciones que necesitan usar sus propias direcciones IP con entrega de contenido global, entre ellas:

- Grandes empresas con requisitos de listas de permitidos de direcciones IP
- Empresas que migran desde otros CDN y ya cuentan con direcciones IP existentes
- Organizaciones con políticas de seguridad estrictas que exigen rangos de direcciones IP específicos
- Empresas que requieren configuraciones de pila dual (IPv4/IPv6) para lograr un alcance global

¿Cuándo usar esta característica?

Use BYOIP para servicios globales cuando necesite lo siguiente:

- Mantener listas de permitidos de direcciones IP existentes con socios o clientes
- Migrar desde otro CDN con direcciones IP propias
- Cumplir requisitos normativos que exigen rangos de direcciones IP específicos
- Implemente arquitecturas de pila dual compatibles con clientes IPv4 e IPv6

> **Note**
>
> Requiere bloques de CIDR IPv4 de /24. La pila dual (IPv4 e IPv6) requiere bloques de CIDR IPv6 de /24 IPv6. Actualmente, esta característica está disponible solo para CloudFront.

Requisitos previos

Complete estos pasos antes de empezar:

- Configuración de IPAM: Integración de IPAM con cuentas en una organización de AWS y Creación de un IPAM
- Verificación de dominio – Verificación del control de dominio
- Creación de grupos de nivel superior: siga los pasos 1 y 2 de Incorporación de su propio CIDR IPv4 a IPAM o Incorporación de su propio CIDR IPv6 a IPAM
- ROA (autorización de origen de ruta): asegúrese de que las ROA estén configuradas para los prefijos IPv4 (/24) e IPv6 (/48) si se utiliza una pila doble

Pasos de configuración para servicios globales

Los siguientes pasos difieren del proceso de BYOIP regional estándar y establecen el patrón de los servicios globales. Para las implementaciones de doble pila, debe crear grupos independientes para IPv4 e IPv6 y, a continuación, aprovisionar ambos a CloudFront.

Paso 1: creación de un grupo, o grupos, global para servicios anycast

En lugar de crear un grupo regional, cree un grupo global para servicios anycast:

Consola

Para crear un grupo global mediante la consola:

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, seleccione Grupos
3. Seleccione Crear grupo
4. Origen: seleccione su grupo de BYOIP de nivel superior
5. Configuración regional: seleccione Global
6. Servicio: seleccione Servicios globales (esta opción aparece cuando se selecciona Global)
7. Origen de IP pública: seleccione BYOIP
8. CIDR para aprovisionar: especifique el rango de CIDR de /24 (para IPv4) o el rango de CIDR de /48 (para IPv6)
9. Seleccione Crear grupo

CLI

Para IPv4:

```
aws ec2 create-ipam-pool \
  --ipam-scope-id scope-id \
  --locale None \
  --address-family ipv4 \
  --source-ipam-pool-id top-level-pool-id

aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id global-pool-id \
  --cidr your-ipv4-/24
```

Para IPv6:

```
aws ec2 create-ipam-pool \
  --ipam-scope-id scope-id \
  --locale None \
  --address-family ipv6 \
  --source-ipam-pool-id top-level-pool-id

aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id global-pool-id \
```

```
--cidr your-ipv6-/48
```

Important

- Para IPv4: debe asignar el bloque /24 completo a este grupo. Puede aprovisionar rangos más específicos dentro de este bloque para diferentes usos.
- Para IPv6: debe asignar el bloque /48 completo a este grupo. Puede aprovisionar rangos más específicos dentro de este bloque para diferentes usos.

Paso 2: creación de recursos específicos del servicio

Para CloudFront, cree una lista de direcciones IP anycast que use el grupo de IPAM. Para obtener instrucciones detalladas, consulte Incorporación de su propia IP a CloudFront mediante IPAM en la Guía para desarrolladores de Amazon CloudFront.

Parámetros clave para la integración con IPAM:

- Tipo de dirección IP: seleccione BYOIP
- Grupo de IPAM: seleccione el grupo global creado en el Paso 1 (IPv4 o IPv6)
- Cantidad de direcciones IP: introduzca 3 (requisito para CloudFront)

Paso 3: asociación con recursos del servicio

Asocie la lista de direcciones IP estáticas anycast con una distribución de CloudFront. Para obtener instrucciones detalladas, consulte Incorporación de su propia IP a CloudFront mediante IPAM en la Guía para desarrolladores de Amazon CloudFront.

Configuración clave:

- En la configuración de la distribución, seleccione la lista de direcciones IP anycast creada en el Paso 2

Paso 4: prepare todo para la migración

- Reducir el TTL de DNS: establezca el TTL de DNS de los registros en 60 segundos o menos
- Esperar la propagación: conceda el tiempo necesario para que el nuevo TTL se aplique en Internet

Paso 5: anuncio de CIDR a nivel mundial

Usar el comando de anuncio global de IPAM:

Consola

Para anunciar el CIDR mediante la consola:

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, seleccione Grupos
3. Seleccione el grupo global
4. Seleccione la pestaña CIDR
5. Seleccione el CIDR y elija Acciones > Anunciar CIDR
6. Confirme el anuncio

CLI

Para IPv4:

```
aws ec2 advertise-byoip-cidr \
  --cidr your-ipv4-/24
```

Para IPv6:

```
aws ec2 advertise-byoip-cidr \
  --cidr your-ipv6-/48
```

> **Important**
>
> - Antes de ejecutar este comando, retire el anuncio del CIDR del proveedor anterior
> - Actualice los registros DNS para que apunten a CloudFront y completar la migración (registros A para IPv4, registros AAAA para IPv6)

Eliminación

Para limpiar los recursos creados en este tutorial:

- Eliminar los recursos de CloudFront: siga las instrucciones de limpieza de Incorporación de su propia IP a CloudFront mediante IPAM de la Guía para desarrolladores de Amazon CloudFront
- Retirar el CIDR y eliminar los grupos de IPAM: siga el proceso de limpieza estándar descrito en Paso 8: Eliminar

> **Important**
>
> Elimine primero los recursos de CloudFront y, a continuación, realice la limpieza de IPAM para evitar interrupciones del servicio.

Tutorial: Transferir un CIDR IPv4 de BYOIP a IPAM

Siga estos pasos para transferir un CIDR IPv4 existente a IPAM. Si ya tiene un CIDR IPv4 con AWS, puede mover el CIDR a IPAM desde un grupo IPv4 público. No se puede trasladar un CIDR IPv6 a IPAM.

En este tutorial, se asume que ya trajo correctamente un rango de direcciones IP a AWS mediante el proceso descrito en Traiga sus propias direcciones IP (BYOIP) en Amazon EC2 y ahora quiere transferir ese rango de direcciones IP a IPAM. Si va a traer una nueva dirección IP a AWS por primera vez, siga los pasos de Tutorial: incorpore sus direcciones IP a IPAM.

Si transfiere un grupo IPv4 público a IPAM, las asignaciones existentes no se verán afectadas. Una vez que transfiera un grupo IPv4 público a IPAM, según el tipo de recurso, podrá supervisar las asignaciones existentes. Para obtener más información, consulte Monitorear el uso de CIDR por recurso.

> **Note**
>
> - En este tutorial, se presupone que ya ha completado los pasos en Creación de un IPAM.
> - Cada paso de este tutorial debe realizarlo una de dos cuentas AWS:
>   - La cuenta de administrador de IPAM. En este tutorial, esta cuenta se llamará cuenta de IPAM.
>   - La cuenta de su organización propietaria del CIDR de BYOIP. En este tutorial, esta cuenta se llamará cuenta de propietario CIDR de BYOIP.

Contenido

Paso 1: Crear perfiles con nombre y roles de IAM de la AWS CLI

Para completar este tutorial como un usuario de AWS único, puede utilizar perfiles con nombre de AWS CLI para cambiar de un rol de IAM a otro. Los perfiles con nombre son conjuntos de configuraciones y credenciales a los que se hace referencia cuando se utiliza la opción `--profile` con la AWS CLI. Para obtener más información sobre cómo crear roles de IAM y perfiles con nombre para las cuentas de AWS, consulte Uso de un rol de IAM en la AWS CLI.

Cree un rol y un perfil con nombre para cada una de las tres cuentas de AWS que utilizará en este tutorial:

- Un perfil llamado `ipam-account` para la cuenta AWS que es el administrador de IPAM.
- Un perfil llamado `byoip-owner-account` para la cuenta AWS de su organización propietaria del CIDR de BYOIP.

Después de crear los roles de IAM y los perfiles con nombre, regrese a esta página y vaya al paso siguiente. En el resto de este tutorial, observará que los comandos AWS CLI de ejemplo utilizan la opción `--profile` con uno de los perfiles con nombre para indicar qué cuenta debe ejecutar el comando.

Paso 2: Obtenga el ID de alcance público del IPAM

Siga los pasos descritos en esta sección para obtener el ID de alcance público del IPAM. La cuenta de **`ipam-account`** debe realizar este paso.

Ejecute el siguiente comando para obtener su ID de alcance público.

```
aws ec2 describe-ipams --region us-east-1 --profile ipam-account
```

En la salida, verá su ID de alcance público. Tenga en cuenta los valores para `PublicDefaultScopeId`. Lo necesitará en el siguiente paso.


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


Paso 3: Cree un grupo de IPAM

Siga los pasos de esta sección para crear un grupo de IPAM. La cuenta de **`ipam-account`** debe realizar este paso. El grupo de IPAM que cree debe ser un grupo de nivel superior con la opción `--locale` que coincide con la región BYOIP CIDR AWS. Solo puede transferir un BYOIP a un grupo de IPAM de nivel superior.

Important

Al crear el grupo, debe incluir `--aws-service ec2`. El servicio que seleccione determina el servicio AWS donde el CIDR puede ser anunciado. Actualmente, la única opción es `ec2`, lo que significa que los CIDR asignados desde este grupo podrán ser anunciados por el

servicio Amazon EC2 (para direcciones IP elásticas) y el servicio Amazon VPC (para CIDR asociados a VPC).

Para crear un grupo de direcciones IPv4 para el CIDR de BYOIP transferido mediante la AWS CLI

1. Ejecute el siguiente comando para crear un grupo de IPAM. Utilice el ID de alcance público de IPAM que se recuperó en el paso anterior.

```
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
```

   En la salida, verá `create-in-progress`, lo que indica que la creación del grupo se encuentra en curso.

```
{
    "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. Ejecute el siguiente comando hasta que vea el estado `create-complete` en la salida.

```
aws ec2 describe-ipam-pools --region us-east-1 --profile ipam-account
```

La siguiente salida de ejemplo muestra el estado del grupo. Necesitará el ID de propietario en el siguiente paso.

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

Paso 4: Comparta el grupo de IPAM mediante AWS RAM

Siga los pasos de esta sección para compartir un grupo de IPAM utilizando AWS RAM para que otra cuenta de AWS pueda transferir un CIDR IPV4 de BYOIP existente al grupo de IPAM y usarlo. La cuenta de **`ipam-account`** debe realizar este paso.

Para compartir un grupo de direcciones IPv4 mediante AWS CLI

1. Ver los permisos de AWS RAM disponibles para los grupos de IPAM. Necesita ambos ARN para completar los pasos de esta sección.

```
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. Cree un recurso compartido para permitir que la cuenta de **byoip-owner-account** importe los CIDR de BYOIP a IPAM. El valor para `--resource-arns` es el ARN del grupo de IPAM que creó en la sección anterior. El valor para `--principals` es el ID de la cuenta propietaria del CIDR de BYOIP. El valor para `--permission-arns` es el ARN del permiso `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. (Opcional) Si desea permitir que la cuenta de **`byoip-owner-account`** asigne CIDR de direcciones IP desde el grupo de IPAM a grupos IPv4 públicos una vez finalizada la transferencia, copie el ARN de `AWSRAMDefaultPermissionsIpamPool` y cree un segundo recurso compartido. El valor para `--resource-arns` es el ARN del grupo de IPAM que creó en la sección anterior. El valor para `--principals` es el ID de la cuenta propietaria del CIDR de BYOIP. El valor para `--permission-arns` es el ARN del permiso `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"

        }

}
```

Como resultado de la creación del recurso compartido en RAM, la cuenta byoip-owner-account ahora puede mover CIDR a IPAM.

Paso 5: Transfiera un CIDR IPV4 de BYOIP existente a IPAM

Siga los pasos para transferir un CIDR IPv4 de BYOIP existente a IPAM. La cuenta de **`byoip-owner-account`** debe realizar este paso.

> **Important**
>
> Una vez que hayas llevado un rango de direcciones IPv4 a AWS, podrás usar todas las direcciones IP del rango, incluidas la primera dirección (la dirección de red) y la última dirección (la dirección de transmisión).

Para transferir el CIDR de BYOIP a IPAM, el propietario del CIDR de BYOIP debe contar con estos permisos en su política de IAM:

- `ec2:MoveByoipCidrToIpam`
- `ec2:ImportByoipCidrToIpam`

> **Note**
>
> Puede utilizar la Consola de administración de AWS o la AWS CLI para este paso.

AWS Management Console

Para transferir un CIDR de BYOIP al grupo de IPAM:

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/ como la cuenta de **`byoip-owner-account`**.
2. En el panel de navegación, elija Pools (Grupos).
3. Elija el grupo de nivel superior creado y compartido en este tutorial.
4. Elija Acciones > Transferir un CIDR de BYOIP.
5. Elija Transferir un CIDR de BYOIP.
6. Elija su CIDR de BYOIP.
7. Elija Aprovisionar.

Command line

Ejecute los siguientes comandos de la AWS CLI para transferir un CIDR de BYOIP al grupo de IPAM con la AWS CLI:

1. Ejecute el siguiente comando para transferir el CIDR. Asegúrese de que el valor `--region` es la región de AWS del CIDR de 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
```

En la salida, verá el CIDR pendiente de aprovisionamiento.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "pending-transfer"

    }

}
```

2. Asegúrese de que se haya transferido el CIDR. Ejecute el siguiente comando hasta que vea el estado `complete-transfer` en la salida.

```
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
```

En la siguiente salida de ejemplo se muestra el estado.

```
{
    "ByoipCidr": {

        "Cidr": "130.137.249.0/24",

        "State": "complete-transfer"

    }

}
```

Paso 6: Vea el CIDR en IPAM

Siga los pasos de esta sección para ver el CIDR en IPAM. La cuenta de **`ipam-account`** debe realizar este paso.

Para ver el CIDR de BYOIP transferido en el grupo de IPAM mediante la AWS CLI

- Ejecute el siguiente comando para ver la asignación administrada en IPAM. Asegúrese de que el valor `--region` es la región de AWS del CIDR de BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

La salida muestra la asignación en IPAM.

```
{
    "IpamPoolAllocations": [
        {
            "Cidr": "130.137.249.0/24",
```

```
            "IpamPoolAllocationId": "ipam-pool-
alloc-5dedc8e7937c4261b56dc3e3eb53dc46",
            "ResourceId": "ipv4pool-ec2-0019eed22a684e0b3",
            "ResourceType": "ec2-public-ipv4-pool",
            "ResourceOwner": "111122223333"
        }
    ]
}
```

Paso 7: Efectúe una limpieza

Siga los pasos de esta sección para eliminar los recursos que ha creado en este tutorial. La cuenta de **`ipam-account`** debe realizar este paso.

Para eliminar los recursos que se han creado en este tutorial mediante la AWS CLI

1. Para eliminar el recurso compartido del grupo de IPAM, ejecute el siguiente comando para obtener el primer ARN de recurso compartido:

```
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. Copie el ARN del recurso compartido y utilícelo para eliminar el recurso compartido del grupo de 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. Si ha creado un recurso compartido adicional en Paso 4: Comparta el grupo de IPAM mediante AWS RAM, repita los dos pasos anteriores para obtener el ARN del segundo recurso compartido de `PoolShare2` y elimínelo.
4. Ejecute el siguiente comando para obtener el ID de asignación del CIDR de BYOIP. Asegúrese de que el valor `--region` coincida con la región de AWS del CIDR de BYOIP.

```
aws ec2 get-ipam-pool-allocations --region us-west-2  --profile ipam-account --
ipam-pool-id ipam-pool-0d8f3646b61ca5987
```

La salida muestra la asignación en 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. Lance el CIDR del grupo IPv4 público. Cuando ejecute el comando en esta sección, el valor de `--region` debe coincidir con la región de su IPAM.

La cuenta de **`byoip-owner-account`** debe realizar este paso.

```
aws ec2 deprovision-public-ipv4-pool-cidr --region us-east-1  --profile byoip-
owner-account --pool-id ipv4pool-ec2-0019eed22a684e0b3 --cidr 130.137.249.0/24
```

6. Vuelva a ver sus CIDR de BYOIP y asegúrese de que no haya más direcciones aprovisionadas. Al ejecutar el comando en esta sección, el valor de `--region` debe coincidir con la región de su IPAM.

   La cuenta de **`byoip-owner-account`** debe realizar este paso.

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1 --profile byoip-owner-account
   ```

   En la salida aparecerá el recuento de direcciones IP en el grupo IPv4 público.

   ```
   {
       "PublicIpv4Pools": [
           {
               "PoolId": "ipv4pool-ec2-0019eed22a684e0b3",
               "Description": "",
               "PoolAddressRanges": [],
               "TotalAddressCount": 0,
               "TotalAvailableAddressCount": 0,
               "NetworkBorderGroup": "us-east-1",
               "Tags": []
           }
       ]
   }
   ```

7. Ejecute el siguiente comando para eliminar el grupo de nivel superior.

   ```
   aws ec2 delete-ipam-pool --region us-east-1  --profile ipam-account --ipam-pool-
   id ipam-pool-0a03d430ca3f5c035
   ```

   En la salida, puede ver el estado de eliminación.

   ```
   {
       "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: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred

Complete este tutorial para planificar el espacio de direcciones IP de la VPC a fin de asignar direcciones IP a las subredes de la VPC y monitorear las métricas relacionadas con las direcciones IP a nivel de subred y VPC.

> **Note**
>
> En este tutorial, se describe la asignación del espacio de direcciones IPv4 privadas en un alcance de IPAM privado a las VPC y las subredes. También puede completar este tutorial con un rango de CIDR de IPv6 mediante la creación de la VPC con la opción de bloque de CIDR de IPv6 que ofrece Amazon en la consola de VPC.

La planificación del espacio de direcciones IP de la VPC para las subredes le permite realizar lo siguiente:

- Planificar y organizar las direcciones IP de la VPC para asignarlas a las subredes: puede dividir el espacio de direcciones IP de la VPC en bloques de CIDR más pequeños y aprovisionar esos bloques de CIDR a subredes con diferentes necesidades empresariales, por ejemplo, ejecutar cargas de trabajo en subredes de desarrollo o producción.
- Simplificar las asignaciones de direcciones IP para las subredes de la VPC: una vez que se planifique y organice el espacio de direcciones de la VPC, puede elegir una longitud de máscara de red en lugar de introducir un CIDR de forma manual. Por ejemplo, si un desarrollador crea una subred a fin de alojar cargas de trabajo de desarrollo, debe elegir un conjunto y una longitud

de máscara de red para la subred e el IPAM asignará el bloque de CIDR a su subred de forma automática.

En el siguiente ejemplo, se muestra la jerarquía de la estructura de grupos y recursos que creará con este tutorial:

- Alcance privado
  - Grupo de planificación de recursos (10.0.0.0/20)
    - Grupo de subredes de desarrollo (10.0.0.0/24)
      - Subred de desarrollo (10.0.0.0/28)
    - Grupo de subred de producción (10.0.0.1/24)
      - Subred de producción (10.0.0.16/28)

Important

- El grupo de planificación de recursos se puede utilizar para asignar los CIDR a las subredes o como un grupo de orígenes en el que se pueden crear otros grupos. En este tutorial, utilizamos el grupo de planificación de recursos como grupo de orígenes para los grupos de subredes.
- Puede crear varios grupos de planificación de recursos con la misma VPC si la VPC tiene más de un CIDR aprovisionado; si una VPC tiene dos CIDR asignados, por ejemplo, puede crear dos grupos de planificación de recursos, uno de cada CIDR. Cada CIDR se puede asignar a un grupo a la vez.

Paso 1: Crear una VPC

Complete los pasos de esta sección a fin de crear una VPC que se utilizará para la planificación de direcciones IP de la subred. Para más información sobre los permisos de IAM necesarios para crear VPC, consulte Ejemplos de políticas de Amazon VPC en la Guía del usuario de Amazon VPC.

> **Note**
>
> Puede utilizar una VPC existente en lugar de crear una nueva. Sin embargo, en este tutorial la VPC se configura con un bloque de CIDR asignado de forma manual, no con un bloque de CIDR asignado por el IPAM de manera automática.

Para crear una VPC

1. Con la cuenta de administrador del IPAM, abra la consola de VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione Creación de VPC.
3. Ingrese un nombre para la VPC, como tutorial-vpc.
4. Elija IPv4 CIDR manual input (Entrada manual de IPv4 CIDR) e introduzca un bloque de CIDR IPv4. En este tutorial, utilizaremos 10.0.0.0/20.
5. Omita la opción de agregar un bloque de CIDR de IPv6.
6. Seleccione Creación de VPC.
7. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
8. En el panel de navegación izquierdo, elija Recursos.
9. Espere a que aparezca la VPC que ha creado. Esto demora un tiempo y es posible que tenga que actualizar la ventana para que aparezca. El IPAM debe detectar la VPC antes de continuar con el siguiente paso.

Paso 2: Crear un grupo de planificación de recursos

Complete los pasos de esta sección para crear un grupo de planificación de recursos.

Para crear un grupo de planificación de recursos

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado.
4. Elija Create pool (Crear grupo).

5. En Álcance de IPAM, deje seleccionado el alcance privado.
6. (Opcional) Agregue una Etiqueta de nombre para el grupo, como “Grupo-planificación-recursos”.
7. En Origen, elija Alcance del IPAM.
8. En Planificación de recursos, elija Planificar el espacio de IP en una VPC y elija la VPC que creó en el paso anterior. La VPC es el recurso que se utiliza para aprovisionar los CIDR al grupo de planificación de recursos.
9. En CIDR para aprovisionar, elija el CIDR de la VPC para aprovisionar del grupo de recursos. El CIDR que aprovisione al grupo de planificación de recursos debe coincidir con el CIDR aprovisionado para la VPC. En este tutorial, utilizaremos 10.0.0.0/20.
10. Elija Create pool (Crear grupo).
11. Una vez que se haya creado el grupo, elija la pestaña CIDR para ver el estado del CIDR aprovisionado. Actualice la página y espere a que el estado del CIDR cambie de Aprovisionamiento pendiente a Aprovisionado antes de continuar con el siguiente paso.

Paso 3: Crear grupos de subredes

Complete los pasos de esta sección para crear dos grupos de subredes que se utilizarán a fin de asignar espacio de IP a las subredes.

Para crear grupos de subredes

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado.
4. Elija Create pool (Crear grupo).
5. En Álcance de IPAM, deje seleccionado el alcance privado.
6. (Opcional) Agregue una Etiqueta de nombre para el grupo, como “Grupo-subredes-desarrollo”.
7. En Origen, elija Grupo de IPAM y seleccione el grupo de planificación de recursos que creó en el Paso 3. La familia de direcciones, la configuración de planificación de recursos y la configuración regional se heredan de forma automática del grupo de origen.
8. En CIDR para aprovisionar, elija el CIDR para aprovisionar del grupo de subredes. En este tutorial, utilizaremos 10.0.0.0/24.
9. Elija Create pool (Crear grupo).

10. Una vez que se haya creado el grupo, elija la pestaña CIDR para ver el estado del CIDR aprovisionado. Actualice la página y espere a que el estado del CIDR cambie de Aprovisionamiento pendiente a Aprovisionado antes de continuar con el siguiente paso.
11. Repita este proceso para crear otra subred llamada “grupo-subredes-producción”.

En este punto, si desea que el grupo de subredes se encuentre disponible para otras cuentas de AWS, puede compartir el grupo de subredes. Para obtener instrucciones al respecto, consulte Compartir un grupo de IPAM mediante AWS RAM. Luego, regrese aquí para completar el tutorial.

Paso 4: Crear subredes

Complete estos pasos para crear dos subredes.

Para crear subredes

1. Con la cuenta correcta, abra la consola de VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione Subredes > Crear subred.
3. Elija la VPC que creó al principio de este tutorial.
4. Ingrese un nombre para la subred, como “tutorial-subred”.
5. (Opcional) Elija una Zona de disponibilidad.
6. En Bloque de CIDR de IPv4, elija el Bloque de CIDR de IPV4 asignado por el IPAM y elija el grupo de subredes de desarrollo y una máscara de red /28.
7. Elija Create subnet (Crear subred).
8. Repita este proceso para crear otra subred. Esta vez, elija el grupo de subredes de producción y una máscara de red /28.
9. Regrese a la consola de IPAM y elija Recursos en el panel de navegación izquierdo.
10. Busque los grupos de subredes que creó y espere a que aparezcan debajo de estos. Esto demora un tiempo y es posible que tenga que actualizar la ventana para que aparezca.

Se ha completado el tutorial. Puede crear grupos de subredes adicionales según sea necesario o lanzar una instancia de EC2 en una de las subredes.

El IPAM publica métricas relacionadas con el uso de direcciones IP en las subredes. Puede configurar las alarmas de CloudWatch en la métrica SubnetIPUsage, lo que le permitirá tomar medidas cuando se superen los umbrales de utilización de IP. Si, por ejemplo, tiene un CIDR /24

(256 direcciones IP) asignado a una subred y desea recibir una notificación cuando se haya utilizado el 80 % de las IP, puede configurar una alarma de CloudWatch para que le avise cuando se alcance este umbral. A fin de obtener más información sobre cómo crear una alarma para el uso de la IP de la subred, consulte Consejo rápido para crear alarmas.

Paso 5: Eliminar

Complete estos pasos para eliminar los recursos que ha creado en este tutorial.

Para limpiar los recursos.

1. Utilizando la cuenta de administrador de IPAM, abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el ámbito privado.
4. Elija el grupo de planificación de recursos y elija Acción > Eliminar.
5. Seleccione Eliminar en cascada. Se eliminarán el grupo de planificación de recursos y los grupos de subredes. Esto no eliminará las subredes en sí. Permanecerán con los CIDR que se les han aprovisionado, aunque los CIDR ya no pertenecerán a un grupo de IPAM.
6. Elija Eliminar.
7. Eliminar las subredes.
8. Eliminar la VPC.

Ha completado la limpieza.

Asignación de direcciones IP elásticas secuenciales de un grupo del IPAM

El IPAM le permite aprovisionar bloques IPv4 públicos propiedad de Amazon a grupos del IPAM y asignar direcciones IP elásticas secuenciales de esos grupos a los recursos de AWS.

Las direcciones IP elásticas asignadas de forma contigua son direcciones IPv4 públicas que se asignan secuencialmente. Por ejemplo, si Amazon le proporciona un bloque de CIDR IPv4 público de `192.0.2.0/30` y usted asigna las cuatro direcciones IPv4 públicas disponibles de ese bloque de CIDR, un ejemplo de cuatro direcciones IP elásticas secuenciales es `192.0.2.0`, `192.0.2.1`, `192.0.2.2` y `192.0.2.3`.

Las direcciones IP elásticas asignadas de forma contigua le permiten simplificar las reglas de seguridad y redes de las siguientes maneras:

- Administración de la seguridad: el uso de direcciones IPv4 secuenciales reduce la sobrecarga de administración del firewall. Puede agregar un prefijo completo con una sola regla y asociar las IP del mismo prefijo a medida que vaya escalando, lo que le permite ahorrar tiempo y esfuerzo.
- Acceso empresarial: puede simplificar el espacio de direcciones compartido con sus clientes utilizando un bloque de CIDR completo en lugar de una larga lista de direcciones IPv4 públicas individuales. Esto evita la necesidad de comunicar constantemente los cambios de IP a medida que la aplicación se escala en AWS.
- Administración de IP simplificada: el uso de direcciones IPv4 secuenciales simplifica la administración de IP públicas para su equipo central de redes, ya que reduce la necesidad de hacer un seguimiento de las IP públicas individuales y, en cambio, les permite centrarse en un número limitado de prefijos de IP.

En este tutorial, conocerá los pasos necesarios para asignar direcciones IP elásticas secuenciales de un grupo del IPAM. Creará un grupo del IPAM con un bloque de CIDR IPv4 público contiguo proporcionado por Amazon, asignará direcciones IP elásticas del grupo y aprenderá a supervisar las asignaciones de grupos del IPAM.

> **Note**
>
> - El aprovisionamiento de bloques de CIDR IPv4 públicos propiedad de Amazon conlleva cargos. Para obtener más información, consulte la pestaña Bloque IPv4 contiguo proporcionado por Amazon en la página Precios de Amazon VPC.
> - En este tutorial se da por sentado que desea crear un IPAM con uno que utiliza con una sola cuenta. Si desea compartir bloques IPv4 públicos contiguos propiedad de Amazon entre cuentas, primero Integración de IPAM con cuentas en una organización de AWS y, a continuación, Compartir un grupo de IPAM mediante AWS RAM. Si lleva a cabo la integración con AWS Organizations, tiene la opción de crear una política de control de servicio para evitar el desaprovisionamiento de los bloques IPv4 contiguos asignados al grupo.
> - No puede transferir direcciones IP elásticas secuenciales asignadas desde un grupo del IPAM a otras cuentas de AWS. En cambio, el IPAM le permite compartir grupos del IPAM entre cuentas de AWS mediante la integración del IPAM con AWS Organizations (como se mencionó anteriormente).

- Existen límites en cuanto al número de bloques de CIDR IPv4 públicos propiedad de Amazon que se pueden aprovisionar y a su tamaño. Para obtener más información, consulte Cuotas de IPAM.

Contenido

Paso 1: crear un IPAM

Complete los pasos de esta sección para crear un IPAM.

AWS Management Console

Para crear un IPAM

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En la AWS Management Console, elija la región de AWS en la que desea crear el IPAM. Cree el IPAM en su región principal de operaciones.
3. En la página de inicio del servicio, elija Create IPAM (Crear IPAM).
4. Seleccione Allow Amazon VPC IP Address Manager to replicate data from source account(s) into the IPAM delegate account (Permitir al Administrador de direcciones IP de Amazon VPC replicar los datos de las cuentas de origen en la cuenta delegada de IPAM). Si no selecciona esta opción, no puede crear un IPAM.
5. Elija un Nivel de IPAM. Para obtener más información sobre las características disponibles en cada nivel y los costos asociados a los niveles, consulte la pestaña de IPAM en la Página de precios de Amazon VPC.
6. En Operating regions (Regiones operativas), seleccione las regiones de AWS en las que este IPAM puede administrar y descubrir recursos. La región de AWS en la que va a crear su IPAM se selecciona como una de las regiones operativas de forma predeterminada.

Por ejemplo, si va a crear este IPAM en la región `us-east-1` de AWS, pero desea crear grupos de IPAM regionales más adelante que proporcionen CIDR a las VPC en `us-west-2`, seleccione `us-west-2` aquí. Si olvida una región operativa, puede volver más adelante y editar la configuración del IPAM.

> **Note**
>
> Si crea un IPAM en el nivel gratuito, puede seleccionar varias regiones operativas para su IPAM, pero la única característica de IPAM que se encontrará disponible en todas las regiones operativas es Información sobre IP públicas. No puede utilizar otras características del nivel gratuito, como BYOIP, en todas las regiones operativas del IPAM. Solo puede utilizarlas en la región de origen del IPAM. Para utilizar todas las características del IPAM en todas las regiones operativas, cree un IPAM en el nivel avanzado.

7. Elija Create IPAM (Crear IPAM).

Command line

Los comandos de esta sección están vinculados a la documentación de referencia de AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Cree el IPAM con el comando create-ipam:

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

Respuesta de ejemplo:

```
{
    "Ipam": {
        "OwnerId": "320805250157",
        "IpamId": "ipam-0755477df834ea06b",
        "IpamArn": "arn:aws:ec2::320805250157:ipam/ipam-0755477df834ea06b",
        "IpamRegion": "us-east-1",
        "PublicDefaultScopeId": "ipam-scope-01bc7290e4a9202f9",
        "PrivateDefaultScopeId": "ipam-scope-0a50983b97a7a583a",
        "ScopeCount": 2,
        "OperatingRegions": [
            {
```

```
                "RegionName": "us-east-1"
            }
        ],
        "State": "create-in-progress",
        "Tags": [],
        "DefaultResourceDiscoveryId": "ipam-res-disco-02cc5b34cc3f04f09",
        "DefaultResourceDiscoveryAssociationId": "ipam-res-disco-
assoc-06b3a4dccfc81f7c1",
        "ResourceDiscoveryAssociationCount": 1,
        "Tier": "advanced"
    }
}
```

Necesitará su PublicDefaultScopeId en el siguiente paso. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.

Paso 2: crear un grupo de IPAM y aprovisionar un CIDR

Complete los pasos de esta sección para crear un grupo del IPAM desde el que asignará las direcciones IP elásticas.

AWS Management Console

Para crear un grupo

1. Abra la consola de IPAM en https://console.aws.amazon.com/ipam/.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el alcance público. Para obtener más información acerca de los alcances, consulte Cómo funciona IPAM.
4. Elija Create pool (Crear grupo).
5. (Opcional) Agregue una Name tag (Etiqueta de nombre) y una Description (Descripción) para el grupo.
6. En Origen, elija Alcance del IPAM.
7. En Address family (Familia de direcciones), elija IPv4.
8. En Planificación de recursos, deje seleccionado Planificar el espacio de IP en el alcance.
9. En Locale (Configuración regional), elija la configuración regional para el grupo. La configuración regional es la Región AWS en la que desea que este grupo de IPAM esté

disponible para asignaciones. Las opciones disponibles proceden de las regiones operativas que eligió al crear su IPAM.

10. En Service (Servicio), elija EC2 (EIP/VPC). El servicio que seleccione determina el servicio de AWS donde se anunciará el CIDR. Actualmente, la única opción es EC2 (EIP/VPC), lo que significa que los CIDR asignados desde este grupo se anunciarán para el servicio Amazon EC2 (para direcciones IP elásticas).
11. En Fuente de IP pública, seleccione Propiedad de Amazon.
12. En CIDR que se aprovisionará, seleccione Agregar CIDR público propiedad de Amazon. Seleccione una longitud de máscara de red entre `/29` (8 direcciones IP) y `/30` (4 direcciones IP). Puede agregar hasta 2 CIDR de forma predeterminada. Para obtener información sobre cómo aumentar los límites de los CIDR IPv4 públicos contiguos proporcionados por Amazon, consulte Cuotas de IPAM.
13. Deje sin seleccionar la opción Configure this pool's allocation rule settings.
14. (Opcional) Elija Tags (Etiquetas) para el grupo.
15. Elija Create pool (Crear grupo).

Antes de continuar, asegúrese de que este CIDR se haya aprovisionado. Puede ver el estado del aprovisionamiento en la pestaña CIDR en la página de detalles del grupo.

Command line

Para crear un grupo

1. Cree un grupo de IPAM con el comando create-ipam-pool. La configuración regional es la Región AWS en la que desea que este grupo de IPAM esté disponible para asignaciones. Las opciones disponibles proceden de las regiones operativas que eligió al crear su IPAM.

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

Ejemplo de respuesta con estado `create-in-progress`:

```
{

    "IpamPool": {
```

```
        "OwnerId": "320805250157",

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

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

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

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

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

        "PoolDepth": 1,

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

        "AutoImport": false,

        "AddressFamily": "ipv4",

        "Tags": [],

        "AwsService": "ec2",

        "PublicIpSource": "amazon"

    }

}
```

2. Compruebe que el grupo se creó correctamente con el comando describe-ipam-pools.

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

Ejemplo de respuesta con estado `create-complete`:

```
{
```

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

3. Aprovisionar un CIDR en el grupo con el comando provision-ipam-pool-cidr. Seleccione una `--netmask-length` de entre `/29` (8 direcciones IP) y `/30` (4 direcciones IP). Puede agregar hasta 2 CIDR de forma predeterminada. Para obtener información sobre cómo aumentar los límites de los CIDR IPv4 públicos contiguos proporcionados por Amazon, consulte Cuotas de IPAM.

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

Ejemplo de respuesta con estado `pending-provision`:

```
{

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

4. Antes de continuar, asegúrese de que este CIDR se haya aprovisionado. Se puede ver el estado del aprovisionamiento mediante el comando get-ipam-pool-cidrs.

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

Ejemplo de respuesta con estado `provisioned`:

```
{

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

Paso 3: asignar una dirección IP elástica desde el grupo

Complete los pasos de esta sección para asignar una dirección IP elástica desde el grupo.

AWS Management Console

Siga los pasos de Allocate an Elastic IP address en la Guía del usuario de Amazon EC2 para asignar la dirección, pero tenga en cuenta lo siguiente:

- Asegúrese de que la región de AWS en la que se encuentra en la consola de EC2 coincida con la opción de configuración regional que eligió al crear el grupo en el Paso 2.
- Al elegir el grupo de direcciones, seleccione la opción Asignar mediante un grupo de IPAM IPv4 y elija el grupo que creó en el paso 1.

Command line

Asigne una dirección del grupo con el comando allocate-address. El valor de `--region` que utilice debe coincidir con la opción `-locale` que eligió al crear el grupo en el paso 2. Incluya el ID del grupo del IPAM que creó en el paso 2 en `--ipam-pool-id`.

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

Respuesta de ejemplo:

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

Si lo desea, también puede elegir un `/32` específico de su grupo de IPAM mediante la opción `--address`.

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

Respuesta de ejemplo:

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

Para obtener más información, consulte Allocate an Elastic IP address en la Guía del usuario de Amazon EC2.

Paso 4: asociar la dirección IP elástica a una instancia de EC2

Complete los pasos de esta sección a fin de asociar la dirección IP elástica a una instancia de EC2.

AWS Management Console

Siga los pasos de Asociar una dirección IP elástica en la Guía del usuario de Amazon EC2 para asignar una dirección IP elástica del grupo del IPAM, pero tenga en cuenta lo siguiente: cuando utilice la opción de la Consola de administración de AWS, la región de AWS a la que asocie la dirección IP elástica debe coincidir con la opción de configuración regional que eligió al crear el grupo en el Paso 2.

Command line

Asocie la dirección IP elástica a una instancia con el comando associate-address. La `--region` a la que asocia la dirección IP elástica debe coincidir con la opción `--locale` que eligió cuando creó el grupo en el Paso 2.

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

Respuesta de ejemplo:

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

Para obtener más información, consulte Asociación de una dirección IP elástica a una instancia o una interfaz de red en la Guía del usuario de Amazon EC2.

Paso 5: seguimiento y supervisión del uso del grupo

Una vez que haya asignado las direcciones IP elásticas del grupo del IPAM, puede rastrear y supervisar las asignaciones del grupo del IPAM.

AWS Management Console

- Consulte los detalles del grupo del IPAM en la pestaña Asignaciones en la consola del IPAM. Todas las direcciones IP elásticas asignadas desde el grupo del IPAM tienen un tipo de recurso de EIP.
- Use Información sobre IP públicas:
  - En Tipos de IP públicas, filtre por EIP propiedad de Amazon. Muestra el número total de direcciones IPv4 públicas asignadas a las direcciones IP elásticas propiedad de Amazon. Si filtra según esta medida y se desplaza hasta Direcciones IP públicas en la parte inferior de la página, verá las direcciones IP elásticas que ha asignado.
  - En Uso de EIP, filtre por EIP propiedad de Amazon asociadas o EIP propiedad de Amazon sin asociar. Muestra el número total de direcciones IP elásticas que ha asignado en su cuenta de AWS y que ha asociado o no a una instancia de EC2, una interfaz de red o un recurso de AWS. Si filtra según esta medida y se desplaza hasta Direcciones IP públicas en la parte inferior de la página, verá los detalles de los recursos filtrados.
  - En Uso de IPv4 contiguas propiedad de Amazon, supervise el uso de direcciones IPv4 públicas secuenciales a lo largo del tiempo y los grupos del IPAM de IPv4 relacionados propiedad de Amazon.
- Utilice Amazon CloudWatch para rastrear y supervisar las métricas relacionadas con los bloques IPv4 públicos contiguos proporcionados por Amazon que se han aprovisionado a los grupos del IPAM. Para ver las métricas disponibles específicas de los bloques IPv4 contiguos, consulte Métricas de IP públicas en Métricas del IPAM. Además de ver las métricas, puede crear alarmas en Amazon CloudWatch para que le notifiquen cuando se alcancen los umbrales. La creación de alarmas y la configuración de notificaciones con Amazon CloudWatch se encuentra fuera del ámbito de este tutorial. Para obtener más información, consulte Uso de las alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Command line

- Ver las asignaciones del grupo de IPAM con el comando get-ipam-pool-allocations. Todas las direcciones IP elásticas asignadas desde el grupo del IPAM tienen un tipo de recurso de EIP.

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

  Respuesta de ejemplo:

```
{
     "IpamPoolAllocations": [
        {
            "Cidr": "18.97.0.40/32",
            "IpamPoolAllocationId": "ipam-pool-
alloc-0bd07df786e8148aba2763e2b6c1c44bd",
            "ResourceId": "eipalloc-0c9decaa541d89aa9",
            "ResourceType": "eip",
            "ResourceRegion": "us-east-1",
            "ResourceOwner": "320805250157"
        }
    ]
}
```

- Utilice Amazon CloudWatch para rastrear y supervisar las métricas relacionadas con los bloques IPv4 públicos contiguos proporcionados por Amazon que se han aprovisionado a los grupos del IPAM. Para ver las métricas disponibles específicas de los bloques IPv4 contiguos, consulte Métricas de IP públicas en Métricas del IPAM. Además de ver las métricas, puede crear alarmas en Amazon CloudWatch para que le notifiquen cuando se alcancen los umbrales. La creación de alarmas y la configuración de notificaciones con Amazon CloudWatch se encuentra fuera del ámbito de este tutorial. Para obtener más información, consulte Uso de las alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Ya ha completado el tutorial. Ha creado un grupo del IPAM con un bloque CIDR IPv4 público contiguo proporcionado por Amazon, ha asignado direcciones IP elásticas del grupo y ha aprendido a supervisar las asignaciones de grupos del IPAM. Continúe con la sección siguiente para eliminar los recursos que ha creado en este tutorial.

Eliminación

Siga los pasos de esta sección para eliminar los recursos que ha creado en este tutorial.

Paso 1: anulación de la asociación de la dirección IP elástica

Siga los pasos de Disassociate an Elastic IP address en la Guía del usuario de Amazon EC2 con el objetivo de anular la asociación de la dirección IP elástica.

Paso 2: liberación de la dirección IP elástica

Siga los pasos de Release an Elastic IP address en la Guía del usuario de Amazon EC2 para liberar una dirección IP elástica del grupo de IPv4 público.

Paso 3: desaprovisionamiento del CIDR del grupo del IPAM

Siga los pasos de Anular el aprovisionamiento del CIDR de un grupo para desaprovisionar el CIDR público propiedad de Amazon del grupo del IPAM. Este paso es obligatorio para eliminar el grupo. Se le facturará el bloque de IPv4 contiguo proporcionado por Amazon hasta que se finalice este paso.

Paso 4: eliminación del grupo del IPAM

Siga los pasos de Eliminar un grupo para eliminar el grupo del IPAM.

Paso 5: eliminación de IPAM

Siga los pasos de Eliminar un IPAM para eliminar el IPAM.

Se ha completado la limpieza del tutorial.

Identity and Access Management en IPAM

AWS utiliza credenciales de seguridad para identificarlo y concederle acceso a sus recursos de AWS. Puede utilizar las características de AWS Identity and Access Management (IAM) para permitir que otros usuarios, servicios y aplicaciones usen sus recursos de AWS total o parcialmente, sin necesidad de compartir sus credenciales de seguridad.

En esta sección se describen los roles vinculados a servicios de AWS que se crean específicamente para IPAM y las políticas administradas adjuntas a los roles vinculados a servicios de IPAM. Para obtener más información sobre los roles y políticas de AWS IAM, consulte Términos y conceptos de roles en la Guía del usuario de IAM.

Para obtener más información sobre la administración de identidades y accesos para una VPC, consulte Administración de identidades y accesos para Amazon VPC en la Guía del usuario de Amazon VPC.

Contenido

Roles vinculados a servicios para IPAM

IPAM utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM. Los roles vinculados a servicios están predefinidos por IPAM e incluyen todos los permisos que el servicio requiere para llamar a otras soluciones de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de IPAM, ya que no tendrá que agregar manualmente los permisos necesarios. IPAM define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo IPAM puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Permisos de roles vinculados a servicios

IPAM utiliza el rol vinculado a servicios AWSServiceRoleForIPAM para llamar a las acciones en la política administrada adjunta AWSIPAMServiceRolePolicy. Para obtener más información sobre las acciones permitidas en esa política, consulte Políticas administradas por AWS para IPAM.

Este rol vinculado a servicios también tiene una política de confianza de IAM que permite que el servicio de `ipam.amazonaws.com` asuma el rol vinculado a servicios.

Creación del rol vinculado a servicios

IPAM supervisa el uso de direcciones IP en una o más cuentas al asumir el rol vinculado a servicios de una cuenta, al descubrir los recursos y sus CIDR y al integrar los recursos con IPAM.

El rol vinculado a servicios se crea de una de estas dos maneras:

- Al integrar con AWS Organizations

  Si Integración de IPAM con cuentas en una organización de AWS mediante la consola de IPAM o mediante el comando `enable-ipam-organization-admin-account` de AWS CLI, el rol vinculado a servicios AWSServiceRoleForIPAM se crea automáticamente en cada una de sus cuentas de miembros de AWS Organizations. Como resultado de ello, IPAM puede detectar los recursos de todas las cuentas de miembros.

  > **Important**
  >
  > Para que IPAM cree el rol vinculado a servicios en su nombre:
  >
  > - La cuenta de administración de AWS Organizations que permite la integración de IPAM con AWS Organizations deben tener adjunta una política de IAM que permita las siguientes acciones:
  >   - `ec2:EnableIpamOrganizationAdminAccount`
  >   - `organizations:EnableAwsServiceAccess`
  >   - `organizations:RegisterDelegatedAdministrator`
  >   - `iam:CreateServiceLinkedRole`
  > - La cuenta de IPAM debe tener adjunta una política de IAM que permita la acción `iam:CreateServiceLinkedRole`.

- Cuando crea una IPAM mediante una sola cuenta de AWS

Si Utilizar IPAM con una sola cuenta, el rol vinculado a servicios AWSServiceRoleForIPAM se crea automáticamente al crear un IPAM como esa cuenta.

> **Important**
>
> Si utiliza IPAM con una sola cuenta de AWS, antes de crear un IPAM, debe asegurarse de que la cuenta de AWS que utiliza tenga adjunta una política de IAM que permita la acción `iam:CreateServiceLinkedRole`. Al crear el IPAM, se crea automáticamente el rol vinculado a servicios AWSServiceRoleForIPAM. Para obtener más información sobre la administración de las políticas de IAM, consulte Edición de la descripción de un rol vinculado a servicios en la Guía del usuario de IAM.

Editar el rol vinculado a servicios

No puede editar el rol vinculado a servicios AWSServiceRoleForIPAM.

Eliminar el rol vinculado a servicios

Si ya no tiene que utilizar IPAM, le recomendamos que elimine el rol vinculado a servicios AWSServiceRoleForIPAM.

> **Note**
>
> Puede eliminar el rol vinculado a servicios solo después de eliminar todos los recursos de IPAM en su cuenta de AWS. Esto garantiza que no pueda eliminar accidentalmente la capacidad de monitoreo de IPAM.

Siga estos pasos para eliminar el rol vinculado a un servicio mediante AWS CLI:

1. Elimine los recursos de IPAM mediante deprovision-ipam-pool-cidr y delete-ipam. Para obtener más información, consulte Anular el aprovisionamiento del CIDR de un grupo y Eliminar un IPAM.
2. Desactive la cuenta de IPAM con disable-ipam-organization-admin-account.
3. Desactive el servicio de IPAM con disable-aws-service-accessmediante la opción `--service-principal ipam.amazonaws.com`.

4. Elimine el rol vinculado a servicios: delete-service-linked-role. Al eliminar el rol vinculado a servicios, también se elimina la política administrada de IPAM. Para obtener más información, consulte Eliminación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Políticas administradas por AWS para IPAM

Si utiliza el IPAM con una sola cuenta de AWS y crea un IPAM, la política administrada AWSIPAMServiceRolePolicy se crea de forma automática en su cuenta de IAM y se adjunta al rol vinculado a servicios AWSServiceRoleForIPAM.

Si habilita la integración de IPAM con AWS Organizations, la política administrada AWSIPAMServiceRolePolicy se crea automáticamente en su cuenta de IAM y en cada una de las cuentas de miembros de AWS Organizations, y la política administrada se adjunta al rol vinculado a servicios AWSServiceRoleForIPAM.

Esta política administrada permite a IPAM hacer lo siguiente:

- Monitorear los CIDR asociados con los recursos de red en todos los miembros de su organización de AWS.
- Almacenar métricas relacionadas con IPAM en Amazon CloudWatch, como el espacio de direcciones IP disponible en los grupos de IPAM y el número de CIDR de recursos que cumplen las reglas de asignación.
- Modifique y lea las listas de prefijos administradas.

En el ejemplo siguiente, se muestran detalles de la política administrada que se creó.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "IPAMDiscoveryDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeByoipCidrs",
```

```
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:ListByoipCidrs",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsPublishActions",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IPAM"
                }
            }
        }
    ]
}
```

La primera instrucción en el ejemplo anterior permite a IPAM supervisar los CIDR utilizados por una sola cuenta de AWS o por los miembros de su organización de AWS.

La segunda instrucción del ejemplo anterior utiliza la clave de condición `cloudwatch:PutMetricData` para permitir que IPAM almacene métricas de IPAM en su espacio de nombres de Amazon CloudWatch en `AWS/IPAM`. La Consola de administración de AWS utiliza estas métricas para mostrar datos sobre las asignaciones de los grupos y alcances de IPAM. Para obtener más información, consulte Monitorear el uso de CIDR con el panel de IPAM.

Actualizaciones de la política administrada por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para IPAM debido a que este servicio comenzó a realizar un seguimiento de estos cambios.

Cambio	Descripción	Fecha
AWSIPAMServiceRolePolicy	Se agregaron acciones a la política administrada AWSIPAMServiceRolePolicy (ec2:ModifyManagedPrefixList, ec2:DescribeManagedPrefixLists y ec2:GetManagedPrefixListEntries) para permitir que IPAM lea y modifique las listas de prefijos administradas.	31 de octubre de 2025
AWSIPAMServiceRolePolicy	Se añadieron acciones a la política administrada AWSIPamServiceRolePolicy (`organizations:ListChildren` ,`organizations:ListParents` y `organizations:DescribeOrganizationalUnit`) para permitir que el IPAM obtenga los detalles de las unidades organizativas (OU) de AWS Organizations, de modo que los clientes	21 de noviembre de 2024

Cambio	Descripción	Fecha
	puedan usar el IPAM a nivel de OU.	
AWSIPAMServiceRolePolicy	Se agregó una acción a la política administrada AWSIPAMServiceRolePolicy (`ec2:GetIpamDiscoveredPublicAddresses`) para permitir que IPAM obtenga direcciones IP públicas durante la detección de recursos.	13 de noviembre de 2023
AWSIPAMServiceRolePolicy	Se agregaron acciones a la política administrada AWSIPAMServiceRolePolicy (`ec2:DescribeAccountAttributes`, `ec2:DescribeNetworkInterfaces`, `ec2:DescribeSecurityGroups`, `ec2:DescribeSecurityGroupRules`, `ec2:DescribeVpnConnections`, `globalaccelerator:ListAccelerators` y `globalaccelerator:ListByoipCidrs`) para permitir que IPAM obtenga direcciones IP públicas durante la detección de recursos.	1 de noviembre de 2023

Cambio	Descripción	Fecha
AWSIPAMServiceRolePolicy	Se agregaron dos acciones a la política administrada AWSIPAMServiceRolePolicy (`ec2:GetIpamDiscoveredAccounts` y `ec2:GetIpamDiscoveredResourceCidrs`) para permitir que IPAM monitoree las cuentas de AWS y los CIDR de recursos durante la detección de recursos.	25 de enero de 2023
IPAM comenzó a realizar un seguimiento de los cambios	IPAM comenzó el seguimiento de los cambios de las políticas administradas por AWS.	2 de diciembre de 2021

Política de ejemplo

El ejemplo de política de esta sección contiene todas las acciones de AWS Identity and Access Management (IAM) relevantes para el uso completo de IPAM. Según cómo utilice IPAM, es posible que no necesite incluir todas las acciones de IAM. Para disfrutar de una experiencia completa al utilizar la consola de IPAM, es posible que deba incluir acciones de IAM adicionales para servicios como AWS Organizations, AWS Resource Access Manager (AWS RAM) y Amazon CloudWatch.

JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIpamByoasn",
                "ec2:DeprovisionIpamByoasn",
                "ec2:DescribeIpamByoasn",
```

```
                "ec2:DisassociateIpamByoasn",
                "ec2:ProvisionIpamByoasn",
                "ec2:CreateIpam",
                "ec2:DescribeIpams",
                "ec2:ModifyIpam",
                "ec2:DeleteIpam",
                "ec2:CreateIpamScope",
                "ec2:DescribeIpamScopes",
                "ec2:ModifyIpamScope",
                "ec2:DeleteIpamScope",
                "ec2:CreateIpamPool",
                "ec2:DescribeIpamPools",
                "ec2:ModifyIpamPool",
                "ec2:DeleteIpamPool",
                "ec2:ProvisionIpamPoolCidr",
                "ec2:GetIpamPoolCidrs",
                "ec2:DeprovisionIpamPoolCidr",
                "ec2:AllocateIpamPoolCidr",
                "ec2:GetIpamPoolAllocations",
                "ec2:ReleaseIpamPoolAllocation",
                "ec2:CreateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveries",
                "ec2:ModifyIpamResourceDiscovery",
                "ec2:DeleteIpamResourceDiscovery",
                "ec2:AssociateIpamResourceDiscovery",
                "ec2:DescribeIpamResourceDiscoveryAssociations",
                "ec2:DisassociateIpamResourceDiscovery",
                "ec2:GetIpamResourceCidrs",
                "ec2:ModifyIpamResourceCidr",
                "ec2:GetIpamAddressHistory",
                "ec2:GetIpamDiscoveredResourceCidrs",
                "ec2:GetIpamDiscoveredAccounts",
                "ec2:GetIpamDiscoveredPublicAddresses"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/ipam.amazonaws.com/
AWSServiceRoleForIPAM",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ipam.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

Cuotas de IPAM

En esta sección, se enumeran las cuotas relacionadas con IPAM. La consola de Service Quotas proporciona información sobre las cuotas de IPAM. Puede utilizar la consola de Service Quotas a fin de consultar las cuotas predeterminadas y solicitar aumentos de cuota para las cuotas ajustables. Para obtener más información, consulte este tema acerca de cómo solicitar un aumento de cuota en la Guía del usuario de Service Quotas.

Nombre	Predeterminado	Ajustable
Bloques de CIDR IPv4 públicos contiguos proporcionados por Amazon	2	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.
Longitud de la máscara de red de los bloques de CIDR IPv4 públicos contiguos proporcionados por Amazon	/29	El tamaño aceptable está comprendido entre /29 y /30. Para solicitar un aumento, póngase en contacto con el Centro de AWS Support tal y como se describe en AWS Service Quotas en la Referencia general de AWS.
Longitud de máscara de red del bloque de CIDR de IPv6 proporcionado por Amazon	/52	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.

Nombre	Predeterminado	Ajustable
Bloques de CIDR de IPv6 proporcionados por Amazon por grupo regional	1	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.
Números de sistema autónomo (ASN) que puede traer al IPAM	5	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.
CIDR por grupo	50	Sí
Destinos habilitados por política de IPAM	100	Sí. Para solicitar un ajuste del límite de cuota, póngase en contacto con el Centro de soporte de AWS, tal como se describe en Cuotas de servicio de AWS en Referencia general de AWS.
Administradores de IPAM por organización	1	No
IPAM por región	1	No

Nombre	Predeterminado	Ajustable
Políticas de IPAM por IPAM	10	Sí. Para solicitar un ajuste del límite de cuota, póngase en contacto con el Centro de soporte de AWS, tal como se describe en Cuotas de servicio de AWS en Referencia general de AWS.
Reglas de asignación de políticas de IPAM por par recurso–configuración regional*	10	Sí. Para solicitar un ajuste del límite de cuota, póngase en contacto con el Centro de soporte de AWS, tal como se describe en Cuotas de servicio de AWS en Referencia general de AWS.
Exclusiones de unidades organizativas por detección de recursos	10	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.
Profundidad del grupo (el número de grupos dentro de cada grupo)	10	Sí
Grupos por alcance	50	Sí
Solucionadores de listas de prefijos por IPAM	10	Sí

Nombre	Predeterminado	Ajustable
Destinos de solucionador de listas de prefijos por solucionador de listas de prefijos	50	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.
Reglas por solucionador de listas de prefijos	100	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.
Entradas CIDR por versión de solucionador de listas de prefijos	1 000	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.
Asociaciones de detección de recursos por IPAM	5	Sí
Detección de recursos por región	1	No
Métricas de utilización de recursos	50	Sí. Contacte al Centro de soporte de AWS como se describe en AWS Service Quotas en la Referencia general de AWS.

Nombre	Predeterminado	Ajustable
Alcances por IPAM	5	Sí. Al crear un IPAM, se crea un alcance privado y otro público para usted. Si desea crear alcances adicionales, serán alcances privados. No puede crear alcances públicos adicionales.

* Par recurso–configuración regional: al definir reglas de asignación, debe especificar tanto un tipo de recurso (el recurso de AWS, como EIP, ALB o clústeres de RDS) como una configuración regional (la región de AWS o la zona local donde se aplica la regla). Las reglas de asignación se limitan a esta combinación de tipo de recurso y configuración regional. Por ejemplo, si define una política para EIP en us-east-1, puede configurar hasta 10 reglas para ese par específico de recurso y configuración regional*.

Precios de IPAM

El Administrador de direcciones IP (IPAM) de Amazon VPC es un servicio que facilita la administración del espacio de direcciones IP en los recursos de AWS y las redes en las instalaciones. El IPAM proporciona una forma centralizada de planificar, supervisar y controlar las direcciones IP que utilizan sus recursos de AWS y en las instalaciones.

En esta sección, se describe cómo ver información relacionada con el precio y los costos de IPAM actuales.

Contenido

Ver información sobre precios

IPAM se ofrece en dos niveles: el nivel gratuito y el nivel avanzado. Para obtener más información sobre las características disponibles en cada nivel y los costos asociados a los niveles, consulte la pestaña IPAM en la página de precios de Amazon VPC.

Consulta de costos y su uso actuales mediante AWS Cost Explorer

Al utilizar el nivel avanzado de IPAM, paga un precio por hora por cada dirección IP activa gestionada por IPAM. Si desea ver y analizar los costos y el uso de IPAM, puede usar el AWS Cost Explorer.

1. Abra la consola de AWS Cost Management en https://console.aws.amazon.com/cost-management/home.
2. Elija Explorador de costos.
3. Para filtrar el uso de IPAM, elija Tipo de uso e ingrese **`IPAddressManager`**.
4. Seleccione una o varias casillas. Cada una de ellas representa una región de AWS diferente.
5. Haga clic en Apply.

Si selecciona, por ejemplo, USE1-IPAddressManager-IP-Hours(Hrs) y la región de origen del IPAM es us-east-1, verá el número de las horas de IP activas que IPAM facturó en todas las regiones junto

con los costos. Si el uso en horas es, por ejemplo, 18, esto significa que puede tener una dirección IP activa por 18 horas o tres direcciones IP en tres regiones distintas, cada una activa por 6 horas, o cualquier combinación cuya suma sea 18 horas.

Para obtener más información sobre AWS Cost Explorer, consulte Analyzing your costs with AWS Cost Explorer en la Guía del usuario de AWS Cost Management.

Información relacionada

Si bien el sitio de documentación técnica de AWS es un recurso integral, hay muchos otros lugares donde encontrar información sobre los servicios de AWS. Los blogs, documentos técnicos, estudios de casos y foros de la comunidad de AWS pueden proporcionar información valiosa, ejemplos del mundo real y perspectivas alternativas más allá de los detalles técnicos oficiales. Explorar estas fuentes diversas puede proporcionarle una comprensión más completa de las ofertas de AWS.

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con el Administrador de direcciones IP de Amazon VPC:

- Amazon VPC IP Address Manager Best Practices (Prácticas recomendadas de Amazon VPC IP Address Manager): publicación de blog de AWS sobre prácticas recomendadas para planificar y crear un esquema de direcciones escalable con Amazon VPC IP Address Manager.
- Network Address Management and Auditing at Scale with Amazon VPC IP Address Manager (Administración y auditoría de direcciones de red a escala con Amazon VPC IP Address Manager): publicación de blog de AWS que presenta Amazon VPC IP Address Manager y muestra cómo utilizar este servicio en la consola de AWS.
- Configure el acceso detallado a sus recursos compartidos mediante AWS Resource Access Manager: una publicación de blog de AWS que explica cómo compartir un grupo de IPAM con las cuentas de una unidad organizativa de AWS Organizations.
- Visualize enterprise IP address management and planning with CIDR map: un blog de AWS en el que se explica cómo visualizar todo el panorama de IPv4 e IPv6 mediante el mapa de CIDR del IPAM en la consola del IPAM.

Historial de documentos para IPAM

En la tabla siguiente se describen las versiones de IPAM.

Característica	Descripción	Fecha de lanzamiento
Incorporación de su propia IP a CloudFront mediante IPAM	Use IPAM para administrar los CIDR de BYOIP para servicios globales de AWS, comenzando por los servicios anycast de CloudFront.	21 de noviembre de 2025
Defina la estrategia de asignación de IPv4 pública con políticas de IPAM	Ahora puede usar políticas de IPAM para definir reglas que asignan servicios de AWS a grupos de IPAM específicos, lo que ayuda a definir la estrategia de asignación de IPv4 pública.	19 de noviembre de 2025
Integre IPAM con la infraestructura de Infoblox	Ahora puede integrar IPAM con la infraestructura de Infoblox, lo que permite administrar direcciones IP de AWS mediante los flujos de trabajo existentes de Infoblox y, al mismo tiempo, obtener capacidades nativas en la nube de AWS. Esta integración está disponible para ámbitos privados y requiere el nivel avanzado de IPAM.	7 de noviembre de 2025
Automatización de las actualizaciones de la lista de prefijos	Ahora puede usar los solucionadores de listas de prefijos de IPAM para automatizar las actualizaciones de las listas de prefijos en función de los CIDR de los grupos de IPAM.	31 de octubre de 2025
Administrar las alarmas desde la consola de IPAM	Ahora es posible crear y administrar alarmas de Amazon CloudWatch directamente de la consola de IPAM. Las alarmas relacionadas con IPAM aparecerán como barras de advertencia e indicadores visuales cuando estén en los estados INSUFFICIENT_DATA o ALARM.	21 de agosto de 2025

Característica	Descripción	Fecha de lanzamiento
Habilitar la distribución de costos	Cuando habilita la distribución de costos, distribuye los cargos por las direcciones IP activas a las cuentas que utilizan las direcciones IP y no al propietario del IPAM. Esto resulta útil para las grandes organizaciones en las que el administrador delegado de IPAM administra las direcciones IP de forma centralizada mediante el IPAM y cada cuenta es responsable de su propio uso, lo que elimina la necesidad de realizar cálculos de facturación manuales.	1 de mayo de 2025
Excluir las unidades organizativas del IPAM	Si su IPAM está integrado con AWS Organizations, ahora puede excluir las unidades organizativas del IPAM. El IPAM no administrará las direcciones IP de las cuentas con exclusiones de unidades organizativas.	21 de noviembre de 2024
Actualizaciones de política administrada de AWS: actualización de una política existente	Se ha actualizado la AWSIPAMServiceRolePolicy existente.	21 de noviembre de 2024
Asignación de direcciones IP elásticas secuenciales de un grupo del IPAM	Ahora el IPAM le permite aprovisionar bloques IPv4 públicos propiedad de Amazon a grupos del IPAM y asignar direcciones IP elásticas secuenciales de esos grupos a los recursos de AWS. Las direcciones IP elásticas secuenciales le permiten simplificar sus necesidades de redes y listas de permitidos para la seguridad.	28 de agosto de 2024

Característica	Descripción	Fecha de lanzamiento
GUA y ULA privados de IPv6	Ahora puede aprovisionar rangos GUA y ULA de IPv6 privados a un grupo de IPAM en un ámbito privado. Las direcciones IPv6 privadas solo están disponibles en IPAM. Para más información sobre el direccionamiento IPv6 privado, consulte Direcciones IPv6 privadas en la Guía del usuario de Amazon VPC.	8 de agosto de 2024
Niveles gratuito y avanzado de IPAM	Ahora puede elegir entre el nivel gratuito y avanzado para su IPAM.	17 de noviembre de 2023
Información sobre las IP públicas	Anteriormente, solo podía ver la Información sobre IP públicas en una sola región. Ahora puede ver la Información sobre IP públicas en todas las regiones. Además, ahora puede ver Información sobre direcciones IP públicas en Amazon CloudWatch.	17 de noviembre de 2023
Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred	Ahora puede utilizar el IPAM para planificar el espacio de IP de subred dentro de una VPC y monitorear las métricas relacionadas con las direcciones IP a nivel de subred y VPC.	17 de noviembre de 2023
Uso de su propio ASN (BYOASN)	Ahora puede traer su propio número de sistema autónomo (ASN) a AWS.	17 de noviembre de 2023
Actualizaciones de política administrada de AWS: actualización de una política existente	Se ha actualizado la AWSIPAMServiceRole Policy existente.	17 de noviembre de 2023

Característica	Descripción	Fecha de lanzamiento
Actualizaciones de política administrada de AWS: actualización de una política existente	Se ha actualizado la AWSIPAMServiceRolePolicy existente.	1 de noviembre de 2023
Métricas de utilización de recursos	IPAM ahora publica las métricas de utilización de IP de los recursos que IPAM supervisa en Amazon CloudWatch.	2 de agosto de 2023
Información sobre las IP públicas	La información sobre las IP públicas muestra todas las direcciones IPv4 públicas utilizadas por los servicios de esta región en su cuenta. Puede utilizar esta información para identificar el uso de direcciones IPv4 públicas y ver las recomendaciones para liberar las direcciones IP elásticas no utilizadas.	28 de julio de 2023
Actualizaciones de política administrada de AWS: actualización de una política existente	Se ha actualizado la AWSIPAMServiceRolePolicy existente.	25 de enero de 2023
Integración de IPAM con cuentas ajenas a su organización	Ahora puede administrar direcciones IP ajenas a su organización desde una única cuenta de IPAM y compartir grupos de IPAM con las cuentas de otras AWS Organizations.	25 de enero de 2023
Bloque de CIDR contiguo de IPv6 proporcionado por Amazon para grupos de IPAM	Al crear un grupo de IPAM en el alcance público, ahora puede aprovisionar en el grupo un bloque de CIDR contiguo de IPv6 proporcionado por Amazon. Para obtener más información, consulte Creación de grupos de direcciones IPv6 en su IPAM.	25 de enero de 2023

Característica	Descripción	Fecha de lanzamiento
Versión inicial	En esta versión, se presenta el Administrador de direcciones IP (IPAM) de Amazon VPC.	2 de diciembre de 2021