Realojar sus aplicaciones en una arquitectura de cuentas múltiples AWS mediante puntos finales de interfaz de VPC

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Realojar sus aplicaciones en una arquitectura de cuentas múltiples AWS mediante puntos finales de interfaz de VPC

Table of Contents

Realojar sus aplicaciones en una arquitectura de múltiples cuentas en AWS mediante puntos finales de interfaz de VPC

Dipin Jain y Saurabh Shankar, Amazon Web Services

Febrero de 2025 (historial del documento)

Muchas organizaciones realojan (elevan y trasladan) sus aplicaciones a entornos AWS de red aislados o semiaislados, incluidos los centros de datos locales y otras infraestructuras en la nube o híbridas, mediante el uso de. AWS Transform MGN Por lo general, estas redes aisladas no permiten que el tráfico de salida llegue a los puntos finales públicos, tal como se describe en los requisitos de red de MGN. Puede abordar esta limitación mediante el uso de puntos finales de interfaz de nube privada virtual (VPC), como se explica en el patrón de AWS orientación prescriptiva Conectarse a planos de datos y control de MGN a través de una red privada.

Muchas organizaciones también utilizan una arquitectura de landing zone de múltiples cuentas (MALZ) para obtener beneficios de aislamiento, seguridad y facturación por cuenta. Para permitir la migración gradual mediante MGN a través de una red segura a varios destinos Cuentas de AWS, debe crear puntos finales de interfaz de VPC en cada destino. Cuenta de AWS Esto aumenta el costo y la complejidad de administrar esos recursos.

En esta guía, se analizan las opciones para centralizar los puntos finales de la interfaz de VPC para realojar las aplicaciones en una arquitectura de varias cuentas. AWS Estas opciones simplifican la arquitectura y reducen los costes en estos casos de uso.

Resultados empresariales específicos

Esta guía proporciona soluciones para tres casos de uso del realojamiento. Se centra en reducir los costos y los gastos operativos, y en mejorar la seguridad y la utilización de los recursos.

Casos de uso

- Sus aplicaciones están asignadas a diferentes unidades de negocio y usted desea migrarlas a diferentes cuentas de AWS destino de la misma manera Región de AWS para simplificar la facturación y el aislamiento.

La solución a este escenario implica crear puntos finales de VPC en una cuenta de AWS red central y utilizarlos AWS Transit Gateway para conectarse a las cuentas de la aplicación de destino.

- Desea migrar sus aplicaciones a diferentes cuentas de AWS destino en varias Regiones de AWS para mantenerlas cerca de los usuarios o para facilitar la recuperación ante desastres. Se trata de una extensión del primer caso de uso.

  La solución a este escenario implica crear puntos de enlace de VPC para cada uno de ellos Región de AWS en una cuenta de red AWS central y permitir el acceso entre cuentas mediante una pasarela de tránsito interconectada y Amazon Route 53.
- Sus aplicaciones están asignadas a diferentes unidades de negocio y usted quiere migrarlas a diferentes cuentas de AWS destino de la misma manera con Región de AWS fines de facturación y aislamiento. También desea utilizar menos VPC para la organización provisional de MGN y gestionar de forma centralizada el enrutamiento de las VPC de almacenamiento provisional a fin de reducir los costes y la sobrecarga administrativa.

  La solución a este escenario implica compartir los puntos finales de la VPC mediante una subred de área de ensayo compartida, con and (). AWS Organizations AWS Resource Access Manager AWS RAM

Destinatarios previstos

Esta guía está destinada a consultores de migración, arquitectos de aplicaciones, arquitectos de infraestructura y propietarios de aplicaciones que buscan soluciones para estos casos de uso.

Solución 1: Crear puntos finales de VPC en una cuenta de red central para una sola región

Caso de uso

Sus aplicaciones están asignadas a diferentes unidades de negocio y desea migrarlas a diferentes cuentas de AWS destino de la misma manera con Región de AWS fines de facturación y aislamiento.

Retos

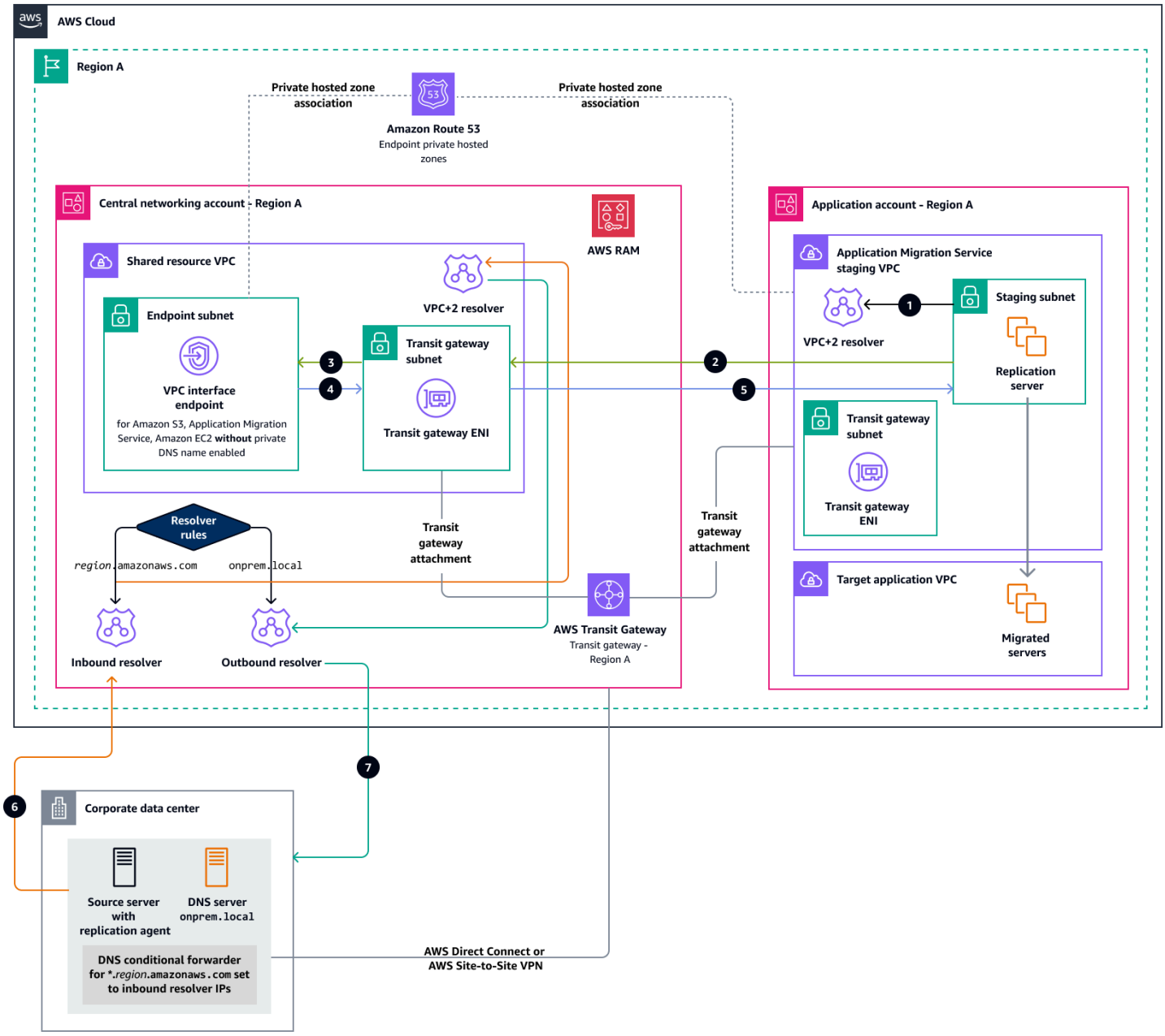
Para lograrlo a través de una red privada, tendría que crear varios puntos finales de interfaz de VPC en cada cuenta de destino. Esto aumenta los gastos administrativos y los costes de mantenimiento de los puntos finales. (Consulte los AWS PrivateLink precios).

Solución

Cree puntos finales de VPC en una cuenta de AWS red central y utilice Transit Gateway para conectarse a las cuentas de las aplicaciones de destino.

Arquitectura

El siguiente diagrama ilustra la arquitectura de esta solución.



En el diagrama, los números representan el siguiente flujo de tráfico:

1. La instancia de Amazon Elastic Compute Cloud (Amazon EC2) o el servidor de replicación MGN que necesite conectarse a Amazon Simple Storage Service (Amazon S3), MGN o Amazon EC2 a través de un punto final de interfaz ubicado en la cuenta de red central VPC primero debe resolver el nombre de dominio consultando la resolución de VPC+2. La zona alojada privada del punto final se asocia a la VPC de almacenamiento provisional de MGN en la misma región para completar la resolución del dominio.

> **Note**
>
> Para cada zona alojada privada que asocie a una VPC, el solucionador crea una regla y la asocia a la VPC. Si asocias la zona alojada privada a varias VPC, el solucionador asocia la regla a todas las VPC.

2. Cuando la instancia conoce la IP privada a la que debe conectarse, envía el tráfico a la ENI de la puerta de enlace de tránsito. El tráfico se envía a la puerta de enlace de tránsito y se reenvía a la VPC de recursos compartidos, en función de la tabla de rutas de la puerta de enlace de tránsito.
3. La pasarela de tránsito ENI de la VPC de recursos compartidos reenvía el tráfico al punto final de la interfaz correspondiente.
4. El punto final de la VPC devuelve la respuesta a la puerta de enlace de tránsito ENI.
5. El tráfico se reenvía a la puerta de enlace de tránsito. Como se especifica en la tabla de rutas de la pasarela de tránsito, el tráfico se envía a la VPC de puesta en escena de radio MGN. La pasarela de tránsito ENI envía la respuesta al destino, es decir, a la instancia EC2 o al servidor de replicación MGN.
6. Una aplicación cliente que se encuentra en el centro de datos corporativo resuelve un nombre de dominio en el formulario `<aws_service>.<aws_region>.amazonaws.com` (por ejemplo,`mgn.us-east-1.amazonaws.com`). Envía la consulta a su solucionador de DNS preconfigurado. El solucionador de DNS del centro de datos corporativo tiene una regla de reenvío que dirige cualquier consulta de DNS para `amazonaws.com` dominios al punto final de entrada de Route 53 Resolver. Transit Gateway reenvía la consulta a la VPC de recursos compartidos, que reenvía la consulta de DNS al punto final de entrada de Route 53 Resolver.

   El punto final de entrada del Route 53 Resolver utiliza el solucionador VPC+2. La zona alojada privada del punto final que está asociada a la VPC de recursos compartidos contiene los registros de DNS para `amazonaws.com` que Route 53 Resolver pueda resolver la consulta.
7. El punto final saliente de Route 53 Resolver devuelve la respuesta a la consulta de DNS a la aplicación cliente local.

Pasos para la implementación

Para configurar la arquitectura que se muestra en el diagrama anterior, siga estos pasos:

1. Conecte su centro de datos corporativo a la cuenta de red central a AWS través de AWS Direct Connect o AWS Site-to-Site VPN.
2. En la cuenta de red, utilice Transit Gateway para proporcionar conectividad entre las VPC. La puerta de enlace de tránsito se comparte Cuentas de AWS mediante el uso de la subred provisional de la cuenta de la aplicación de destino y AWS RAM, además, se conecta a ella a través de un adjunto de VPC.

> **Note**
>
> Cuentas de AWS No es necesario que Target forme parte de la misma organización. AWS Para obtener más información, consulte los recursos que se pueden compartir en la AWS RAM documentación.

3. Cree puntos de enlace de interfaz de VPC para Amazon EC2, MGN y Amazon S3 en la cuenta de red central sin habilitar un nombre de DNS privado.

> **Note**
>
> Al crear un punto final de VPC para un Servicio de AWS, puede habilitar el DNS privado. Cuando está habilitada, la configuración crea una zona alojada privada de Route 53 administrada para usted. Esta zona gestionada resuelve el nombre DNS de una VPC. Sin embargo, no funciona fuera de la VPC. Esta es la razón por la que se utilizan el uso compartido de zonas alojadas privadas y Route 53 Resolver para ayudar a obtener una resolución de nombres unificada para los puntos finales de VPC compartidos.

4. Cree una zona alojada privada para cada punto final (MGN, Amazon EC2, Amazon S3). Por ejemplo, para MGN en la región: `us-east-1`
   - Cree una zona alojada privada con el nombre `mgn.us-east-1.amazonaws.com` de dominio.
   - Cree un registro de host de tipo A que apunte el nombre de dominio a las IP de los puntos finales.
5. Cree reglas de entrada y salida de Route 53 Resolver para facilitar la resolución de DNS híbridos y comparta las reglas con las que sean necesarias Cuenta de AWS en la misma región.

Solución 2: Crear puntos finales de VPC en una cuenta de red central para varias regiones

Caso de uso

Desea migrar sus aplicaciones o servidores a diferentes cuentas de AWS destino en varias Regiones de AWS, para mantenerlos cerca de sus usuarios o para permitir la continuidad empresarial en situaciones de recuperación ante desastres. Se trata de una extensión del primer caso de uso.

Retos

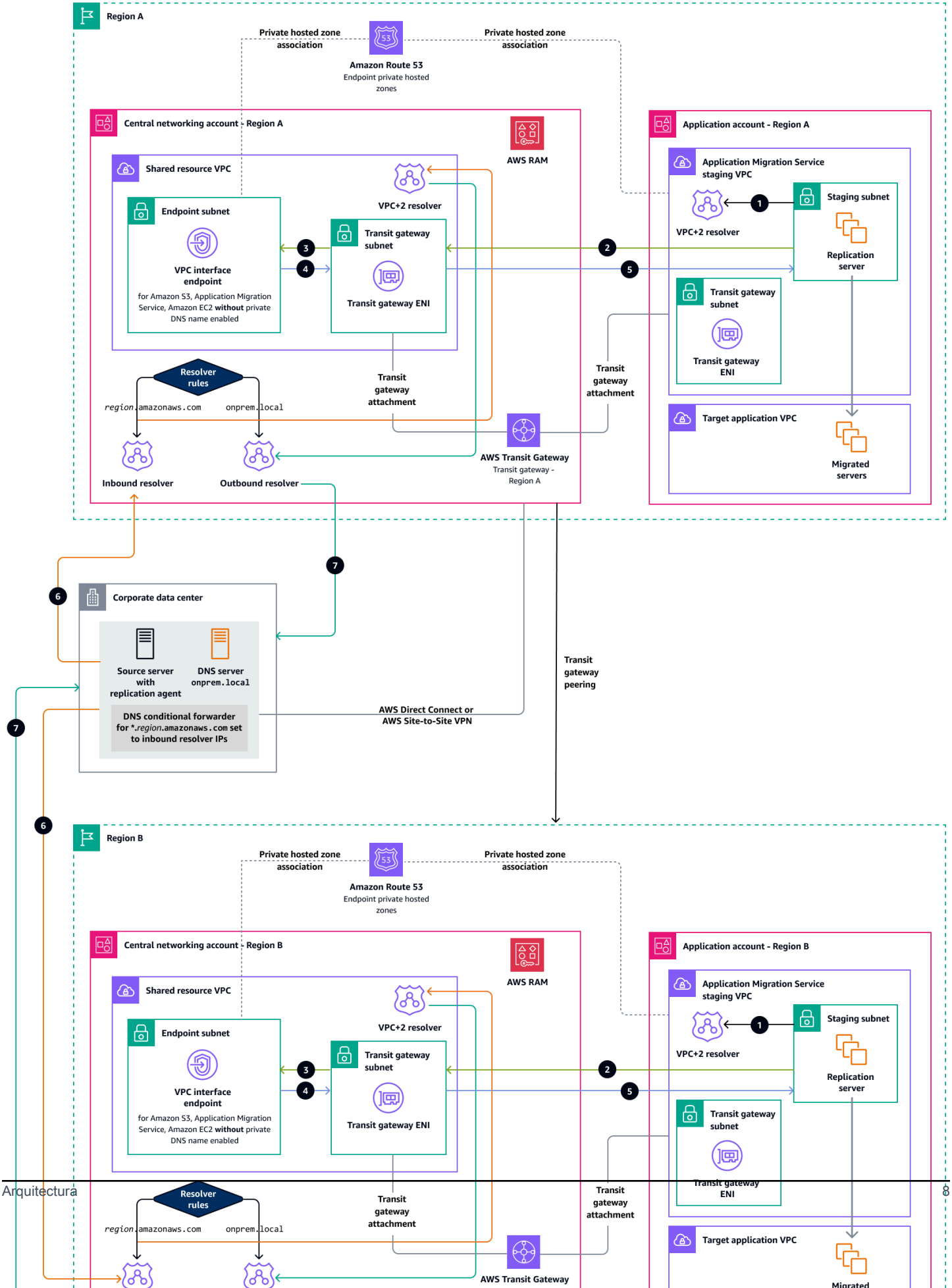
Para lograrlo a través de una red privada, tendría que crear varios puntos finales de interfaz de VPC en cada cuenta de destino. Esto se vuelve aún más complejo en un escenario multirregional y aumenta los gastos administrativos y los costes de mantenimiento de varios puntos finales. (Consulte los AWS PrivateLink precios).

Solución

Cree puntos finales de VPC para cada región en una cuenta de red central y habilite el acceso entre cuentas mediante una puerta de enlace de tránsito interconectada y Route 53.

Arquitectura

El siguiente diagrama ilustra la arquitectura de esta solución.


Region A
Private hosted zone association
Amazon Route 53
Endpoint private hosted zones
Private hosted zone association
Central networking account - Region A
AWS RAM
Application account - Region A
Shared resource VPC
VPC+2 resolver
Application Migration Service staging VPC
Endpoint subnet
VPC interface endpoint
for Amazon S3, Application Migration Service, Amazon EC2 without private DNS name enabled
Transit gateway subnet
Transit gateway ENI
Staging subnet
Replication server
Transit gateway attachment
Resolver rules
region.amazonaws.com
onprem.local
Inbound resolver
Outbound resolver
AWS Transit Gateway
Transit gateway - Region A
Target application VPC
Migrated servers
Corporate data center
Source server with replication agent
DNS server onprem.local
DNS conditional forwarder for *.region.amazonaws.com set to inbound resolver IPs
AWS Direct Connect or AWS Site-to-Site VPN
Transit gateway peering
Region B
Private hosted zone association
Amazon Route 53
Endpoint private hosted zones
Private hosted zone association
Central networking account - Region B
AWS RAM
Application account - Region B
Shared resource VPC
VPC+2 resolver
Application Migration Service staging VPC
Endpoint subnet
VPC interface endpoint
for Amazon S3, Application Migration Service, Amazon EC2 without private DNS name enabled
Transit gateway subnet
Transit gateway ENI
Staging subnet
Replication server
Transit gateway attachment
Resolver rules
region.amazonaws.com
onprem.local
AWS Transit Gateway
Target application VPC
Migrated

El flujo de tráfico es el mismo que en la solución 1, excepto que las cuentas de las dos regiones están conectadas mediante interconexión entre pasarelas de tránsito.

Pasos para la implementación

1. En la cuenta de red central, cree un punto final de interfaz de VPC para cada destino. Región de AWS
2. En la cuenta de red central, cree una zona alojada privada para cada punto final de cada región y asocie la zona a las VPC de la aplicación de destino en la misma región.
3. En la cuenta de red central, cree una puerta de enlace de tránsito para cada región de destino y compártala con las cuentas de destino de la misma región mediante AWS RAM.
4. Conecte las pasarelas de tránsito entre regiones mediante el emparejamiento de pasarelas de tránsito y actualice las tablas de rutas de las pasarelas de tránsito según sea necesario.
5. En la cuenta de red central, cree reglas de resolución para cada región de destino y compártalas con las cuentas de destino de la misma región mediante. AWS RAM

Solución 3: compartir los puntos finales de la interfaz de VPC

Caso de uso

Sus aplicaciones están asignadas a diferentes unidades de negocio y desea migrarlas a diferentes cuentas de AWS destino en la misma región con fines de facturación y aislamiento.

Retos

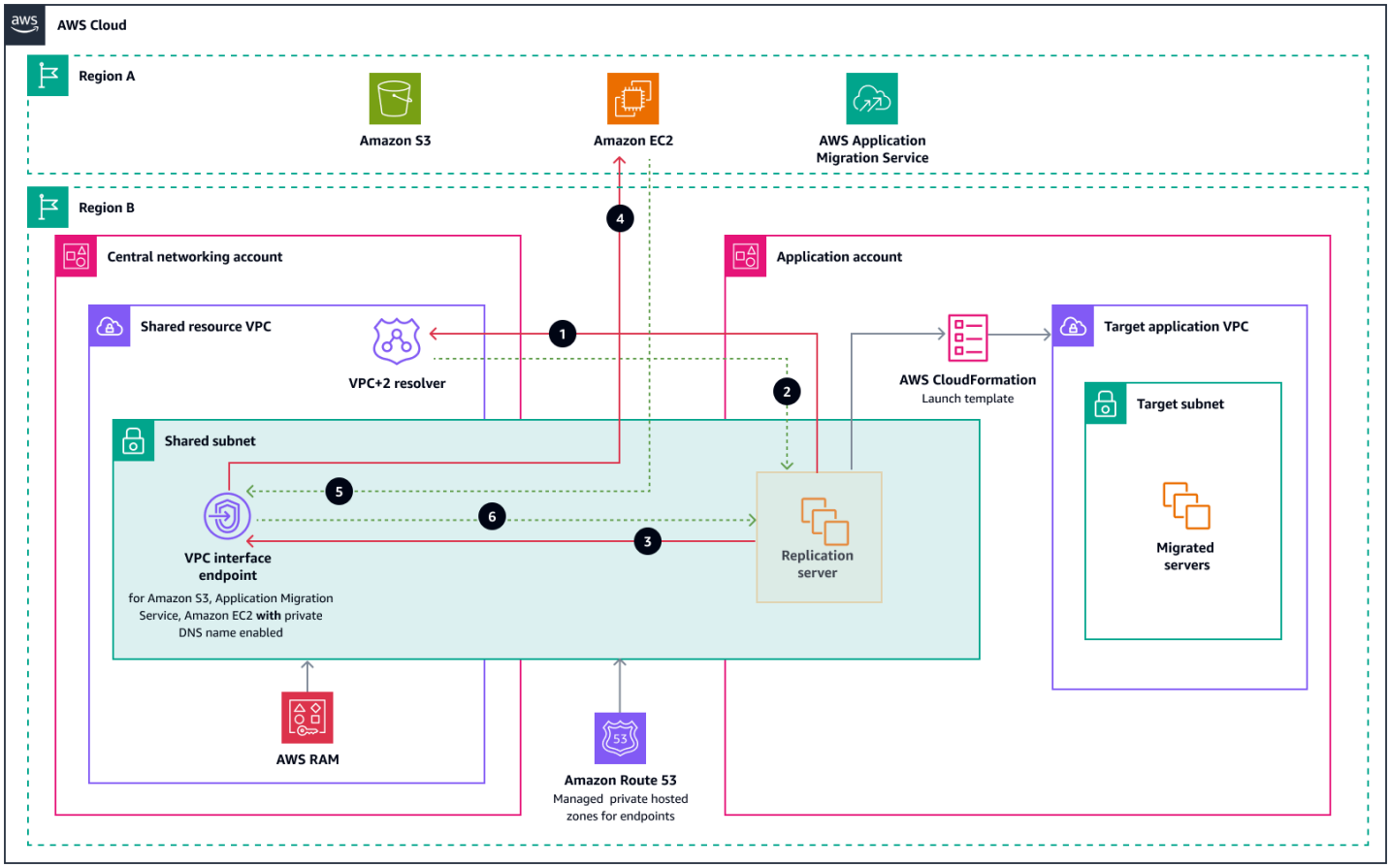
Las cuentas de carga de trabajo múltiples aumentan tanto la sobrecarga administrativa como el costo de los puntos finales de la interfaz de VPC individuales en cada cuenta. Por lo tanto, es posible que desee disponer de menos VPC de almacenamiento provisional para MGN y gestionar de forma centralizada el enrutamiento de las VPC de almacenamiento provisional a fin de reducir los costes y la sobrecarga administrativa.

Solución

Comparta los puntos finales de la VPC mediante una subred de área de ensayo compartida, y. AWS Organizations AWS RAM Para obtener más información sobre el uso compartido de VPC, consulte la documentación de Amazon VPC.

Arquitectura

El siguiente diagrama ilustra la arquitectura de esta solución.



El diagrama ilustra el siguiente flujo de tráfico:

1. El servidor de replicación de MGN consulta el DNS de la VPC+2 para resolver el punto final de la API para MGN, Amazon EC2 o Amazon S3.

2. El DNS de VPC+2 resuelve la IP privada del punto final con la ayuda de zonas AWS alojadas privadas administradas y responde al servidor de replicación MGN.

3-6. El servidor de replicación usa esa IP para conectarse a la Servicio de AWS API a través del punto final de la interfaz del servicio.

Pasos para la implementación

1. En la cuenta de red central, cree la VPC provisional y la subred para MGN.
2. Cree puntos de enlace para MGN, Amazon EC2 o Amazon S3 con los nombres de DNS privados habilitados. Esto crea una zona alojada privada AWS administrada y la asocia a la VPC provisional.

3. Comparta la subred provisional con las cuentas de aplicaciones de destino de la misma organización y. AWS Región de AWS
4. Para la conectividad híbrida entre el centro de datos local AWS y el centro de datos local (no se muestra en el diagrama anterior), utilice Transit Gateway Direct Connect o AWS Site-to-Site VPN con los puntos finales de Route 53 Resolver, como se muestra en las soluciones 1 y 2.

Limitaciones

- Las Cuentas de AWS VPC participantes y las VPC propietarias deben formar parte de la misma organización en. AWS Organizations
- Para obtener una lista de los recursos que se pueden compartir, consulte la documentación de Amazon VPC.
- Para conocer las limitaciones de uso compartido de VPC, consulte la documentación de Amazon VPC.

Consideraciones sobre el diseño

- Para reducir la sobrecarga operativa, cree un recurso una vez y utilícelo AWS RAM para compartirlo con otras cuentas. Esto elimina la necesidad de aprovisionar recursos duplicados en cada cuenta y reduce la sobrecarga operativa.
- Simplifique la administración de la seguridad de sus recursos compartidos mediante un único conjunto de políticas y permisos. Si crea recursos duplicados en sus cuentas independientes, debe implementar políticas y permisos idénticos y mantenerlos sincronizados en todas las cuentas. En su lugar, puede administrar todos los usuarios que comparten un AWS RAM recurso mediante un único conjunto de políticas y permisos. AWS RAM ofrece una experiencia coherente para compartir diferentes tipos de AWS recursos.
- Proporcione visibilidad y auditabilidad. Consulta los detalles de uso de tus recursos compartidos integrándolos AWS RAM con Amazon CloudWatch y AWS CloudTrail. Para obtener más información, consulte Monitorear AWS RAM el uso EventBridge y el registro de las llamadas a la AWS RAM API AWS CloudTrail en la AWS RAM documentación.

Preguntas frecuentes

P: ¿Con quién puedo compartir recursos?

R: Puedes compartir recursos con cualquier persona Cuenta de AWS. Si formas parte de una organización AWS Organizations y está activado el uso compartido dentro de tu organización, también puedes compartir recursos con las unidades organizativas (OUs) o con toda la organización. En el caso de los tipos de recursos compatibles, también puedes compartir los recursos con los roles AWS Identity and Access Management (de IAM) y los usuarios de IAM. Si compartes recursos con cuentas ajenas a tu organización, esas cuentas reciben una invitación para unirse al recurso compartido. Una vez que acepten la invitación, pueden empezar a usar los recursos compartidos.

P: ¿Se me cobrará algún cargo por compartir mis recursos con otras Cuentas de AWS personas?

R: No. Puede compartir recursos sin costo adicional.

P: ¿Puedo dejar de compartir un recurso?

R: Sí. Para dejar de compartir un recurso, elimínelo del recurso compartido o elimine el recurso compartido.

P: ¿Cómo puedo garantizar la seguridad en AWS RAM?

R: La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y seguridad en la nube. Para obtener más información, consulte Seguridad AWS RAM en la AWS RAM documentación.

Prácticas recomendadas

- Evite los puntos únicos de fallo. Para los puntos finales de VPC y los puntos finales de Route 53 Resolver, utilice dos o más zonas de disponibilidad para obtener una alta disponibilidad.
- No utilice los puntos de enlace de Route 53 Resolver para reenviar consultas de DNS entre ellos. VPCs Le recomendamos encarecidamente que utilice el servidor DNS de Amazon (resolución .2) como resolución de DNS para todas las instancias de Amazon EC2. Este solucionador proporciona el nivel más alto de disponibilidad y escalabilidad con la latencia más baja.
- Para obtener más información sobre las prácticas recomendadas, consulte las prácticas recomendadas para Resolver en la documentación de Route 53.

Recursos

- Acceso y Servicio de AWS uso de un punto final de VPC de interfaz (documentación de Amazon VPC)
- Comparta sus subredes de VPC con otras cuentas (documentación de Amazon VPC)
- Recursos AWS RAM de Amazon VPC que se pueden compartir (documentación)
- Integración AWS Transit Gateway con AWS PrivateLink y Amazon Route 53 Resolver (AWS entrada de blog)
- Centralización de los puntos finales de VPC AWS Transit Gateway con AWS (arquitectura de referencia)
- Conéctese a los planos de datos y control de MGN a través de una red privada (Guía AWS prescriptiva)

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	18 de febrero de 2025

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.