Hospedando novamente seus aplicativos em uma arquitetura de várias contas AWS usando endpoints de interface VPC

AWS Recomendações

AWS Recomendações: Hospedando novamente seus aplicativos em uma arquitetura de várias contas AWS usando endpoints de interface VPC

Table of Contents

Introdução 1
Resultados de negócios desejados 1
Público-alvo 2
Solução 1: conta de rede central, região única 3
Caso de uso 3
Desafios 3
Solução 3
Arquitetura 3
Etapas de implementação 5
Solução 2: conta de rede central, várias regiões 7
Caso de uso 7
Desafios 7
Solução 7
Arquitetura 7
Etapas de implementação 9
Solução 3: compartilhamento de endpoints da interface VPC 10
Caso de uso 10
Desafios 10
Solução 10
Arquitetura 10
Etapas de implementação 11
Limitações 12
Considerações sobre design 12
Perguntas frequentes 13
Práticas recomendadas 14
Recursos 15
Histórico do documento 16
..... xvii

Hospedando novamente seus aplicativos em uma arquitetura de várias contas no AWS usando endpoints de interface VPC

Dipin Jain e Saurabh Shankar, Amazon Web Services

Fevereiro de 2025 (histórico do documento)

Muitas organizações rehospedam (elevam e transferem) seus aplicativos para ambientes AWS de rede isolados ou semi-isolados, incluindo data centers locais e outras infraestruturas de nuvem ou híbridas, usando. AWS Transform MGN Essas redes isoladas normalmente não permitem nenhum tráfego de saída para os endpoints públicos descritos nos requisitos de rede do MGN. Você pode resolver essa limitação usando endpoints de interface de nuvem privada virtual (VPC), conforme discutido no padrão de orientação AWS prescritiva Conecte-se aos dados e planos de controle da MGN em uma rede privada.

Muitas organizações também usam uma arquitetura multi-account landing zone (MALZ) para benefícios de isolamento, segurança e cobrança por conta. Para permitir a migração lift-and-shift usando o MGN em uma rede segura para vários destinos Contas da AWS, você deve criar endpoints de interface VPC em cada destino. Conta da AWS Isso aumenta o custo e a complexidade do gerenciamento desses recursos.

Este guia discute as opções para centralizar os endpoints da interface VPC para rehospedar seus aplicativos em uma arquitetura de várias contas em. AWS Essas opções simplificam a arquitetura e reduzem os custos desses casos de uso.

Resultados de negócios desejados

Este guia fornece soluções para três casos de uso de rehospedagem. Ele se concentra na redução de custos e na sobrecarga operacional e na melhoria da segurança e da utilização de recursos.

Casos de uso:

- Seus aplicativos são mapeados para diferentes unidades de negócios e você deseja migrá-los para contas de AWS destino diferentes da mesma forma para Região da AWS simplificar o faturamento e o isolamento.

A solução para esse cenário envolve a criação de VPC endpoints em uma conta de AWS rede central e o uso AWS Transit Gateway para se conectar às contas do aplicativo de destino.

- Você deseja migrar seus aplicativos para diferentes contas de AWS destino em várias Regiões da AWS para manter seus aplicativos próximos aos seus usuários ou para facilitar a recuperação de desastres. Essa é uma extensão do primeiro caso de uso.

  A solução para esse cenário envolve a criação de VPC endpoints para cada um Região da AWS em uma conta de rede AWS central e a habilitação do acesso entre contas usando um gateway de trânsito emparelhado e o Amazon Route 53.
- Seus aplicativos são mapeados para diferentes unidades de negócios e você deseja migrá-los para contas de AWS destino diferentes da mesma forma Região da AWS para fins de cobrança e isolamento. Você também quer usar menos VPCs para a preparação do MGN e gerenciar centralmente o roteamento das VPCs de preparação para reduzir os custos e a sobrecarga administrativa.

  A solução para esse cenário envolve o compartilhamento de VPC endpoints usando uma sub-rede de área de armazenamento compartilhada, com e (). AWS Organizations AWS Resource Access Manager AWS RAM

Público-alvo

Este guia é para consultores de migração, arquitetos de aplicativos, arquitetos de infraestrutura e proprietários de aplicativos que estão procurando soluções para esses casos de uso.

Solução 1: criar endpoints VPC em uma conta de rede central para uma única região

Caso de uso

Seus aplicativos são mapeados para diferentes unidades de negócios e você deseja migrá-los para contas de AWS destino diferentes da mesma forma Região da AWS para fins de cobrança e isolamento.

Desafios

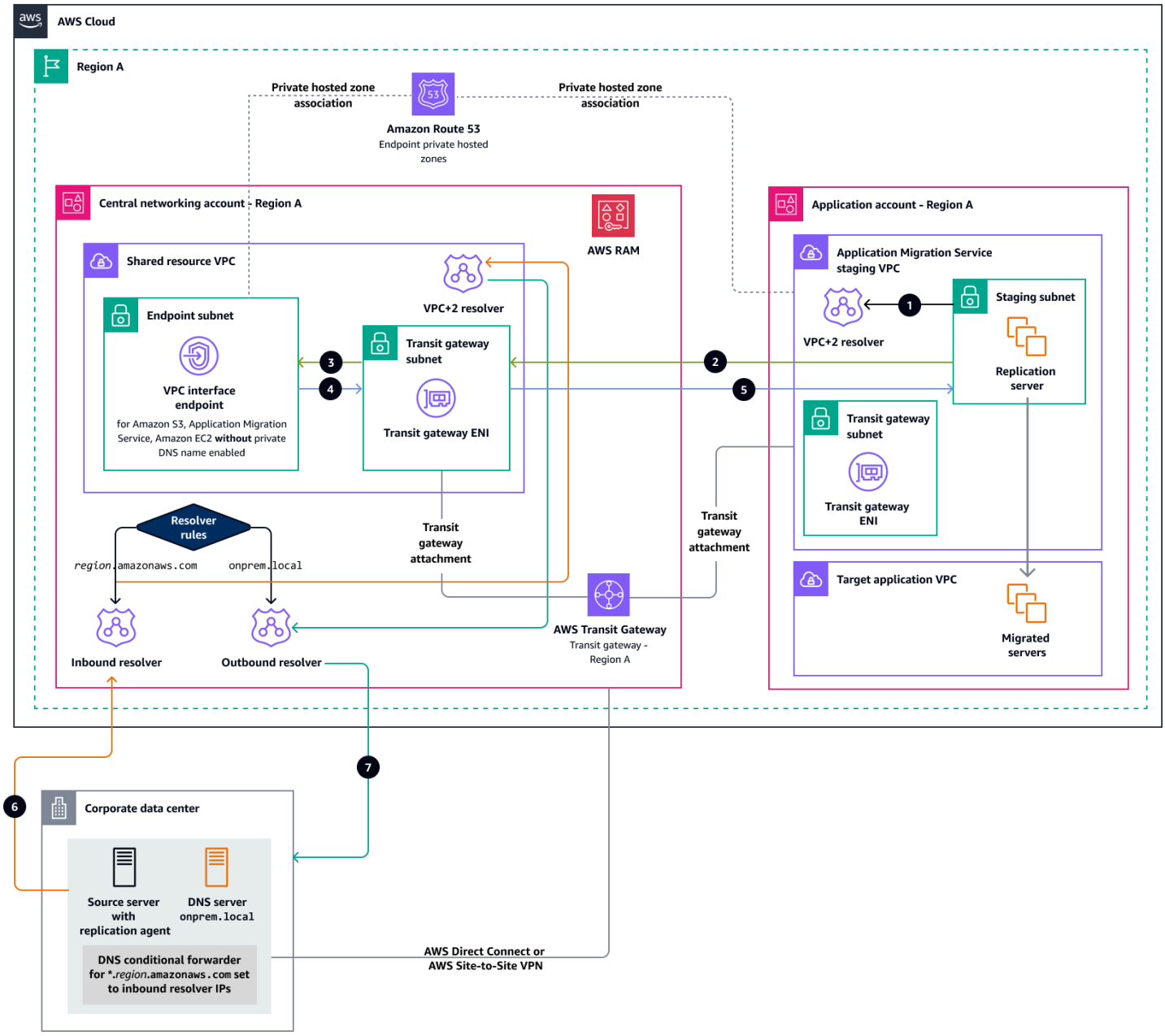
Para conseguir isso em uma rede privada, você precisaria criar vários endpoints de interface VPC em cada conta de destino. Isso aumenta a sobrecarga administrativa e os custos de manutenção dos endpoints. (Veja AWS PrivateLink os preços.)

Solução

Crie endpoints VPC em uma conta de AWS rede central e use o Transit Gateway para se conectar às contas do aplicativo de destino.

Arquitetura

O diagrama a seguir ilustra a arquitetura dessa solução.



No diagrama, os números representam o seguinte fluxo de tráfego:

1. A instância do Amazon Elastic Compute Cloud (Amazon EC2) ou o servidor de replicação MGN que precisa se conectar ao Amazon Simple Storage Service (Amazon S3), MGN ou Amazon EC2 por meio de um endpoint de interface localizado na conta de rede central. A VPC precisa primeiro resolver o nome de domínio consultando o resolvedor VPC+2. A zona hospedada privada do endpoint está associada à MGN que prepara a VPC na mesma região para concluir a resolução do domínio.

> **Note**
>
> Para cada zona hospedada privada que você associa a uma VPC, o resolvedor cria uma regra e a associa à VPC. Se você associar a zona hospedada privada a várias VPCs, o resolvedor associará a regra a todas as VPCs.

2. Quando a instância conhece o IP privado ao qual se conectar, ela envia o tráfego para a ENI do gateway de trânsito. O tráfego é enviado para o gateway de trânsito e encaminhado para a VPC de recursos compartilhados, com base na tabela de rotas do gateway de trânsito.
3. A ENI do gateway de trânsito na VPC de recursos compartilhados encaminha o tráfego para o endpoint da interface correspondente.
4. O VPC endpoint envia a resposta de volta para a ENI do gateway de trânsito.
5. O tráfego é encaminhado para o gateway de trânsito. Conforme especificado na tabela de rotas do Transit Gateway, o tráfego é enviado para a VPC de teste do spoke MGN. A resposta é enviada pela ENI do gateway de trânsito para o destino, ou seja, para a instância do EC2 ou para o servidor de replicação MGN.
6. Um aplicativo cliente localizado no data center corporativo resolve um nome de domínio no formato `<aws_service>.<aws_region>.amazonaws.com` (por exemplo,`mgn.us-east-1.amazonaws.com`). Ele envia a consulta para seu resolvedor de DNS pré-configurado. O resolvedor de DNS no data center corporativo tem uma regra de encaminhamento que aponta qualquer consulta de DNS para `amazonaws.com` domínios para o endpoint de entrada do Resolvedor do Route 53. O Transit Gateway encaminha a consulta para o recurso compartilhado VPC, que encaminha a consulta DNS no endpoint de entrada do Route 53 Resolver.

   O endpoint de entrada do Route 53 Resolver usa o resolvedor VPC+2. A zona hospedada privada do endpoint associada ao recurso compartilhado VPC contém os registros de DNS `amazonaws.com` para que o Route 53 Resolver possa resolver a consulta.
7. O endpoint de saída do Resolvedor do Route 53 retorna a resposta da consulta DNS para o aplicativo cliente local.

Etapas de implementação

Para configurar a arquitetura mostrada no diagrama anterior, siga estas etapas:

1. Conecte seu data center corporativo à conta de rede central em AWS AWS Direct Connect ou AWS Site-to-Site VPN.
2. Na conta de rede, use o Transit Gateway para fornecer conectividade entre VPCs. O gateway de trânsito é compartilhado Contas da AWS usando AWS RAM e conectado posteriormente à sub-rede intermediária da conta do aplicativo de destino por meio de um anexo VPC.

> **Note**
>
> Contas da AWS O Target não precisa fazer parte da mesma AWS organização. Para obter mais informações, consulte Recursos compartilháveis na AWS RAM documentação.

3. Crie endpoints de interface VPC para Amazon EC2, MGN e Amazon S3 na conta da rede central sem habilitar um nome DNS privado.

> **Note**
>
> Ao criar um VPC endpoint para um AWS service (Serviço da AWS), você pode habilitar o DNS privado. Quando ativada, a configuração cria uma zona hospedada privada gerenciada do Route 53 para você. Essa zona gerenciada resolve o nome DNS em uma VPC. No entanto, ele não funciona fora da VPC. Esse é o motivo para usar o compartilhamento de zona hospedada privada e o Route 53 Resolver para ajudar a obter uma resolução unificada de nomes para endpoints de VPC compartilhados.

4. Crie uma zona hospedada privada para cada endpoint (MGN, Amazon EC2, Amazon S3). Por exemplo, para a MGN na `us-east-1` região:
   - Crie uma zona hospedada privada com o nome do domínio`mgn.us-east-1.amazonaws.com`.
   - Crie um registro de host do tipo A que direcione o nome do domínio para os IPs do endpoint.
5. Crie regras de entrada e saída do Route 53 Resolver para facilitar a resolução de DNS híbrido e compartilhe as regras com os necessários Conta da AWS na mesma região.

Solução 2: criar VPC endpoints em uma conta de rede central para várias regiões

Caso de uso

Você deseja migrar seus aplicativos ou servidores para diferentes contas de AWS destino em várias Regiões da AWS, para mantê-los próximos aos seus usuários ou para permitir a continuidade dos negócios em cenários de recuperação de desastres. Essa é uma extensão do primeiro caso de uso.

Desafios

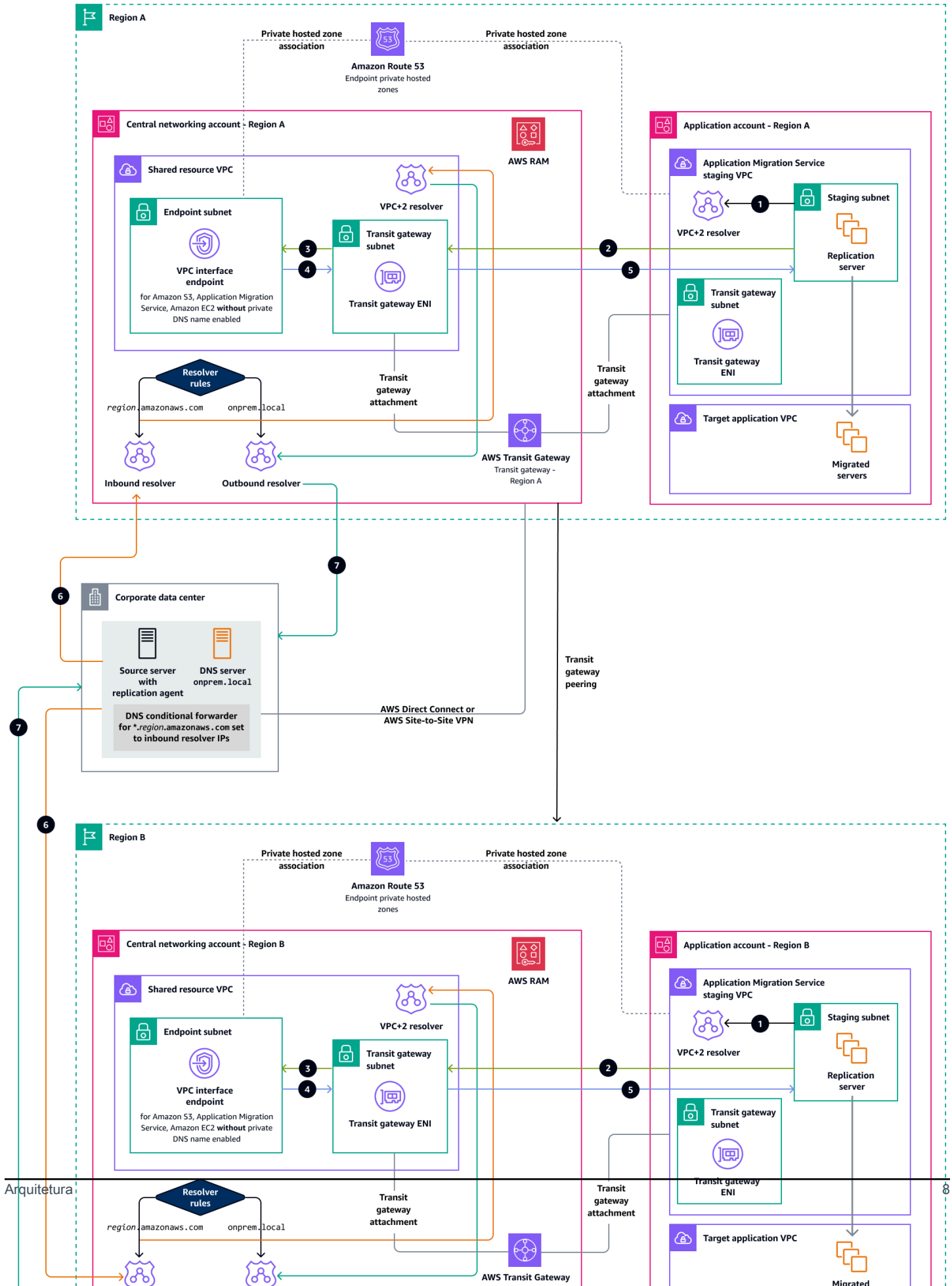
Para conseguir isso em uma rede privada, você precisaria criar vários endpoints de interface VPC em cada conta de destino. Isso se torna ainda mais complexo em um cenário multirregional e aumenta a sobrecarga administrativa e os custos de manutenção de vários endpoints. (Veja AWS PrivateLink os preços.)

Solução

Crie endpoints VPC para cada região em uma conta de rede central e habilite o acesso entre contas usando um gateway de trânsito emparelhado e o Route 53.

Arquitetura

O diagrama a seguir ilustra a arquitetura dessa solução.


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

O fluxo de tráfego é o mesmo da solução 1, exceto que as contas nas duas regiões são conectadas pelo peering do gateway de trânsito.

Etapas de implementação

1. Na conta de rede central, crie um endpoint de interface VPC para cada destino. Região da AWS
2. Na conta de rede central, crie uma zona hospedada privada para cada endpoint em cada região e associe a zona às VPCs do aplicativo de destino na mesma região.
3. Na conta de rede central, crie um gateway de trânsito para cada região de destino e compartilhe o gateway com contas de destino na mesma região usando AWS RAM.
4. Conecte gateways de trânsito entre regiões usando o emparelhamento do gateway de trânsito e atualize as tabelas de rotas do gateway de trânsito conforme necessário.
5. Na conta de rede central, crie regras de resolução para cada região de destino e compartilhe essas regras com contas de destino na mesma região usando AWS RAM.

Solução 3: compartilhamento de endpoints da interface VPC

Caso de uso

Seus aplicativos são mapeados para diferentes unidades de negócios e você deseja migrá-los para contas de AWS destino diferentes na mesma região para fins de cobrança e isolamento.

Desafios

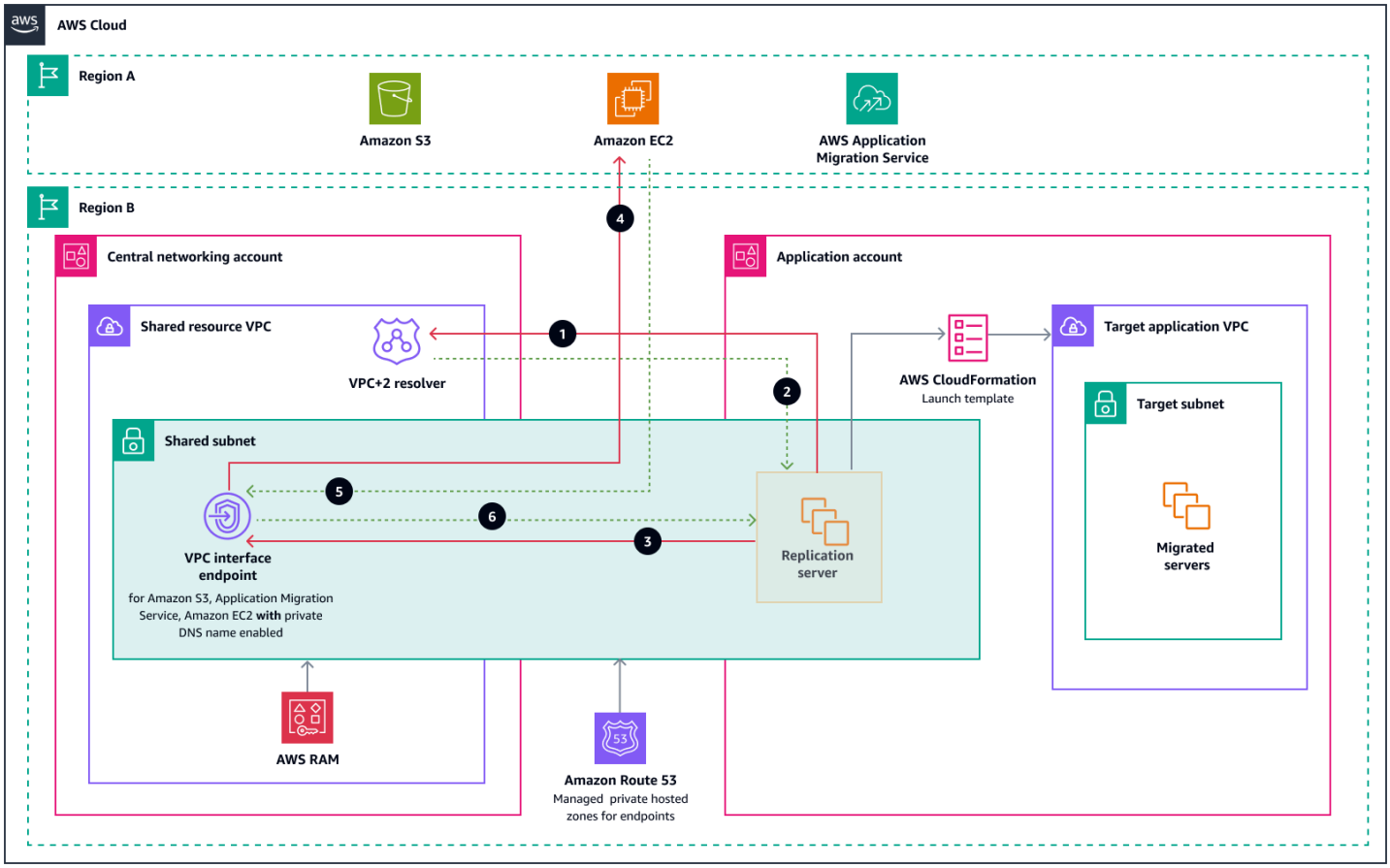
Várias contas de carga de trabalho aumentam a sobrecarga administrativa e o custo de endpoints individuais da interface VPC em cada conta. Portanto, talvez você queira ter menos VPCs de teste para MGN e gerenciar centralmente o roteamento para as VPCs de preparação para reduzir custos e despesas administrativas.

Solução

Compartilhe endpoints de VPC usando uma sub-rede de área de armazenamento compartilhada, e. AWS Organizations AWS RAM Para obter mais informações sobre o compartilhamento de VPC, consulte a documentação da Amazon VPC.

Arquitetura

O diagrama a seguir ilustra a arquitetura dessa solução.



O diagrama ilustra o seguinte fluxo de tráfego:

1. O servidor de replicação MGN consulta o DNS da VPC+2 para resolver o endpoint da API para MGN, Amazon EC2 ou Amazon S3.

2. O VPC+2 DNS resolve o IP privado do endpoint com a ajuda de zonas hospedadas privadas AWS gerenciadas e responde ao servidor de replicação MGN.

3-6. O servidor de replicação usa esse IP para se conectar à AWS service (Serviço da AWS) API por meio do endpoint da interface do serviço.

Etapas de implementação

1. Na conta de rede central, crie a VPC de teste e a sub-rede para MGN.
2. Crie endpoints para MGN, Amazon EC2 ou Amazon S3 com nomes DNS privados habilitados. Isso cria uma zona hospedada privada AWS gerenciada e a associa à VPC de teste.

3. Compartilhe a sub-rede de teste com contas de aplicativos de destino na mesma AWS organização e. Região da AWS
4. Para conectividade híbrida entre AWS e seu data center local (não mostrada no diagrama anterior), use o Transit Gateway Direct Connect ou AWS Site-to-Site VPN com os endpoints do Route 53 Resolver, conforme mostrado na solução 1 e na solução 2.

Limitações

- As Contas da AWS VPCs participantes e as VPCs proprietárias devem fazer parte da mesma organização em. AWS Organizations
- Para obter uma lista de recursos compartilháveis, consulte a documentação da Amazon VPC.
- Para as limitações de compartilhamento da VPC, consulte a documentação da Amazon VPC.

Considerações sobre design

- Para reduzir sua sobrecarga operacional, crie um recurso uma vez e use-o AWS RAM para compartilhar esse recurso com outras contas. Isso elimina a necessidade de provisionar recursos duplicados em todas as contas e reduz a sobrecarga operacional.
- Simplifique o gerenciamento da segurança de seus recursos compartilhados usando um único conjunto de políticas e permissões. Se você criar recursos duplicados em suas contas separadas, precisará implementar políticas e permissões idênticas e mantê-las sincronizadas em todas as contas. Em vez disso, você pode gerenciar todos os usuários que compartilham um AWS RAM recurso por meio de um único conjunto de políticas e permissões. AWS RAM oferece uma experiência consistente para compartilhar diferentes tipos de AWS recursos.
- Forneça visibilidade e auditabilidade. Veja os detalhes de uso de seus recursos compartilhados por meio da integração AWS RAM com a Amazon CloudWatch e. AWS CloudTrail Para obter mais informações, consulte Monitoramento, AWS RAM uso EventBridge e registro de chamadas da AWS RAM API AWS CloudTrail na AWS RAM documentação.

Perguntas frequentes

P: Com quem posso compartilhar recursos?

R: Você pode compartilhar recursos com qualquer um Conta da AWS. Se você faz parte de uma organização AWS Organizations e o compartilhamento dentro de sua organização está ativado, você também pode compartilhar recursos com unidades organizacionais (OUs) ou com toda a organização. Para tipos de recursos compatíveis, você também pode compartilhar recursos com funções AWS Identity and Access Management (IAM) e usuários do IAM. Se você compartilha recursos com contas que estão fora da sua organização, essas contas recebem um convite para participar do compartilhamento de recursos. Depois de aceitarem o convite, eles poderão começar a usar os recursos compartilhados.

P: Serei cobrado por compartilhar meus recursos com outras Contas da AWS pessoas?

R: Não. Você pode compartilhar recursos sem custo adicional.

P: Posso parar de compartilhar um recurso?

R: Sim. Para parar de compartilhar um recurso, remova-o do compartilhamento de recursos ou exclua o compartilhamento de recursos.

P: Como posso garantir a segurança em AWS RAM?

R: A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança na nuvem e segurança na nuvem. Para obter mais informações, consulte Segurança AWS RAM na AWS RAM documentação.

Práticas recomendadas

- Evite pontos únicos de falha. Para endpoints VPC e endpoints do Route 53 Resolver, use duas ou mais zonas de disponibilidade para alta disponibilidade.
- Não use os endpoints do Route 53 Resolver para encaminhar consultas de DNS entre eles. VPCs É altamente recomendável que você use o Amazon DNS Server (resolvedor .2) como resolvedor de DNS para todas as instâncias dentro da Amazon. EC2 Esse resolvedor fornece o mais alto nível de disponibilidade e escalabilidade com a menor latência.
- Para obter mais práticas recomendadas, consulte Melhores práticas para o Resolver na documentação do Route 53.

Recursos

- Acesse e AWS service (Serviço da AWS) use uma interface VPC endpoint (documentação da Amazon VPC)
- Compartilhe suas sub-redes VPC com outras contas (documentação da Amazon VPC)
- Recursos AWS RAM compartilháveis da Amazon VPC (documentação)
- Integração AWS Transit Gateway com AWS PrivateLink e Amazon Route 53 Resolver (postagem AWS do blog)
- Centralizando endpoints de VPC AWS Transit Gateway com AWS (arquitetura de referência)
- Conecte-se aos planos de dados e controle da MGN em uma rede privada (orientação AWS prescritiva)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Publicação inicial	—	18 de fevereiro de 2025

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.