VPC 인터페이스 엔드포인트를 사용하여의 다중 계정 아키텍처 AWS 에서 애플리케이션 리호스팅

AWS 권장 가이드

AWS 권장 가이드: VPC 인터페이스 엔드포인트를 사용하여의 다중 계정 아키텍처 AWS 에서 애플리케이션 리호스팅

Table of Contents

VPC 인터페이스 엔드포인트를 사용하여의 다중 계정 아키텍처 AWS 에서 애플리케이션 리호스팅

Dipin Jain과 Saurabh Shankar, Amazon Web Services

2025년 2월(문서 기록)

많은 조직이를 사용하여 온프레미스 데이터 센터 및 기타 클라우드 또는 하이브리드 인프라를 포함하여 AWS 격리된 또는 반격리된 네트워크 환경에서 애플리케이션을 로 리호스팅(리프트 앤 시프트)합니다AWS Transform MGN. 이러한 격리된 네트워크는 일반적으로 MGN에 대한 네트워크 요구 사항에 설명된 퍼블릭 엔드포인트로의 송신 트래픽을 허용하지 않습니다. AWS 권장 가이드 패턴 프라이빗 네트워크를 통해 MGN 데이터 및 컨트롤 플레인에 연결에 설명된 대로 Virtual Private Cloud(VPC) 인터페이스 엔드포인트를 사용하여 이러한 제한을 해결할 수 있습니다.

또한 많은 조직에서 격리, 보안 및 계정당 결제 혜택을 위해 다중 계정 랜딩 존(MALZ) 아키텍처를 사용합니다. 보안 네트워크를 통해 MGN을 사용하여 여러 대상으로 lift-and-shift 마이그레이션을 활성화하려면 모든 대상에 VPC 인터페이스 엔드포인트를 생성 AWS 계정해야 합니다 AWS 계정. 이렇게 하면 이러한 리소스를 관리하는 데 드는 비용과 복잡성이 증가합니다.

이 가이드에서는 다중 계정 아키텍처에서 애플리케이션을 리호스팅하기 위한 VPC 인터페이스 엔드포인트를 중앙 집중화하는 옵션을 설명합니다 AWS. 이러한 옵션은 아키텍처를 간소화하고 이러한 사용 사례에 대한 비용을 절감합니다.

목표 비즈니스 성과

이 가이드에서는 세 가지 리호스팅 사용 사례에 대한 솔루션을 제공합니다. 비용 및 운영 오버헤드를 줄이고 보안 및 리소스 사용률을 개선하는 데 중점을 둡니다.

사용 사례:

- 애플리케이션은 서로 다른 사업부에 매핑되며 결제 및 격리 AWS 리전 를 간소화하기 위해 동일한의 서로 다른 AWS 대상 계정으로 마이그레이션하려고 합니다.

  이 시나리오의 솔루션에는 중앙 AWS 네트워킹 계정에 VPC 엔드포인트를 생성하고 AWS Transit Gateway 를 사용하여 대상 애플리케이션 계정에 연결하는 작업이 포함됩니다.
- 애플리케이션을 여러의 다른 AWS 대상 계정으로 마이그레이션 AWS 리전 하여 애플리케이션을 사용자와 가깝게 유지하거나 재해 복구를 용이하게 하려고 합니다. 이는 첫 번째 사용 사례의 확장입니다.

이 시나리오의 솔루션에는 AWS 중앙 네트워킹 계정 AWS 리전 에서 각에 대한 VPC 엔드포인트를 생성하고 피어링된 전송 게이트웨이 및 Amazon Route 53을 사용하여 교차 계정 액세스를 활성화하는 것이 포함됩니다.

- 애플리케이션은 서로 다른 사업부에 매핑되며 결제 및 격리를 AWS 리전 위해 동일한의 서로 다른 AWS 대상 계정으로 마이그레이션하려고 합니다. 또한 MGN 스테이징에 더 적은 VPCs 사용하고 스테이징 VPCs하여 비용과 관리 오버헤드를 줄이고자 합니다.

  이 시나리오의 솔루션에는 AWS Organizations 및 AWS Resource Access Manager ()와 공유 스테이징 영역 서브넷을 사용하여 VPC 엔드포인트를 공유하는 것이 포함됩니다AWS RAM.

대상 독자

이 가이드는 이러한 사용 사례에 대한 솔루션을 찾고 있는 마이그레이션 컨설턴트, 애플리케이션 아키텍트, 인프라 아키텍트 및 애플리케이션 소유자를 위한 것입니다.

솔루션 1: 단일 리전의 중앙 네트워킹 계정에서 VPC 엔드포인트 생성

사용 사례:

애플리케이션은 서로 다른 사업부에 매핑되며 결제 및 격리를 AWS 리전 위해 동일한의 서로 다른 AWS 대상 계정으로 마이그레이션하려고 합니다.

도전 과제

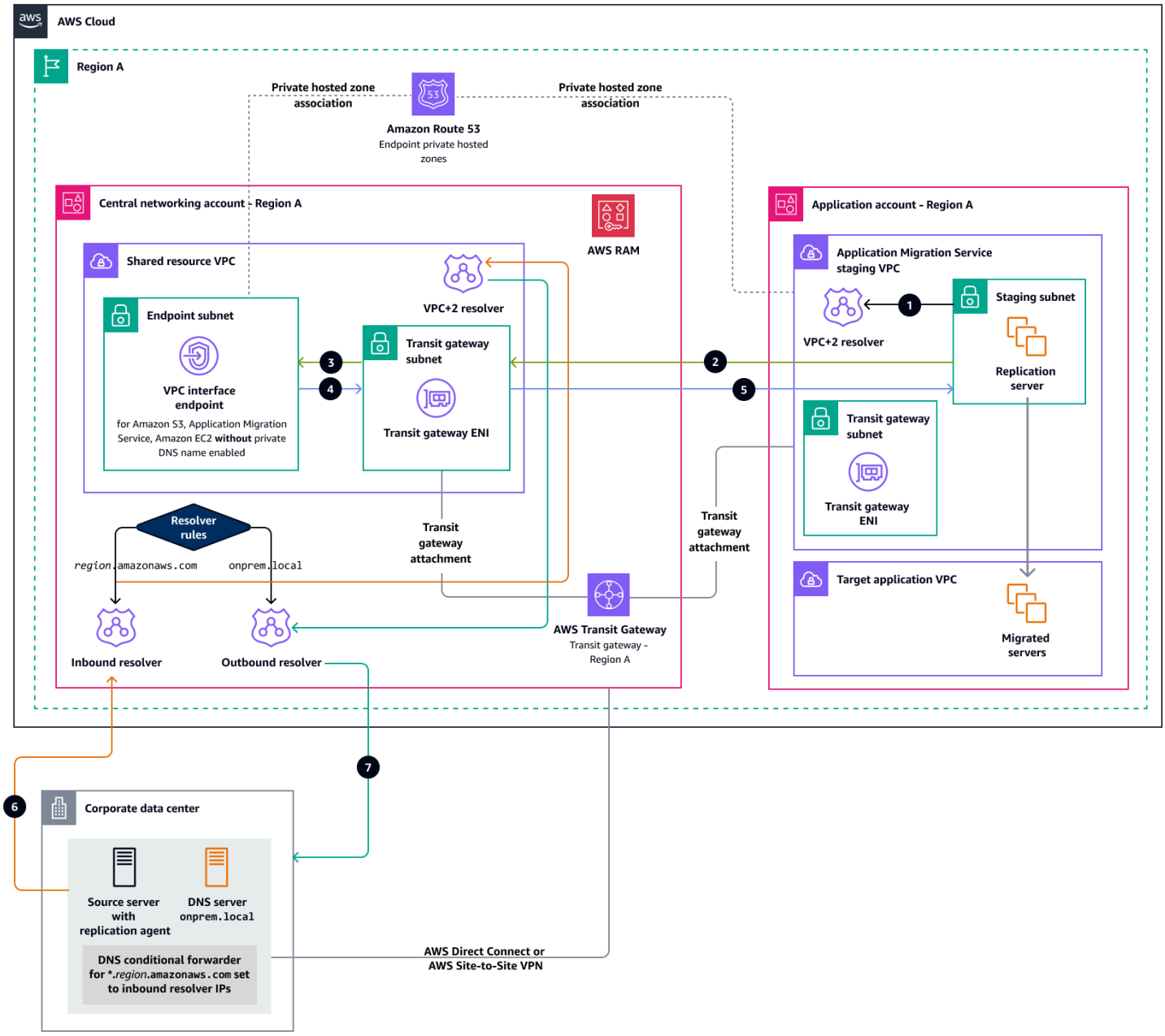
프라이빗 네트워크를 통해 이를 달성하려면 모든 대상 계정에 여러 VPC 인터페이스 엔드포인트를 생성해야 합니다. 이렇게 하면 엔드포인트 유지 관리에 대한 관리 오버헤드와 비용이 추가됩니다. (AWS PrivateLink 요금 참조)

Solution

중앙 AWS 네트워킹 계정에서 VPC 엔드포인트를 생성하고 Transit Gateway를 사용하여 대상 애플리케이션 계정에 연결합니다.

아키텍처

다음 다이어그램은이 솔루션의 아키텍처를 보여줍니다.



다이어그램에서 숫자는 다음 트래픽 흐름을 나타냅니다.

1. 중앙 네트워킹 계정 VPC에 있는 인터페이스 엔드포인트를 통해 Amazon Simple Storage Service(Amazon EC2 Amazon S3 EC2) 인스턴스 또는 MGN 복제 서버는 먼저 VPC+2 해석기를 쿼리하여 도메인 이름을 확인해야 합니다. Amazon EC2 엔드포인트 프라이빗 호스팅 영역은 동일한 리전의 MGN 스테이징 VPC와 연결되어 도메인 확인을 완료합니다.

> **Note**
>
> VPC와 연결하는 각 프라이빗 호스팅 영역에 대해 해석기는 규칙을 생성하고 VPC와 연결합니다. 프라이빗 호스팅 영역을 여러 VPCs와 연결하는 경우 해석기는 규칙을 모든 VPCs와 연결합니다.

2. 인스턴스가 연결할 프라이빗 IP를 알고 있으면 트래픽을 전송 게이트웨이 ENI로 전송합니다. 트래픽은 전송 게이트웨이 라우팅 테이블에 따라 전송 게이트웨이로 전송되고 공유 리소스 VPC로 전달됩니다.
3. 공유 리소스 VPC의 전송 게이트웨이 ENI는 트래픽을 해당 인터페이스 엔드포인트로 전달합니다.
4. VPC 엔드포인트는 응답을 전송 게이트웨이 ENI로 다시 보냅니다.
5. 트래픽은 전송 게이트웨이로 전달됩니다. 전송 게이트웨이 라우팅 테이블에 지정된 대로 트래픽은 스포크 MGN 스테이징 VPC로 전송됩니다. 응답은 전송 게이트웨이 ENI에서 대상, 즉 EC2 인스턴스 또는 MGN 복제 서버로 전송됩니다.
6. 회사 데이터 센터에 있는 클라이언트 애플리케이션은 도메인 이름을 형식으로 확인합니다`<aws_service>.<aws_region>.amazonaws.com`(예: `mgn.us-east-1.amazonaws.com`). 미리 구성된 DNS 해석기로 쿼리를 전송합니다. 기업 데이터 센터의 DNS 해석기에는 `amazonaws.com` 도메인에 대한 모든 DNS 쿼리를 Route 53 Resolver 인바운드 엔드포인트로 가리키는 전달 규칙이 있습니다. Transit Gateway는 쿼리를 공유 리소스 VPC로 전달하고, 공유 리소스 VPC는 Route 53 Resolver 인바운드 엔드포인트에서 DNS 쿼리를 전달합니다.

   Route 53 Resolver 인바운드 엔드포인트는 VPC+2 해석기를 사용합니다. 공유 리소스 VPC와 연결된 엔드포인트 프라이빗 호스팅 영역에는에 대한 DNS 레코드`amazonaws.com`가 있으므로 Route 53 Resolver가 쿼리를 해결할 수 있습니다.
7. Route 53 Resolver 아웃바운드 엔드포인트는 온프레미스 클라이언트 애플리케이션에 DNS 쿼리 응답을 반환합니다.

구현 단계

이전 다이어그램에 표시된 아키텍처를 설정하려면 다음 단계를 따르세요.

1. AWS Direct Connect 또는를 통해의 중앙 네트워킹 계정에 AWS 기업 데이터 센터를 연결합니다 AWS Site-to-Site VPN.

2. 네트워킹 계정에서 Transit Gateway를 사용하여 VPCs 간에 연결을 제공합니다. 전송 게이트웨이는 AWS 계정 를 사용하여 간에 공유 AWS RAM되며 VPC 연결을 통해 대상 애플리케이션 계정 스테이징 서브넷에 추가로 연결됩니다.

> **Note**
>
> 대상이 동일한 AWS 조직의 일부가 될 필요는 AWS 계정 없습니다. 자세한 내용은 AWS RAM 설명서의 공유 가능한 리소스를 참조하세요.

3. 프라이빗 DNS 이름을 활성화하지 않고 중앙 네트워크 계정에서 Amazon EC2, MGN 및 Amazon S3에 대한 VPC 인터페이스 엔드포인트를 생성합니다.

> **Note**
>
> 에 대한 VPC 엔드포인트를 생성할 때 프라이빗 DNS를 활성화 AWS 서비스할 수 있습니다. 활성화하면 설정이 관리형 Route 53 프라이빗 호스팅 영역을 생성합니다.이 관리형 영역은 VPC 내에서 DNS 이름을 확인합니다. 그러나 VPC 외부에서는 작동하지 않습니다. 따라서 프라이빗 호스팅 영역 공유 및 Route 53 Resolver를 사용하여 공유 VPC 엔드포인트에 대한 통합 이름 확인을 얻을 수 있습니다.

4. 각 엔드포인트(MGN, Amazon EC2, Amazon S3)에 대한 프라이빗 호스팅 영역을 생성합니다. 예를 들어 `us-east-1` 리전의 MGN의 경우:
   - 도메인 이름이 인 프라이빗 호스팅 영역을 생성합니다`mgn.us-east-1.amazonaws.com`.
   - 도메인 이름이 엔드포인트 IPs를 가리키는 A 유형의 호스트 레코드를 생성합니다.
5. 하이브리드 DNS 확인을 용이하게 하기 위해 Route 53 Resolver 인바운드 및 아웃바운드 규칙을 생성하고 규칙을 동일한 리전 AWS 계정 에 필요한와 공유합니다.

솔루션 2: 여러 리전의 중앙 네트워킹 계정에서 VPC 엔드포인트 생성

사용 사례:

애플리케이션 또는 서버를 여러의 다른 AWS 대상 계정으로 마이그레이션 AWS 리전하여 사용자와 가깝게 유지하거나 재해 복구 시나리오에서 비즈니스 연속성을 활성화하려고 합니다. 이는 첫 번째 사용 사례의 확장입니다.

도전 과제

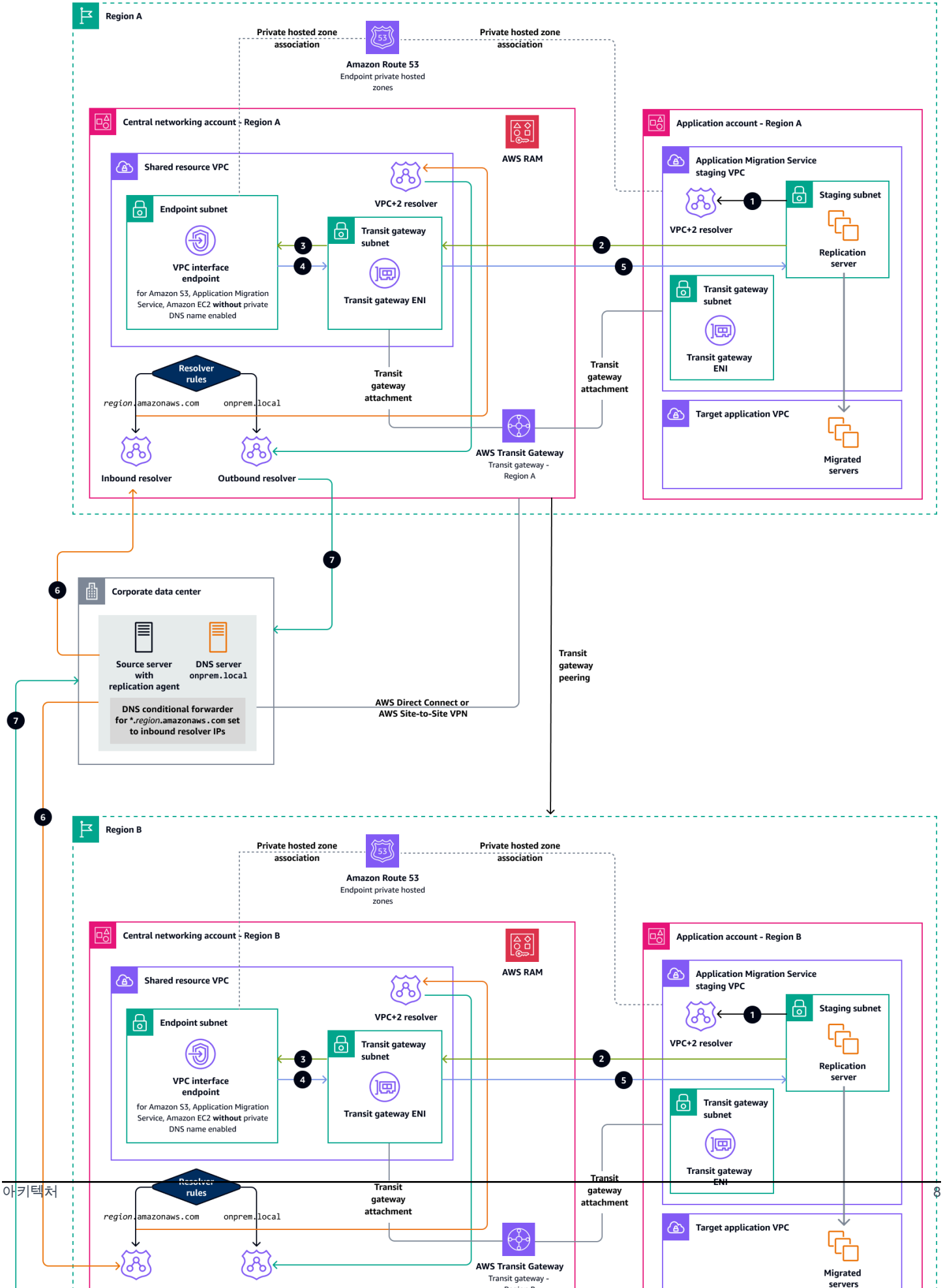
프라이빗 네트워크를 통해 이를 달성하려면 모든 대상 계정에 여러 VPC 인터페이스 엔드포인트를 생성해야 합니다. 이는 다중 리전 시나리오에서 훨씬 더 복잡해지고 여러 엔드포인트 유지 관리에 대한 관리 오버헤드와 비용이 추가됩니다. (AWS PrivateLink 요금 참조)

Solution

중앙 네트워킹 계정의 각 리전에 대해 VPC 엔드포인트를 생성하고 피어링된 전송 게이트웨이 및 Route 53을 사용하여 교차 계정 액세스를 활성화합니다.

아키텍처

다음 다이어그램은이 솔루션의 아키텍처를 보여줍니다.


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
VPC+2 resolver
Transit gateway subnet
Transit gateway ENI
Resolver rules
region.amazonaws.com
onprem.local
Transit gateway attachment
Transit gateway attachment
Target application VPC
Migrated servers
Inbound resolver
Outbound resolver
AWS Transit Gateway
Transit gateway - Region A
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
VPC+2 resolver
Transit gateway subnet
Transit gateway ENI
Resolver rules
region.amazonaws.com
onprem.local
Transit gateway attachment
Transit gateway attachment
Target application VPC
Migrated servers
AWS Transit Gateway
Transit gateway -

트래픽 흐름은 두 리전의 계정이 전송 게이트웨이 피어링에 의해 연결된다는 점을 제외하면 솔루션 1과 동일합니다.

구현 단계

1. 중앙 네트워킹 계정에서 각 대상에 대한 VPC 인터페이스 엔드포인트를 생성합니다 AWS 리전.
2. 중앙 네트워킹 계정에서 각 리전의 각 엔드포인트에 대한 프라이빗 호스팅 영역을 생성하고 해당 영역을 동일한 리전의 대상 애플리케이션 VPCs와 연결합니다.
3. 중앙 네트워킹 계정에서 각 대상 리전에 대한 전송 게이트웨이를 생성하고를 사용하여 게이트웨이를 동일한 리전의 대상 계정과 공유합니다 AWS RAM.
4. 전송 게이트웨이 피어링을 사용하여 리전 간에 전송 게이트웨이를 연결하고 필요에 따라 전송 게이트웨이 라우팅 테이블을 업데이트합니다.
5. 중앙 네트워킹 계정에서 각 대상 리전에 대한 해석기 규칙을 생성하고를 사용하여 이러한 규칙을 동일한 리전의 대상 계정과 공유합니다 AWS RAM.

솔루션 3: VPC 인터페이스 엔드포인트 공유

사용 사례:

애플리케이션은 서로 다른 사업부에 매핑되며 결제 및 격리를 위해 동일한 리전의 서로 다른 AWS 대상 계정으로 마이그레이션하려고 합니다.

도전 과제

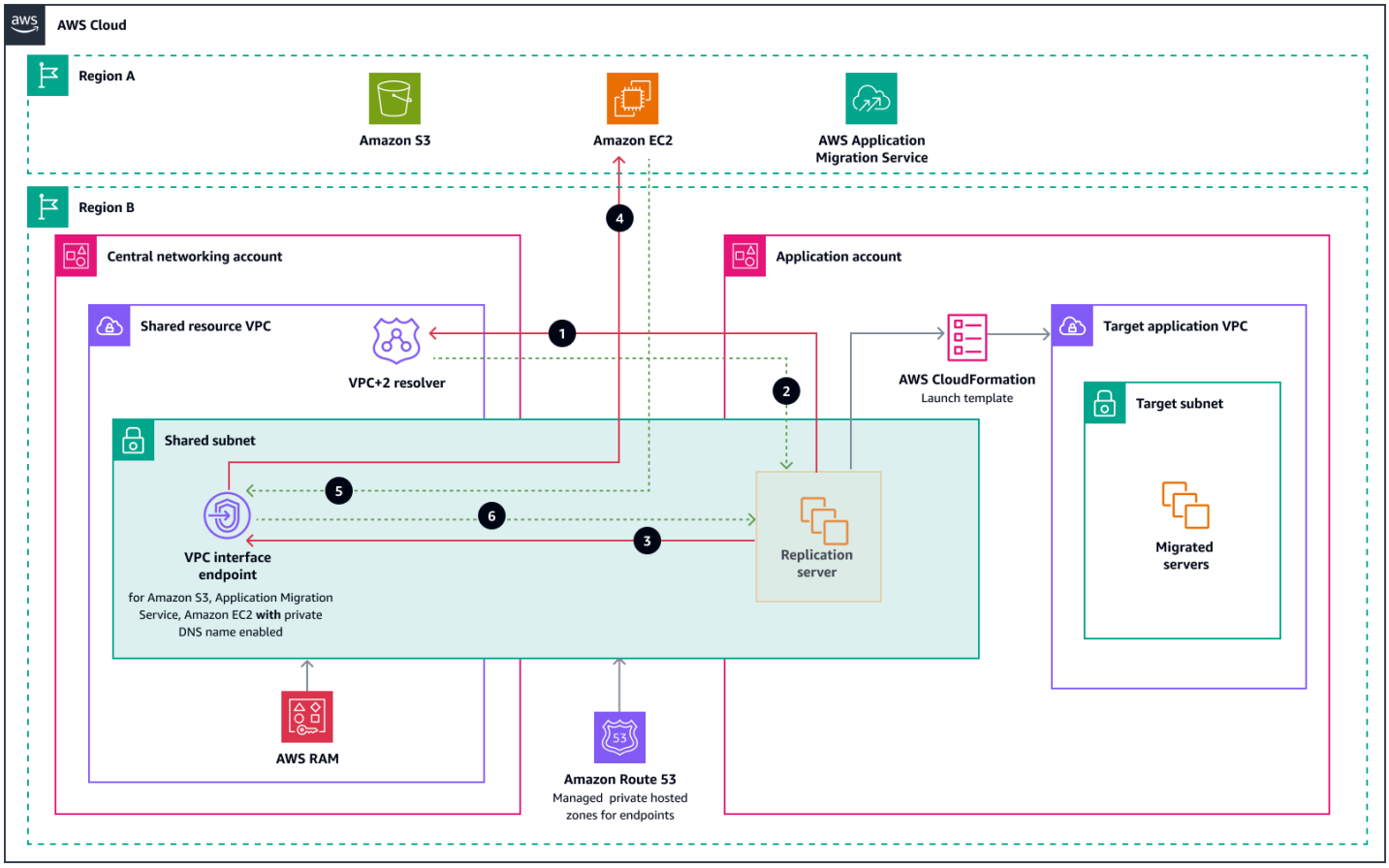
워크로드 계정이 여러 개인 경우 관리 오버헤드와 각 계정의 개별 VPC 인터페이스 엔드포인트 비용이 모두 증가합니다. 따라서 MGN의 스테이징 VPCs를 줄이고 스테이징 VPCs의 라우팅을 중앙에서 관리하여 비용과 관리 오버헤드를 줄일 수 있습니다.

Solution

공유 스테이징 영역 서브넷 AWS Organizations및를 사용하여 VPC 엔드포인트를 공유합니다 AWS RAM. VPC 공유에 대한 자세한 내용은 Amazon VPC 설명서를 참조하세요.

아키텍처

다음 다이어그램은이 솔루션의 아키텍처를 보여줍니다.



다이어그램은 다음 트래픽 흐름을 보여줍니다.

1. MGN 복제 서버는 VPC+2 DNS를 쿼리하여 MGN, Amazon EC2 또는 Amazon S3에 대한 API 엔드포인트를 확인합니다.

2. VPC+2 DNS는 관리형 프라이빗 호스팅 영역의 도움을 받아 엔드포인트의 AWS 프라이빗 IP를 확인하고 MGN 복제 서버에 응답합니다.

3-6. 복제 서버는 해당 IP를 사용하여 서비스의 인터페이스 엔드포인트를 통해 AWS 서비스 API에 연결합니다.

구현 단계

1. 중앙 네트워킹 계정에서 MGN용 스테이징 VPC 및 서브넷을 생성합니다.
2. 프라이빗 DNS 이름이 활성화된 MGN, Amazon EC2 또는 Amazon S3용 엔드포인트를 생성합니다. 이렇게 하면 AWS 관리형 프라이빗 호스팅 영역이 생성되어 스테이징 VPC와 연결됩니다.
3. 스테이징 서브넷을 동일한 AWS 조직 및의 대상 애플리케이션 계정과 공유합니다 AWS 리전.

4. AWS 와 온프레미스 데이터 센터(이전 다이어그램에 표시되지 않음) 간의 하이브리드 연결에는 솔루션 1 및 솔루션 2 AWS Site-to-Site VPN 와 같이 Transit Gateway Direct Connect 또는 Route 53 Resolver 엔드포인트를 사용합니다.

제한 사항

- AWS 계정 참가자 VPCs 소유자 VPC의는 동일한 조직의 일부여야 합니다 AWS Organizations.
- 공유 가능한 리소스 목록은 Amazon VPC 설명서를 참조하세요.
- VPC 공유 제한 사항은 Amazon VPC 설명서를 참조하세요.

설계 고려 사항

- 운영 오버헤드를 줄이려면 리소스를 한 번 생성한 다음 AWS RAM 를 사용하여 해당 리소스를 다른 계정과 공유합니다. 따라서 모든 계정에서 중복 리소스를 프로비저닝할 필요가 없으며 운영 오버헤드가 줄어듭니다.
- 단일 정책 및 권한 세트를 사용하여 공유 리소스의 보안 관리를 간소화합니다. 별도의 계정에서 중복 리소스를 생성하는 경우 동일한 정책 및 권한을 구현하고 모든 계정에서 동기화된 상태를 유지해야 합니다. 대신 단일 정책 및 권한 세트를 통해 AWS RAM 리소스를 공유하는 모든 사용자를 관리할 수 있습니다.는 다양한 유형의 AWS 리소스를 공유할 수 있는 일관된 환경을 AWS RAM 제공합니다.
- 가시성과 감사 가능성을 제공합니다. Amazon CloudWatch 및 AWS RAM 와 통합하여 공유 리소스의 사용 세부 정보를 봅니다 AWS CloudTrail. 자세한 내용은 AWS RAM 설명서의 EventBridge AWS RAM 를 사용한 모니터링 및 를 사용한 AWS RAM API 호출 로깅 AWS CloudTrail을 참조하세요.

FAQ

Q: 리소스를 누구와 공유할 수 있나요?

A: 모든와 리소스를 공유할 수 있습니다 AWS 계정. 의 조직에 속 AWS Organizations 해 있고 조직 내 공유가 활성화된 경우 리소스를 조직 단위(OUs) 또는 전체 조직과 공유할 수도 있습니다. 지원되는 리소스 유형의 경우 AWS Identity and Access Management (IAM) 역할 및 IAM 사용자와 리소스를 공유할 수도 있습니다. 조직 외부의 계정과 리소스를 공유하는 경우 해당 계정은 리소스 공유에 가입하라는 초대를 받습니다. 초대를 수락한 후 공유 리소스를 사용할 수 있습니다.

Q: 리소스를 다른와 공유하면 요금이 발생하나요 AWS 계정?

A: 아니요. 추가 비용 없이 리소스를 공유할 수 있습니다.

Q: 리소스 공유를 중지할 수 있나요?

A: 예. 리소스 공유를 중지하려면 리소스 공유에서 제거하거나 리소스 공유를 삭제합니다.

Q:에서 보안을 보장하려면 어떻게 해야 하나요 AWS RAM?

A: 보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드의 보안으로 설명합니다. 자세한 내용은 AWS RAM 설명서의 의 보안을 AWS RAM 참조하세요.

모범 사례

- 단일 장애 지점을 방지합니다. VPC 엔드포인트 및 Route 53 Resolver 엔드포인트의 경우 고가용성을 위해 둘 이상의 가용 영역을 사용합니다.
- Route 53 Resolver 엔드포인트를 사용하여 VPCs 간에 DNS 쿼리를 전달하지 마십시오. Amazon EC2 내의 모든 인스턴스에 대해 Amazon DNS 서버(.Amazon EC2 해석기)를 DNS 해석기로 사용하는 것이 좋습니다. 이 해석기는 지연 시간을 최소화하면서 최고 수준의 가용성과 확장성을 제공합니다.
- 추가 모범 사례는 Route 53 설명서의 해석기 모범 사례를 참조하세요.

리소스

- 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여에 액세스(Amazon VPC 설명서)
- VPC 서브넷을 다른 계정과 공유(Amazon VPC 설명서)
- 공유 가능한 Amazon VPC 리소스(AWS RAM 문서)
- AWS PrivateLink 및 AWS Transit Gateway 와 통합 Amazon Route 53 Resolver(AWS 블로그 게시물)
- 를 사용하여 VPC 엔드포인트 중앙 집중화 AWS Transit Gateway(AWS 참조 아키텍처)
- 프라이빗 네트워크를 통해 MGN 데이터 및 컨트롤 플레인에 연결(AWS 권장 가이드)

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2025년 2월 18일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.