Menghosting ulang aplikasi Anda dalam arsitektur multi-akun AWS dengan menggunakan titik akhir antarmuka VPC

AWS Panduan Preskriptif

AWS Panduan Preskriptif: Menghosting ulang aplikasi Anda dalam arsitektur multi-akun AWS dengan menggunakan titik akhir antarmuka VPC

Table of Contents

Menghosting ulang aplikasi Anda dalam arsitektur multi-akun AWS dengan menggunakan titik akhir antarmuka VPC

Dipan Jain dan Saurabh Shankar, Amazon Web Services

Februari 2025 (riwayat dokumen)

Banyak organisasi meng-host ulang (mengangkat dan memindahkan) aplikasi mereka AWS dari lingkungan jaringan yang terisolasi atau semi-terisolasi, termasuk pusat data lokal dan infrastruktur cloud atau hybrid lainnya, dengan menggunakan. AWS Transform MGN Jaringan terisolasi ini biasanya tidak mengizinkan lalu lintas keluar ke titik akhir publik yang dijelaskan dalam persyaratan jaringan untuk MGN. Anda dapat mengatasi batasan ini dengan menggunakan titik akhir antarmuka virtual private cloud (VPC), seperti yang dibahas dalam pola Panduan AWS Preskriptif Hubungkan ke data MGN dan bidang kontrol melalui jaringan pribadi.

Banyak organisasi juga menggunakan arsitektur multi-account landing zone (MALZ) untuk manfaat isolasi, keamanan, dan penagihan per akun. Untuk mengaktifkan migrasi lift-and-shift dengan menggunakan MGN melalui jaringan aman ke beberapa target, Akun AWS Anda harus membuat titik akhir antarmuka VPC di setiap target. Akun AWS Ini menambah biaya dan kompleksitas pengelolaan sumber daya tersebut.

Panduan ini membahas opsi untuk memusatkan titik akhir antarmuka VPC untuk menghosting ulang aplikasi Anda dalam arsitektur multi-akun. AWS Opsi ini menyederhanakan arsitektur dan mengurangi biaya untuk kasus penggunaan tersebut.

Hasil bisnis yang ditargetkan

Panduan ini memberikan solusi untuk tiga kasus penggunaan rehosting. Ini berfokus pada pengurangan biaya dan overhead operasional, dan meningkatkan keamanan dan pemanfaatan sumber daya.

Kasus penggunaan:

- Aplikasi Anda dipetakan ke unit bisnis yang berbeda, dan Anda ingin memigrasikannya ke akun AWS target yang berbeda Wilayah AWS untuk menyederhanakan penagihan dan isolasi.

Solusi untuk skenario ini melibatkan pembuatan titik akhir VPC di akun AWS jaringan pusat dan menggunakan AWS Transit Gateway untuk terhubung ke akun aplikasi target.

- Anda ingin memigrasikan aplikasi Anda ke akun AWS target yang berbeda dalam beberapa Wilayah AWS untuk menjaga aplikasi Anda tetap dekat dengan pengguna Anda atau untuk memfasilitasi pemulihan bencana. Ini adalah perpanjangan dari kasus penggunaan pertama.

  Solusi untuk skenario ini melibatkan pembuatan titik akhir VPC untuk masing-masing Wilayah AWS di akun jaringan AWS pusat, dan mengaktifkan akses lintas akun dengan menggunakan gateway transit peered dan Amazon Route 53.
- Aplikasi Anda dipetakan ke unit bisnis yang berbeda, dan Anda ingin memigrasikannya ke akun AWS target yang berbeda Wilayah AWS untuk tujuan penagihan dan isolasi. Anda juga ingin menggunakan lebih sedikit VPC untuk pementasan MGN, dan Anda ingin mengelola perutean secara terpusat untuk VPC pementasan untuk mengurangi biaya dan overhead administratif.

  Solusi untuk skenario ini melibatkan berbagi titik akhir VPC dengan menggunakan subnet area pementasan bersama, dengan dan (). AWS Organizations AWS Resource Access Manager AWS RAM

Audiens yang dituju

Panduan ini untuk konsultan migrasi, arsitek aplikasi, arsitek infrastruktur, dan pemilik aplikasi yang mencari solusi untuk kasus penggunaan ini.

Solusi 1: Membuat titik akhir VPC di akun jaringan pusat untuk satu Wilayah

Kasus penggunaan

Aplikasi Anda dipetakan ke unit bisnis yang berbeda dan Anda ingin memigrasikannya ke akun AWS target yang berbeda Wilayah AWS untuk tujuan penagihan dan isolasi.

Tantangan

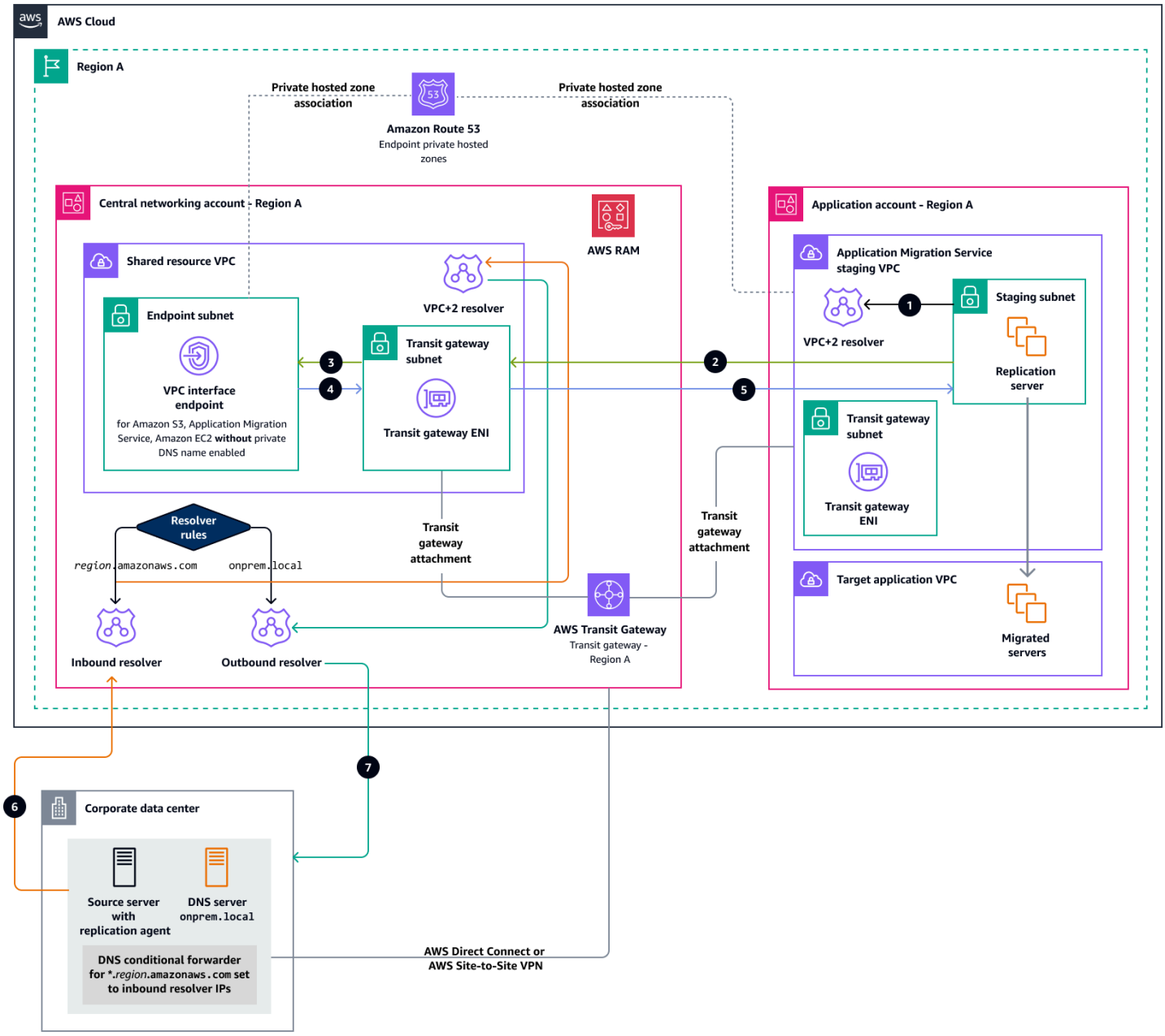
Untuk mencapai ini melalui jaringan pribadi, Anda harus membuat beberapa titik akhir antarmuka VPC di setiap akun target. Ini menambah overhead administratif dan biaya untuk mempertahankan titik akhir. (Lihat AWS PrivateLink harga.)

Solusi

Buat titik akhir VPC di akun AWS jaringan pusat dan gunakan Transit Gateway untuk terhubung ke akun aplikasi target.

Arsitektur

Diagram berikut menggambarkan arsitektur untuk solusi ini.



Dalam diagram, angka-angka mewakili arus lalu lintas berikut:

1. Instans Amazon Elastic Compute Cloud (Amazon EC2) atau server replikasi MGN yang perlu terhubung ke Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), MGN, atau Amazon EC2 melalui titik akhir antarmuka yang terletak di akun jaringan pusat VPC terlebih dahulu harus menyelesaikan nama domain dengan menanyakan VPC+2 reg pemecah. Zona host pribadi titik akhir dikaitkan dengan VPC pementasan MGN di Wilayah yang sama untuk menyelesaikan resolusi domain.

> **Note**
>
> Untuk setiap zona host pribadi yang Anda kaitkan dengan VPC, resolver membuat aturan dan mengaitkannya dengan VPC. Jika Anda mengaitkan zona host pribadi dengan beberapa VPC, resolver mengaitkan aturan dengan semua VPC.

2. Ketika instance mengetahui IP pribadi untuk terhubung, ia mengirimkan lalu lintas ke gateway transit ENI. Lalu lintas dikirim ke gateway transit dan diteruskan ke VPC sumber daya bersama, berdasarkan tabel rute gateway transit.
3. Gerbang transit ENI di VPC sumber daya bersama meneruskan lalu lintas ke titik akhir antarmuka yang sesuai.
4. Titik akhir VPC mengirimkan respons kembali ke gateway transit ENI.
5. Lalu lintas diteruskan ke gateway transit. Seperti yang ditentukan dalam tabel rute gateway transit, lalu lintas dikirim ke VPC pementasan MGN spoke. Respons dikirim oleh gateway transit ENI ke tujuan, yaitu, ke instans EC2 atau server replikasi MGN.
6. Aplikasi klien yang terletak di pusat data perusahaan menyelesaikan nama domain dalam formulir `<aws_service>.<aws_region>.amazonaws.com` (misalnya,`mgn.us-east-1.amazonaws.com`). Ini mengirimkan kueri ke resolver DNS yang telah dikonfigurasi sebelumnya. Penyelesai DNS di pusat data perusahaan memiliki aturan penerusan yang mengarahkan kueri DNS apa pun untuk `amazonaws.com` domain ke titik akhir masuk Route 53 Resolver. Transit Gateway meneruskan kueri ke VPC sumber daya bersama, yang meneruskan kueri DNS di titik akhir masuk Route 53 Resolver.

   Titik akhir masuk Route 53 Resolver menggunakan resolver VPC+2. Zona host pribadi titik akhir yang terkait dengan VPC sumber daya bersama menyimpan catatan `amazonaws.com` DNS, sehingga Resolver Route 53 dapat menyelesaikan kueri.
7. Titik akhir keluar Route 53 Resolver mengembalikan respons kueri DNS ke aplikasi klien lokal.

Langkah-langkah implementasi

Untuk mengatur arsitektur yang ditunjukkan pada diagram sebelumnya, ikuti langkah-langkah berikut:

1. Hubungkan pusat data perusahaan Anda ke akun jaringan pusat AWS melalui AWS Direct Connect atau AWS Site-to-Site VPN.

2. Di akun jaringan, gunakan Transit Gateway untuk menyediakan konektivitas antar VPC. Gateway transit dibagi antara Akun AWS dengan menggunakan AWS RAM, dan selanjutnya terhubung ke subnet pementasan akun aplikasi target melalui lampiran VPC.

> **Note**
>
> Target Akun AWS tidak harus menjadi bagian dari AWS organisasi yang sama. Untuk informasi selengkapnya, lihat Sumber daya yang dapat dibagikan dalam AWS RAM dokumentasi.

3. Buat titik akhir antarmuka VPC untuk Amazon EC2, MGN, dan Amazon S3 di akun jaringan pusat tanpa mengaktifkan nama DNS pribadi.

> **Note**
>
> Saat Anda membuat titik akhir VPC ke sebuah Layanan AWS, Anda dapat mengaktifkan DNS pribadi. Saat diaktifkan, pengaturan akan membuat zona host pribadi Route 53 terkelola untuk Anda. Zona terkelola ini menyelesaikan nama DNS dalam VPC. Namun, itu tidak berfungsi di luar VPC. Ini adalah alasan untuk menggunakan berbagi zona host pribadi dan Resolver Route 53 untuk membantu mendapatkan resolusi nama terpadu untuk titik akhir VPC bersama.

4. Buat zona host pribadi untuk setiap titik akhir (MGN, Amazon EC2, Amazon S3). Misalnya, untuk MGN di `us-east-1` Wilayah:
   - Buat zona host pribadi dengan nama domain`mgn.us-east-1.amazonaws.com`.
   - Buat catatan host tipe A yang mengarahkan nama domain ke IP endpoint.
5. Buat aturan masuk dan keluar Resolver Route 53 untuk memfasilitasi resolusi DNS hibrida, dan bagikan aturan dengan yang diperlukan Akun AWS di Wilayah yang sama.

Solusi 2: Membuat titik akhir VPC di akun jaringan pusat untuk beberapa Wilayah

Kasus penggunaan

Anda ingin memigrasikan aplikasi atau server Anda ke akun AWS target yang berbeda dalam beberapa akun Wilayah AWS, agar tetap dekat dengan pengguna Anda atau untuk mengaktifkan kelangsungan bisnis dalam skenario pemulihan bencana. Ini adalah perpanjangan dari kasus penggunaan pertama.

Tantangan

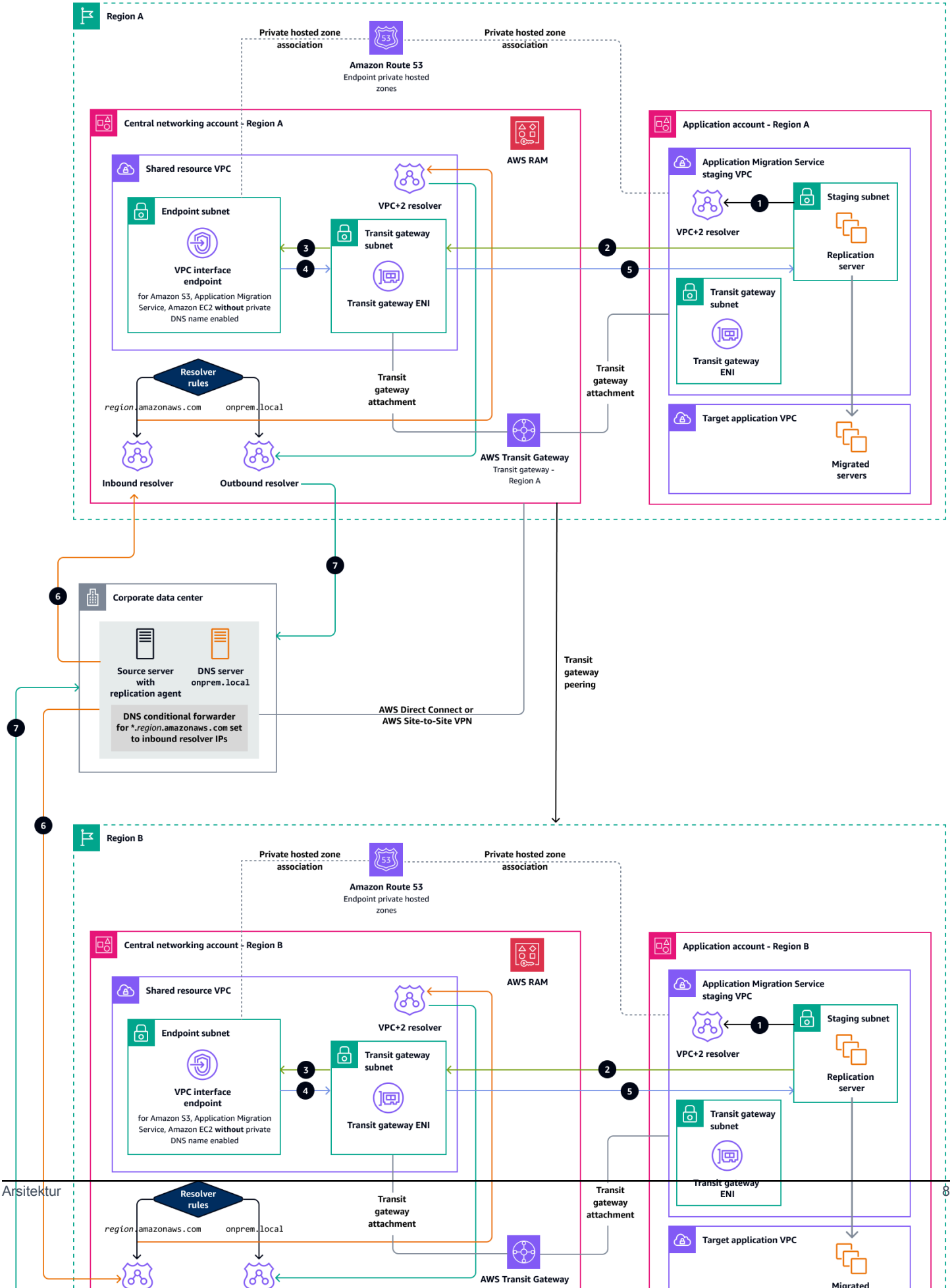
Untuk mencapai ini melalui jaringan pribadi, Anda harus membuat beberapa titik akhir antarmuka VPC di setiap akun target. Ini menjadi lebih kompleks dalam skenario Multi-wilayah dan menambah overhead administratif dan biaya untuk mempertahankan beberapa titik akhir. (Lihat AWS PrivateLink harga.)

Solusi

Buat titik akhir VPC untuk setiap Wilayah di akun jaringan pusat dan aktifkan akses lintas akun dengan menggunakan gateway transit peered dan Route 53.

Arsitektur

Diagram berikut menggambarkan arsitektur untuk solusi ini.


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
AWS Transit Gateway

Arus lalu lintas sama dengan solusi 1, kecuali bahwa akun di dua Wilayah dihubungkan oleh peering gateway transit.

Langkah-langkah implementasi

1. Di akun jaringan pusat, buat titik akhir antarmuka VPC untuk setiap target. Wilayah AWS
2. Di akun jaringan pusat, buat zona host pribadi untuk setiap titik akhir di setiap Wilayah, dan kaitkan zona tersebut dengan VPC aplikasi target di Wilayah yang sama.
3. Di akun jaringan pusat, buat gateway transit untuk setiap Wilayah target, dan bagikan gateway dengan akun target di Wilayah yang sama dengan menggunakan AWS RAM.
4. Hubungkan gateway transit lintas Wilayah dengan menggunakan peering gateway transit, dan perbarui tabel rute gateway transit sesuai kebutuhan.
5. Di akun jaringan pusat, buat aturan resolver untuk setiap Wilayah target, dan bagikan aturan ini dengan akun target di Wilayah yang sama dengan menggunakan. AWS RAM

Solusi 3: Berbagi titik akhir antarmuka VPC

Kasus penggunaan

Aplikasi Anda dipetakan ke unit bisnis yang berbeda, dan Anda ingin memigrasikannya ke akun AWS target yang berbeda di Wilayah yang sama untuk tujuan penagihan dan isolasi.

Tantangan

Beberapa akun beban kerja meningkatkan overhead administratif dan biaya titik akhir antarmuka VPC individual di setiap akun. Oleh karena itu, Anda mungkin ingin memiliki lebih sedikit VPC pementasan untuk MGN dan mengelola perutean secara terpusat untuk VPC pementasan untuk mengurangi biaya dan overhead administratif.

Solusi

Bagikan titik akhir VPC dengan menggunakan subnet area pementasan bersama,, dan. AWS Organizations AWS RAM Untuk informasi selengkapnya tentang berbagi VPC, lihat dokumentasi Amazon VPC.

Arsitektur

Diagram berikut menggambarkan arsitektur untuk solusi ini.

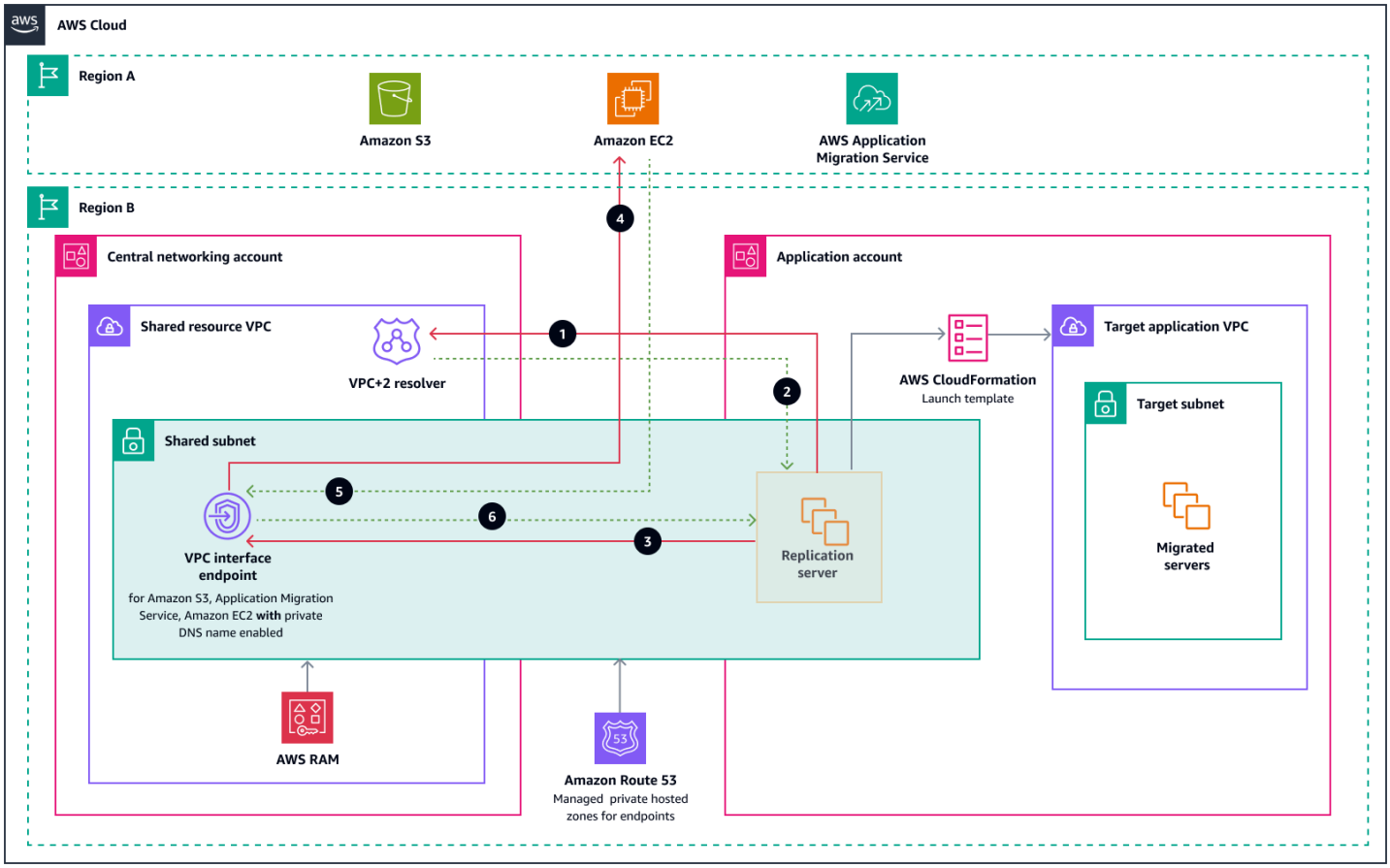


Diagram menggambarkan arus lalu lintas berikut:

1. Server replikasi MGN menanyakan DNS VPC+2 untuk menyelesaikan titik akhir API untuk MGN, Amazon EC2, atau Amazon S3.

2. DNS VPC+2 menyelesaikan IP pribadi titik akhir dengan bantuan zona host pribadi yang AWS dikelola dan merespons server replikasi MGN.

3-6. Server replikasi menggunakan IP tersebut untuk terhubung ke Layanan AWS API melalui titik akhir antarmuka untuk layanan.

Langkah-langkah implementasi

1. Di akun jaringan pusat, buat pementasan VPC dan subnet untuk MGN.
2. Buat titik akhir untuk MGN, Amazon EC2, atau Amazon S3 dengan nama DNS pribadi diaktifkan. Ini menciptakan zona host pribadi AWS terkelola dan mengaitkannya dengan VPC pementasan.

3. Bagikan subnet pementasan dengan akun aplikasi target di AWS organisasi yang sama dan. Wilayah AWS
4. Untuk konektivitas hibrid antara AWS dan pusat data lokal Anda (tidak ditampilkan pada diagram sebelumnya) gunakan Transit Gateway, Direct Connect atau AWS Site-to-Site VPN dengan titik akhir Resolver Route 53, seperti yang ditunjukkan pada solusi 1 dan solusi 2.

Batasan

- Akun AWS Untuk VPC peserta dan pemilik VPC harus menjadi bagian dari organisasi yang sama di. AWS Organizations
- Untuk daftar sumber daya yang dapat dibagikan, lihat dokumentasi Amazon VPC.
- Untuk batasan berbagi VPC, lihat dokumentasi Amazon VPC.

Pertimbangan desain

- Untuk mengurangi overhead operasional Anda, buat sumber daya sekali, lalu gunakan AWS RAM untuk berbagi sumber daya tersebut dengan akun lain. Ini menghilangkan kebutuhan untuk menyediakan sumber daya duplikat di setiap akun dan mengurangi overhead operasional.
- Sederhanakan manajemen keamanan untuk sumber daya bersama Anda dengan menggunakan satu set kebijakan dan izin. Jika Anda membuat sumber daya duplikat di akun terpisah, Anda harus menerapkan kebijakan dan izin yang identik dan membuatnya tetap disinkronkan di semua akun. Sebagai gantinya, Anda dapat mengelola semua pengguna yang berbagi AWS RAM sumber daya melalui satu set kebijakan dan izin. AWS RAM menawarkan pengalaman yang konsisten untuk berbagi berbagai jenis AWS sumber daya.
- Memberikan visibilitas dan auditabilitas. Lihat detail penggunaan untuk sumber daya bersama Anda dengan mengintegrasikan AWS RAM dengan Amazon CloudWatch dan AWS CloudTrail. Untuk informasi selengkapnya, lihat Monitoring AWS RAM using EventBridge and Logging AWS RAM API call with AWS CloudTrail in the AWS RAM documentation.

Pertanyaan yang Sering Diajukan

T: Dengan siapa saya dapat berbagi sumber daya?

A: Anda dapat berbagi sumber daya dengan apa pun Akun AWS. Jika Anda adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, Anda juga dapat berbagi sumber daya dengan unit organisasi (OUs) atau dengan seluruh organisasi Anda. Untuk jenis sumber daya yang didukung, Anda juga dapat berbagi sumber daya dengan peran AWS Identity and Access Management (IAM) dan pengguna IAM. Jika Anda berbagi sumber daya dengan akun yang berada di luar organisasi Anda, akun tersebut menerima undangan untuk bergabung dengan pembagian sumber daya. Setelah mereka menerima undangan, mereka dapat mulai menggunakan sumber daya bersama.

T: Apakah saya akan dikenakan biaya untuk berbagi sumber daya saya dengan orang lain? Akun AWS

A: Tidak. Anda dapat berbagi sumber daya tanpa biaya tambahan.

T: Dapatkah saya berhenti berbagi sumber daya?

A: Ya. Untuk berhenti berbagi sumber daya, hapus dari pembagian sumber daya atau hapus pembagian sumber daya.

T: Bagaimana saya bisa memastikan keamanan AWS RAM?

A: Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menggambarkan ini sebagai keamanan cloud dan keamanan di cloud. Untuk informasi selengkapnya, lihat Keamanan AWS RAM dalam AWS RAM dokumentasi.

Praktik terbaik

- Hindari satu titik kegagalan. Untuk titik akhir VPC dan titik akhir Resolver Route 53, gunakan dua atau lebih Availability Zone untuk ketersediaan tinggi.
- Jangan gunakan titik akhir Route 53 Resolver untuk meneruskan kueri DNS di antaranya. VPCs Kami sangat menyarankan agar Anda menggunakan Amazon DNS Server (.2 resolver) sebagai DNS resolver untuk semua instance di dalam Amazon. EC2 Resolver ini memberikan tingkat ketersediaan dan skalabilitas tertinggi dengan latensi terendah.
- Untuk praktik terbaik tambahan, lihat Praktik terbaik untuk Resolver dalam dokumentasi Route 53.

Sumber daya

- Akses Layanan AWS menggunakan titik akhir VPC antarmuka (dokumentasi Amazon VPC)
- Bagikan subnet VPC Anda dengan akun lain (dokumentasi Amazon VPC)
- Sumber daya AWS RAM Amazon VPC yang dapat dibagikan (dokumentasi)
- Integrasi AWS Transit Gateway dengan AWS PrivateLink dan Amazon Route 53 Resolver (posting AWS blog)
- Memusatkan titik akhir VPC AWS Transit Gateway dengan AWS (Arsitektur Referensi)
- Connect ke data MGN dan pesawat kontrol melalui jaringan pribadi (AWS Prescriptive Guidance)

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Februari 18, 2025

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.