Rehosting delle applicazioni in un'architettura multi-account utilizzando AWS endpoint di interfaccia VPC

# AWS Linee guida prescrittive

# AWS Linee guida prescrittive: Rehosting delle applicazioni in un'architettura multi-account utilizzando AWS endpoint di interfaccia VPC

# Table of Contents

# Rehosting delle applicazioni in un'architettura multi-account su AWS utilizzando gli endpoint dell'interfaccia VPC

Dipin Jain e Saurabh Shankar, Amazon Web Services

Febbraio 2025 (storia del documento)

Molte organizzazioni reospitano (lift and shift) le proprie applicazioni AWS da ambienti di rete isolati o semiisolati, inclusi data center locali e altre infrastrutture cloud o ibride, utilizzando. AWS Transform MGN Queste reti isolate in genere non consentono alcun traffico in uscita verso gli endpoint pubblici, come descritto nei requisiti di rete per MGN. È possibile ovviare a questa limitazione utilizzando gli endpoint dell'interfaccia VPC (Virtual Private Cloud), come illustrato nel modello AWS Prescriptive Guidance Connect to MGN data and control plane su una rete privata.

Molte organizzazioni utilizzano anche un'architettura multi-account landing zone (MALZ) per l'isolamento, la sicurezza e i vantaggi di fatturazione per account. Per abilitare la migrazione lift-and-shift utilizzando MGN su una rete protetta verso più destinazioni, è Account AWS necessario creare endpoint di interfaccia VPC in ogni destinazione. Account AWS Ciò aumenta i costi e la complessità della gestione di tali risorse.

Questa guida illustra le opzioni per centralizzare gli endpoint dell'interfaccia VPC per il rehosting delle applicazioni in un'architettura multi-account su. AWS Queste opzioni semplificano l'architettura e riducono i costi per questi casi d'uso.

## Obiettivi aziendali specifici

Questa guida fornisce soluzioni per tre casi d'uso di rehosting. Si concentra sulla riduzione dei costi e delle spese operative e sul miglioramento della sicurezza e dell'utilizzo delle risorse.

Casi d'uso:

- Le tue applicazioni sono mappate su diverse unità aziendali e desideri migrarle su diversi account di AWS destinazione nello stesso per Regione AWS semplificare la fatturazione e l'isolamento.

  La soluzione a questo scenario prevede la creazione di endpoint VPC in un account di AWS rete centrale e l'utilizzo AWS Transit Gateway per la connessione agli account delle applicazioni di destinazione.

- Desiderate migrare le applicazioni su diversi account di AWS destinazione in più fasi Regioni AWS per mantenere le applicazioni vicine agli utenti o per facilitare il disaster recovery. Si tratta di un'estensione del primo caso d'uso.

  La soluzione a questo scenario prevede la creazione di endpoint VPC per ciascuno di essi Regione AWS in un account di rete AWS centrale e l'abilitazione dell'accesso tra account diversi utilizzando un gateway di transito peer e Amazon Route 53.
- Le tue applicazioni sono mappate su diverse unità aziendali e desideri migrarle su diversi account di AWS destinazione nello stesso Regione AWS per scopi di fatturazione e isolamento. Desideri inoltre utilizzare meno VPC per lo staging di MGN e gestire centralmente il routing per i VPC di staging per ridurre i costi e il sovraccarico amministrativo.

  La soluzione a questo scenario prevede la condivisione degli endpoint VPC utilizzando una sottorete di area di staging condivisa, con and (). AWS Organizations AWS Resource Access Manager AWS RAM

## Destinatari principali

Questa guida è destinata a consulenti in materia di migrazione, architetti di applicazioni, architetti di infrastrutture e proprietari di applicazioni che cercano soluzioni per questi casi d'uso.

# Soluzione 1: creazione di endpoint VPC in un account di rete centrale per una singola regione

## Caso d’uso

Le tue applicazioni sono mappate su diverse unità aziendali e desideri migrarle su diversi account di AWS destinazione nello stesso Regione AWS per scopi di fatturazione e isolamento.

## Sfide

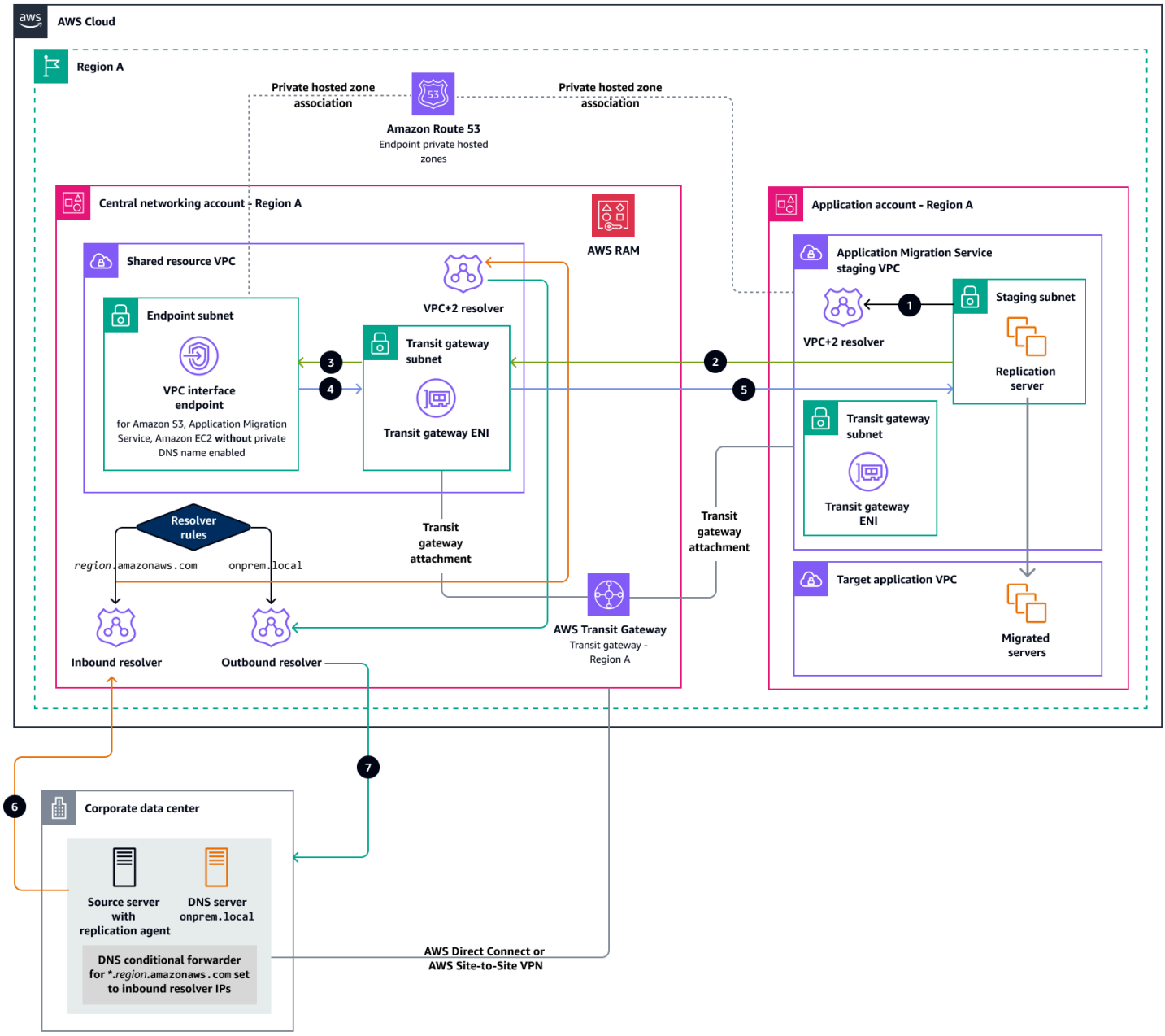
Per raggiungere questo obiettivo su una rete privata, è necessario creare più endpoint di interfaccia VPC in ogni account di destinazione. Ciò si aggiunge al sovraccarico amministrativo e ai costi di manutenzione degli endpoint. (Vedi i AWS PrivateLink prezzi).

## Soluzione

Crea endpoint VPC in un account di AWS rete centrale e utilizza Transit Gateway per connetterti agli account delle applicazioni di destinazione.

## Architecture

Il diagramma seguente illustra l'architettura di questa soluzione.




Nel diagramma, i numeri rappresentano il seguente flusso di traffico:

1. L'istanza Amazon Elastic Compute Cloud (Amazon EC2) o il server di replica MGN che deve connettersi ad Amazon Simple Storage Service (Amazon S3), MGN o Amazon EC2 tramite un endpoint di interfaccia che si trova nell'account di rete centrale VPC deve prima risolvere il nome di dominio interrogando la resolazione VPC+2 ver. La zona ospitata privata dell'endpoint è associata al VPC di staging MGN nella stessa regione per completare la risoluzione del dominio.

> **Note**
>
> Per ogni zona ospitata privata associata a un VPC, il resolver crea una regola e la associa al VPC. Se associ la zona ospitata privata a più VPC, il resolver associa la regola a tutti i VPC.

2. Quando l'istanza conosce l'IP privato a cui connettersi, invia il traffico al gateway di transito ENI. Il traffico viene inviato al gateway di transito e inoltrato al VPC di risorse condivise, in base alla tabella di routing del gateway di transito.
3. Il gateway di transito ENI nella risorsa condivisa VPC inoltra il traffico all'endpoint dell'interfaccia corrispondente.
4. L'endpoint VPC invia la risposta al gateway di transito ENI.
5. Il traffico viene inoltrato al gateway di transito. Come specificato nella tabella delle rotte del gateway di transito, il traffico viene inviato al VPC di staging MGN a pozze. La risposta viene inviata dal gateway di transito ENI alla destinazione, ovvero all'istanza EC2 o al server di replica MGN.
6. Un'applicazione client situata nel data center aziendale risolve un nome di dominio nel formato `<aws_service>.<aws_region>.amazonaws.com` (ad esempio,). `mgn.us-east-1.amazonaws.com` Invia la query al suo resolver DNS preconfigurato. Il resolver DNS del data center aziendale dispone di una regola di inoltro che indirizza qualsiasi query DNS per i domini all'endpoint in entrata Route 53 Resolver. `amazonaws.com` Transit Gateway inoltra la query al VPC della risorsa condivisa, che inoltra la query DNS all'endpoint in ingresso Route 53 Resolver.

   L'endpoint in ingresso del Route 53 Resolver utilizza il resolver VPC+2. La zona ospitata privata dell'endpoint associata alla risorsa condivisa VPC contiene i record `amazonaws.com` DNS, quindi Route 53 Resolver può risolvere la query.
7. L'endpoint in uscita Route 53 Resolver restituisce la risposta alla query DNS all'applicazione client locale.

## Passaggi dell’implementazione

Per configurare l'architettura mostrata nel diagramma precedente, procedi nel seguente modo:

1. Connect il data center aziendale all'account di rete centrale AWS tramite AWS Direct Connect o AWS Site-to-Site VPN.
2. Nell'account di rete, utilizza Transit Gateway per fornire connettività tra VPC. Il gateway di transito viene condiviso Account AWS utilizzando AWS RAM e ulteriormente connesso alla sottorete di staging dell'account dell'applicazione di destinazione tramite un allegato VPC.

> **Note**
>
> Target Account AWS non deve necessariamente far parte della stessa organizzazione. AWS Per ulteriori informazioni, consulta Risorse condivisibili nella AWS RAM documentazione.

3. Crea endpoint di interfaccia VPC per Amazon EC2, MGN e Amazon S3 nell'account di rete centrale senza abilitare un nome DNS privato.

> **Note**
>
> Quando crei un endpoint VPC su un Servizio AWS, puoi abilitare il DNS privato. Se abilitata, l'impostazione crea automaticamente una zona ospitata privata Route 53 gestita. Questa zona gestita risolve il nome DNS all'interno di un VPC. Tuttavia, non funziona al di fuori del VPC. Questo è il motivo per cui utilizziamo la condivisione di zone ospitate private e Route 53 Resolver per ottenere una risoluzione unificata dei nomi per gli endpoint VPC condivisi.

4. Crea una zona ospitata privata per ogni endpoint (MGN, Amazon EC2, Amazon S3). Ad esempio, per MGN nella regione: `us-east-1`
   - Crea una zona ospitata privata con il nome `mgn.us-east-1.amazonaws.com` di dominio.
   - Crea un record host di tipo A che indirizzi il nome di dominio agli IP degli endpoint.
5. Crea regole in entrata e in uscita di Route 53 Resolver per facilitare la risoluzione DNS ibrida e condividi le regole con i requisiti nella stessa regione. Account AWS

# Soluzione 2: creazione di endpoint VPC in un account di rete centrale per più regioni

## Caso d’uso

Desiderate migrare le vostre applicazioni o i vostri server verso diversi account di AWS destinazione in più di un secondo Regioni AWS momento, per mantenerli vicini agli utenti o per consentire la continuità aziendale in scenari di disaster recovery. Si tratta di un'estensione del primo caso d'uso.

## Sfide

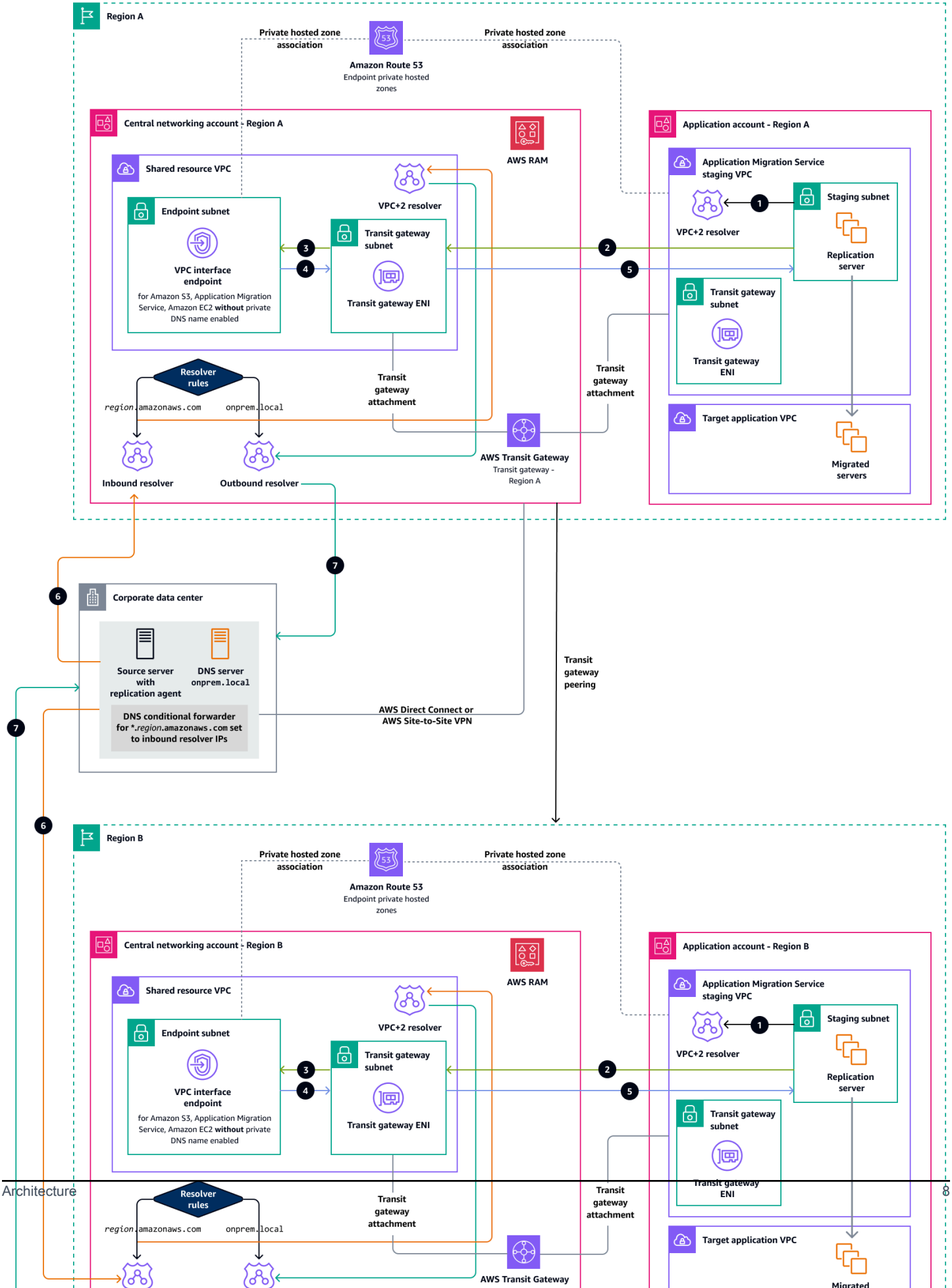
Per raggiungere questo obiettivo su una rete privata, è necessario creare più endpoint di interfaccia VPC in ogni account di destinazione. Ciò diventa ancora più complesso in uno scenario multiregionale e aumenta il sovraccarico amministrativo e i costi per la manutenzione di più endpoint. (Vedi AWS PrivateLink i prezzi).

## Soluzione

Crea endpoint VPC per ogni regione in un account di rete centrale e abilita l'accesso tra account utilizzando un gateway di transito peer e Route 53.

## Architecture

Il diagramma seguente illustra l'architettura di questa soluzione.


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
Resolver rules
region.amazonaws.com
onprem.local
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
Resolver rules
region.amazonaws.com
onprem.local
Transit gateway attachment
Target application VPC
Migrated
AWS Transit Gateway

Il flusso di traffico è lo stesso della soluzione 1, tranne per il fatto che gli account nelle due regioni sono collegati tramite peering del gateway di transito.

## Passaggi dell’implementazione

1. Nell'account di rete centrale, crea un endpoint di interfaccia VPC per ogni destinazione. Regione AWS
2. Nell'account di rete centrale, crea una zona ospitata privata per ogni endpoint in ogni regione e associa la zona ai VPC dell'applicazione di destinazione nella stessa regione.
3. Nell'account di rete centrale, crea un gateway di transito per ogni regione di destinazione e condividi il gateway con gli account di destinazione nella stessa regione utilizzando. AWS RAM
4. Connetti i gateway di transito tra le regioni utilizzando il peering dei gateway di transito e aggiorna le tabelle di routing dei gateway di transito secondo necessità.
5. Nell'account di rete centrale, crea regole resolver per ogni regione di destinazione e condividi queste regole con gli account di destinazione nella stessa regione utilizzando. AWS RAM

# Soluzione 3: condivisione degli endpoint dell'interfaccia VPC

## Caso d’uso

Le tue applicazioni sono mappate su diverse unità aziendali e desideri migrarle su diversi account di AWS destinazione nella stessa regione per scopi di fatturazione e isolamento.

## Sfide

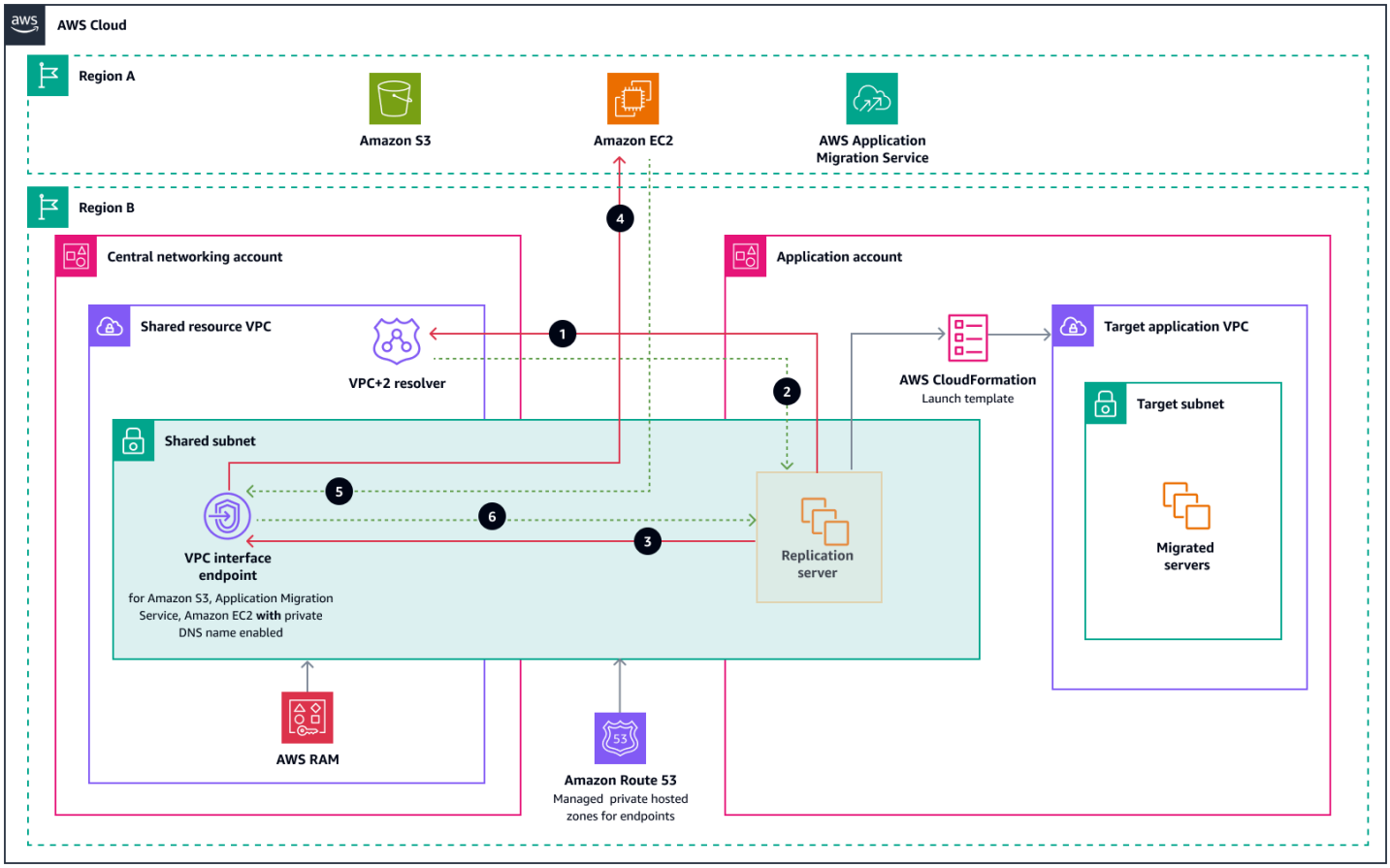
Più account di carico di lavoro aumentano sia il sovraccarico amministrativo che il costo dei singoli endpoint di interfaccia VPC in ogni account. Pertanto, potresti voler disporre di un minor numero di VPC di staging per MGN e gestire centralmente il routing per i VPC di staging per ridurre i costi e il sovraccarico amministrativo.

## Soluzione

Condividi gli endpoint VPC utilizzando una sottorete dell'area di staging condivisa e. AWS Organizations AWS RAM Per ulteriori informazioni sulla condivisione di VPC, consulta la documentazione di Amazon VPC.

## Architecture

Il diagramma seguente illustra l'architettura di questa soluzione.




Il diagramma illustra il seguente flusso di traffico:

1. Il server di replica MGN interroga il DNS VPC+2 per risolvere l'endpoint API per MGN, Amazon EC2 o Amazon S3.

2. Il DNS VPC+2 risolve l'IP privato dell'endpoint con l'aiuto di zone ospitate private AWS gestite e risponde al server di replica MGN.

3-6. Il server di replica utilizza tale IP per connettersi all' Servizio AWS API tramite l'endpoint di interfaccia del servizio.

# Passaggi dell’implementazione

1. Nell'account di rete centrale, create il VPC e la sottorete di staging per MGN.
2. Crea endpoint per MGN, Amazon EC2 o Amazon S3 con nomi DNS privati abilitati. Questo crea una zona ospitata privata AWS gestita e la associa al VPC di staging.

3. Condividi la sottorete di gestione temporanea con gli account delle applicazioni di destinazione nella stessa organizzazione e. AWS Regione AWS
4. Per la connettività ibrida tra AWS e il data center locale (non mostrata nel diagramma precedente) usa Transit Gateway Direct Connect o AWS Site-to-Site VPN con gli endpoint Route 53 Resolver, come mostrato nella soluzione 1 e nella soluzione 2.

## Limitazioni

- Il Account AWS VPC partecipante e il VPC proprietario devono far parte della stessa organizzazione in. AWS Organizations
- Per un elenco di risorse condivisibili, consulta la documentazione di Amazon VPC.
- Per le limitazioni alla condivisione di VPC, consulta la documentazione di Amazon VPC.

## Considerazioni di natura progettuale

- Per ridurre il sovraccarico operativo, crea una risorsa una sola volta e poi usala AWS RAM per condividerla con altri account. Ciò elimina la necessità di fornire risorse duplicate in ogni account e riduce il sovraccarico operativo.
- Semplifica la gestione della sicurezza per le risorse condivise utilizzando un unico set di policy e autorizzazioni. Se crei risorse duplicate in account separati, devi implementare politiche e autorizzazioni identiche e mantenerle sincronizzate su tutti gli account. Puoi invece gestire tutti gli utenti che condividono una AWS RAM risorsa tramite un unico set di politiche e autorizzazioni. AWS RAM offre un'esperienza coerente per la condivisione di diversi tipi di AWS risorse.
- Offri visibilità e verificabilità. Visualizza i dettagli di utilizzo delle tue risorse condivise mediante l'integrazione AWS RAM con Amazon CloudWatch e AWS CloudTrail. Per ulteriori informazioni, consulta Monitoraggio, AWS RAM utilizzo EventBridge e registrazione delle chiamate AWS RAM API con AWS CloudTrail nella AWS RAM documentazione.

# Domande frequenti

D: Con chi posso condividere le risorse?

R: Puoi condividere risorse con chiunque Account AWS. Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, puoi anche condividere le risorse con le unità organizzative (OUs) o con l'intera organizzazione. Per i tipi di risorse supportati, puoi anche condividere risorse con ruoli AWS Identity and Access Management (IAM) e utenti IAM. Se condividi risorse con account esterni all'organizzazione, tali account ricevono un invito a partecipare alla condivisione delle risorse. Dopo aver accettato l'invito, possono iniziare a utilizzare le risorse condivise.

D: Mi verranno addebitati costi per la condivisione delle mie risorse con altri? Account AWS

R: No. Puoi condividere le risorse senza costi aggiuntivi.

D: Posso interrompere la condivisione di una risorsa?

R: Sì. Per interrompere la condivisione di una risorsa, rimuovila dalla condivisione di risorse o elimina la condivisione di risorse.

D: Come posso garantire la sicurezza in AWS RAM?

R: La sicurezza è una responsabilità condivisa tra te AWS e te. Il modello di responsabilità condivisa lo descrive come sicurezza del cloud e sicurezza nel cloud. Per ulteriori informazioni, consulta la sezione Sicurezza AWS RAM nella AWS RAM documentazione.

# Best practice

- Evita singoli punti di errore. Per gli endpoint VPC e gli endpoint Route 53 Resolver, utilizza due o più zone di disponibilità per un'elevata disponibilità.
- Non utilizzare gli endpoint Route 53 Resolver per inoltrare le query DNS tra di loro. VPCs Ti consigliamo vivamente di utilizzare Amazon DNS Server (.2 resolver) come resolver DNS per tutte le istanze all'interno di Amazon. EC2 Questo resolver offre il massimo livello di disponibilità e scalabilità con la latenza più bassa.
- Per ulteriori best practice, consulta Best practice for Resolver nella documentazione di Route 53.

# Resources

- Accedere e Servizio AWS utilizzare un endpoint VPC di interfaccia (documentazione Amazon VPC)
- Condividi le tue sottoreti VPC con altri account (documentazione Amazon VPC)
- Risorse AWS RAM Amazon VPC condivisibili (documentazione)
- Integrazione AWS Transit Gateway con AWS PrivateLink e Amazon Route 53 Resolver(post sul blog)AWS
- Centralizzazione degli endpoint VPC con (architettura di riferimento) AWS Transit GatewayAWS
- Connect ai piani dati e di controllo MGN tramite una rete privata (AWS Prescriptive Guidance)

# Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Pubblicazione iniziale | — | 18 febbraio 2025 |

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.