Rehosten Ihrer Anwendungen in einer Architektur mit mehreren Konten unter Verwendung AWS von VPC-Schnittstellenendpunkten

AWS Prescriptive Guidance

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Prescriptive Guidance: Rehosten Ihrer Anwendungen in einer Architektur mit mehreren Konten unter Verwendung AWS von VPC-Schnittstellenendpunkten

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Rehosten Ihrer Anwendungen in einer Multi-Account-Architektur auf AWS mithilfe von VPC-Schnittstellenendpunkten

Dipin Jain und Saurabh Shankar, Amazon Web Services

Februar 2025 (Geschichte der Dokumente)

Viele Unternehmen rehosten (Lift and Shift) ihre Anwendungen auf AWS isolierte oder halbisolierte Netzwerkumgebungen, einschließlich lokaler Rechenzentren und anderer Cloud- oder Hybrid-Infrastrukturen, mithilfe von AWS Transform MGN Diese isolierten Netzwerke lassen in der Regel keinen ausgehenden Datenverkehr zu den öffentlichen Endpunkten zu, die in den Netzwerkanforderungen für MGN beschrieben sind. Sie können diese Einschränkung umgehen, indem Sie Virtual Private Cloud (VPC) -Schnittstellenendpunkte verwenden, wie im AWS Prescriptive Guidance-Muster „Connect zu MGN-Daten und Steuerungsebenen über ein privates Netzwerk herstellen“ beschrieben.

Viele Unternehmen verwenden auch eine MALZ-Architektur (Multi-Account landing zone), um Isolation, Sicherheit und Abrechnung pro Konto zu gewährleisten. Um die Lift-and-Shift-Migration mithilfe von MGN über ein sicheres Netzwerk zu mehreren Zielen zu ermöglichen AWS-Konten, müssen Sie in jedem Ziel VPC-Schnittstellenendpunkte erstellen. AWS-Konto Dies erhöht die Kosten und die Komplexität der Verwaltung dieser Ressourcen.

In diesem Handbuch werden Optionen für die Zentralisierung von VPC-Schnittstellen-Endpunkten für das Rehosting Ihrer Anwendungen in einer Multi-Account-Architektur beschrieben. AWS Diese Optionen vereinfachen die Architektur und reduzieren die Kosten für solche Anwendungsfälle.

Gezielte Geschäftsergebnisse

Dieses Handbuch bietet Lösungen für drei Rehosting-Anwendungsfälle. Der Schwerpunkt liegt auf der Senkung der Kosten und des Betriebsaufwands sowie auf der Verbesserung der Sicherheit und der Ressourcennutzung.

Anwendungsfälle:

- Ihre Anwendungen sind verschiedenen Geschäftsbereichen zugeordnet, und Sie möchten sie gleichzeitig auf verschiedene AWS Zielkonten migrieren, um die Abrechnung und Isolierung AWS-Region zu vereinfachen.

  Die Lösung für dieses Szenario besteht darin, VPC-Endpunkte in einem zentralen AWS Netzwerkkonto zu erstellen und diese für die Verbindung mit Zielanwendungskonten AWS Transit Gateway zu verwenden.
- Sie möchten Ihre Anwendungen in mehreren Zielkonten auf verschiedene AWS Zielkonten migrieren, AWS-Regionen um Ihre Anwendungen in der Nähe Ihrer Benutzer zu halten oder um die Notfallwiederherstellung zu erleichtern. Dies ist eine Erweiterung des ersten Anwendungsfalls.

  Die Lösung für dieses Szenario beinhaltet die Erstellung von VPC-Endpunkten für jeden AWS-Region in einem AWS zentralen Netzwerkkonto und die Aktivierung des kontoübergreifenden Zugriffs mithilfe eines Peer-Transit-Gateways und Amazon Route 53.
- Ihre Anwendungen sind verschiedenen Geschäftseinheiten zugeordnet, und Sie möchten sie zu Abrechnungs- und AWS-Region Isolierungszwecken auf verschiedene AWS Zielkonten in ein und demselben System migrieren. Außerdem möchten Sie weniger VPCs für das MGN-Staging verwenden und das Routing für die Staging-VPCs zentral verwalten, um Kosten und Verwaltungsaufwand zu reduzieren.

  Die Lösung für dieses Szenario beinhaltet die gemeinsame Nutzung von VPC-Endpunkten mithilfe eines gemeinsamen Staging-Bereich-Subnetzes mit AWS Organizations und (). AWS Resource Access Manager AWS RAM

Zielgruppe

Dieser Leitfaden richtet sich an Migrationsberater, Anwendungsarchitekten, Infrastrukturarchitekten und Anwendungsbesitzer, die nach Lösungen für diese Anwendungsfälle suchen.

Lösung 1: VPC-Endpunkte in einem zentralen Netzwerkkonto für eine einzelne Region erstellen

Anwendungsfall

Ihre Anwendungen sind verschiedenen Geschäftsbereichen zugeordnet, und Sie möchten sie zu Abrechnungs- und AWS-Region Isolierungszwecken auf verschiedene AWS Zielkonten gleichzeitig migrieren.

Herausforderungen

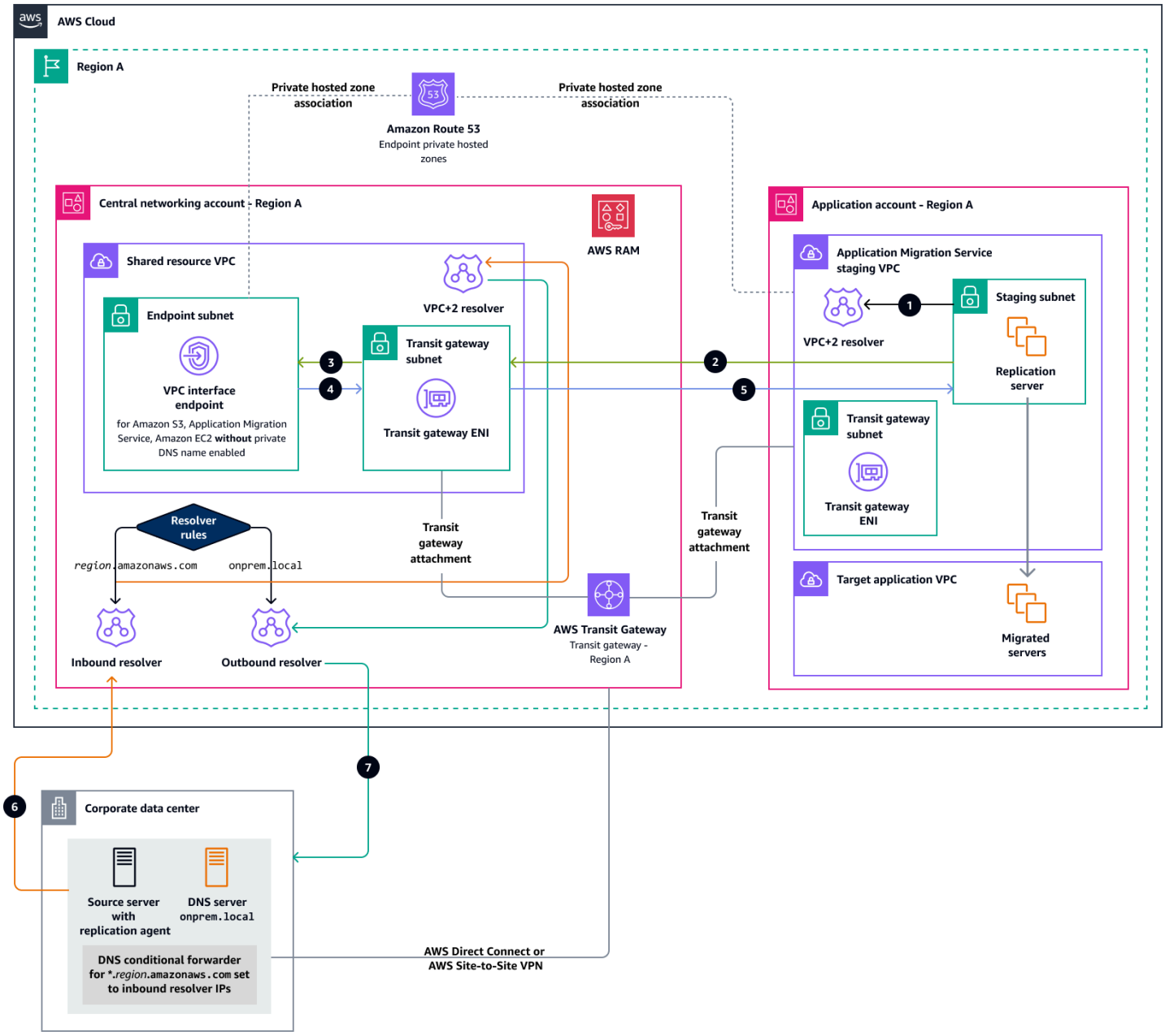
Um dies über ein privates Netzwerk zu erreichen, müssten Sie in jedem Zielkonto mehrere VPC-Schnittstellenendpunkte erstellen. Dies erhöht den Verwaltungsaufwand und die Kosten für die Wartung der Endgeräte. (Siehe AWS PrivateLink Preise.)

Lösung

Erstellen Sie VPC-Endpunkte in einem zentralen AWS Netzwerkkonto und verwenden Sie Transit Gateway, um eine Verbindung zu Zielanwendungskonten herzustellen.

Architektur

Das folgende Diagramm veranschaulicht die Architektur dieser Lösung.



Im Diagramm stellen die Zahlen den folgenden Verkehrsfluss dar:

1. Die Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder der MGN-Replikationsserver, der über einen Schnittstellenendpunkt, der sich in der zentralen Netzwerkkonto-VPC befindet, eine Verbindung zu Amazon Simple Storage Service (Amazon S3), MGN oder Amazon EC2 herstellen muss, muss zunächst den Domainnamen auflösen, indem sie den VPC+2-Resolver abfragt. Die private gehostete Endpunktzone wird der MGN-Staging-VPC in derselben Region zugeordnet, um die Domänenauflösung abzuschließen.

> **Note**
>
> Für jede private gehostete Zone, die Sie einer VPC zuordnen, erstellt der Resolver eine Regel und ordnet sie der VPC zu. Wenn Sie die private gehostete Zone mehreren VPCs zuordnen, ordnet der Resolver die Regel allen VPCs zu.

2. Wenn die Instance die private IP kennt, mit der sie eine Verbindung herstellen soll, sendet sie den Datenverkehr an das Transit-Gateway ENI. Der Verkehr wird an das Transit-Gateway gesendet und auf der Grundlage der Transit-Gateway-Routentabelle an die gemeinsam genutzte Ressourcen-VPC weitergeleitet.
3. Das Transit-Gateway ENI in der gemeinsam genutzten Ressource VPC leitet den Verkehr an den entsprechenden Schnittstellenendpunkt weiter.
4. Der VPC-Endpunkt sendet die Antwort zurück an das Transit-Gateway ENI.
5. Der Verkehr wird an das Transit-Gateway weitergeleitet. Wie in der Routentabelle des Transit-Gateways angegeben, wird der Datenverkehr an die Spoke-MGN-Staging-VPC gesendet. Die Antwort wird vom Transit-Gateway ENI an das Ziel gesendet, d. h. an die EC2-Instance oder den MGN-Replikationsserver.
6. Eine Client-Anwendung, die sich im Rechenzentrum des Unternehmens befindet, löst einen Domainnamen in der folgenden Form auf `<aws_service>.<aws_region>.amazonaws.com` (z. B.). `mgn.us-east-1.amazonaws.com` Sie sendet die Anfrage an ihren vorkonfigurierten DNS-Resolver. Der DNS-Resolver im Unternehmensrechenzentrum verfügt über eine Weiterleitungsregel, die jede DNS-Abfrage für `amazonaws.com` Domänen an den eingehenden Route 53 Resolver-Endpunkt weiterleitet. Transit Gateway leitet die Anfrage an die gemeinsam genutzte Ressourcen-VPC weiter, die die DNS-Abfrage an den eingehenden Route 53 Resolver-Endpunkt weiterleitet.

   Der eingehende Route 53 Resolver-Endpunkt verwendet den VPC+2-Resolver. Die private gehostete Endpunktzone, die der gemeinsam genutzten Ressource VPC zugeordnet ist, enthält die DNS-Einträge für`amazonaws.com`, sodass Route 53 Resolver die Abfrage auflösen kann.
7. Der ausgehende Route 53 Resolver-Endpunkt gibt die Antwort auf die DNS-Anfrage an die lokale Client-Anwendung zurück.

Implementierungsschritte

Gehen Sie wie folgt vor, um die im vorherigen Diagramm gezeigte Architektur einzurichten:

1. Connect Sie Ihr Unternehmensrechenzentrum AWS über AWS Direct Connect oder mit dem zentralen Netzwerkkonto AWS Site-to-Site VPN.
2. Verwenden Sie im Netzwerkkonto Transit Gateway, um Konnektivität zwischen VPCs bereitzustellen. Das Transit-Gateway wird gemeinsam AWS-Konten genutzt und über AWS RAM einen VPC-Anhang weiter mit dem Staging-Subnetz des Zielanwendungskontos verbunden.

   > **Note**
   >
   > Target muss AWS-Konten nicht Teil derselben Organisation sein. AWS Weitere Informationen finden Sie in der AWS RAM Dokumentation unter Gemeinsam nutzbare Ressourcen.

3. Erstellen Sie VPC-Schnittstellenendpunkte für Amazon EC2, MGN und Amazon S3 im zentralen Netzwerkkonto, ohne einen privaten DNS-Namen zu aktivieren.

   > **Note**
   >
   > Wenn Sie einen VPC-Endpunkt für einen erstellen AWS-Service, können Sie privates DNS aktivieren. Wenn diese Einstellung aktiviert ist, erstellt sie eine verwaltete private, gehostete Route 53-Zone für Sie. Diese verwaltete Zone löst den DNS-Namen innerhalb einer VPC auf. Außerhalb der VPC funktioniert es jedoch nicht. Aus diesem Grund werden private Hosted Zone Sharing und Route 53 Resolver verwendet, um eine einheitliche Namensauflösung für gemeinsam genutzte VPC-Endpunkte zu erreichen.

4. Erstellen Sie eine private gehostete Zone für jeden Endpunkt (MGN, Amazon EC2, Amazon S3). Zum Beispiel für MGN in der Region: `us-east-1`
   - Erstellen Sie eine private gehostete Zone mit dem Domainnamen`mgn.us-east-1.amazonaws.com`.
   - Erstellen Sie einen Hosteintrag vom Typ A, der den Domainnamen auf Endpunkt-IPs verweist.
5. Erstellen Sie Regeln für eingehenden und ausgehenden Route 53-Resolver, um die Hybrid-DNS-Auflösung zu erleichtern, und teilen Sie die Regeln mit den erforderlichen Personen AWS-Konto in derselben Region.

Lösung 2: VPC-Endpunkte in einem zentralen Netzwerkkonto für mehrere Regionen erstellen

Anwendungsfall

Sie möchten Ihre Anwendungen oder Server in mehreren Fällen auf verschiedene AWS Zielkonten migrieren AWS-Regionen, um sie in der Nähe Ihrer Benutzer zu halten oder um die Geschäftskontinuität in Notfallwiederherstellungsszenarien zu gewährleisten. Dies ist eine Erweiterung des ersten Anwendungsfalls.

Herausforderungen

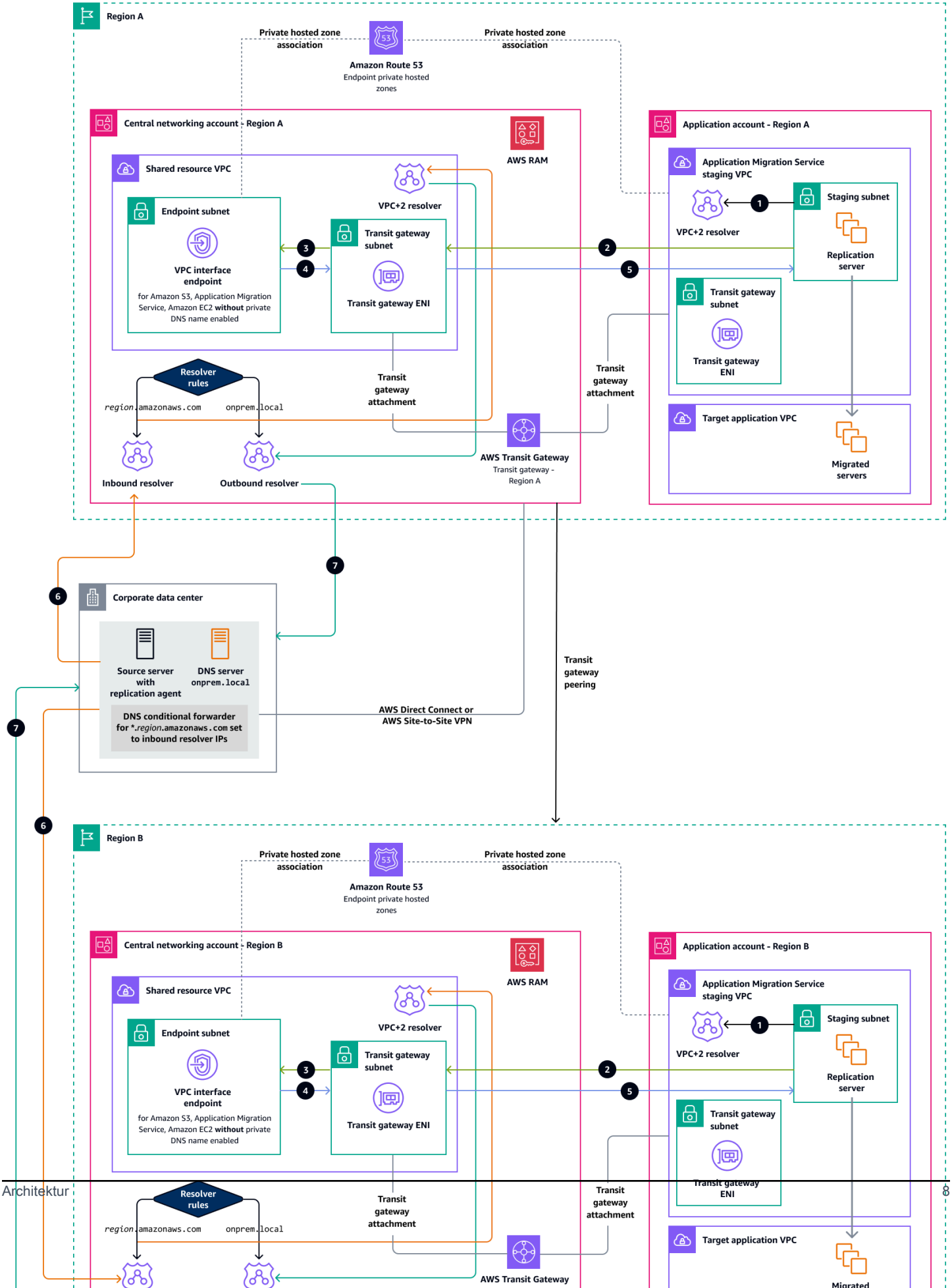
Um dies über ein privates Netzwerk zu erreichen, müssten Sie in jedem Zielkonto mehrere VPC-Schnittstellenendpunkte erstellen. Dies wird in einem Szenario mit mehreren Regionen noch komplexer und erhöht den Verwaltungsaufwand und die Kosten für die Wartung mehrerer Endgeräte. (Siehe AWS PrivateLink Preise.)

Lösung

Erstellen Sie VPC-Endpunkte für jede Region in einem zentralen Netzwerkkonto und ermöglichen Sie den kontoübergreifenden Zugriff mithilfe eines Peer-Transit-Gateways und Route 53.

Architektur

Das folgende Diagramm veranschaulicht die Architektur dieser Lösung.


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

Der Verkehrsfluss ist derselbe wie in Lösung 1, mit der Ausnahme, dass die Konten in den beiden Regionen über Transit-Gateway-Peering miteinander verbunden sind.

Implementierungsschritte

1. Erstellen Sie im zentralen Netzwerkkonto für jedes Ziel AWS-Region einen VPC-Schnittstellenendpunkt.
2. Erstellen Sie im zentralen Netzwerkkonto eine private gehostete Zone für jeden Endpunkt in jeder Region und ordnen Sie die Zone den Zielanwendungs-VPCs in derselben Region zu.
3. Erstellen Sie im zentralen Netzwerkkonto ein Transit-Gateway für jede Zielregion und teilen Sie das Gateway mit Zielkonten in derselben Region, indem Sie AWS RAM
4. Connect Transit-Gateways über Regionen hinweg mithilfe von Transit-Gateway-Peering und aktualisieren Sie die Transit-Gateway-Routentabellen nach Bedarf.
5. Erstellen Sie im zentralen Netzwerkkonto Resolver-Regeln für jede Zielregion und teilen Sie diese Regeln mit Zielkonten in derselben Region, indem Sie AWS RAM

Lösung 3: Gemeinsame Nutzung von VPC-Schnittstellenendpunkten

Anwendungsfall

Ihre Anwendungen sind verschiedenen Geschäftsbereichen zugeordnet, und Sie möchten sie zu Abrechnungs- und Isolierungszwecken auf verschiedene AWS Zielkonten in derselben Region migrieren.

Herausforderungen

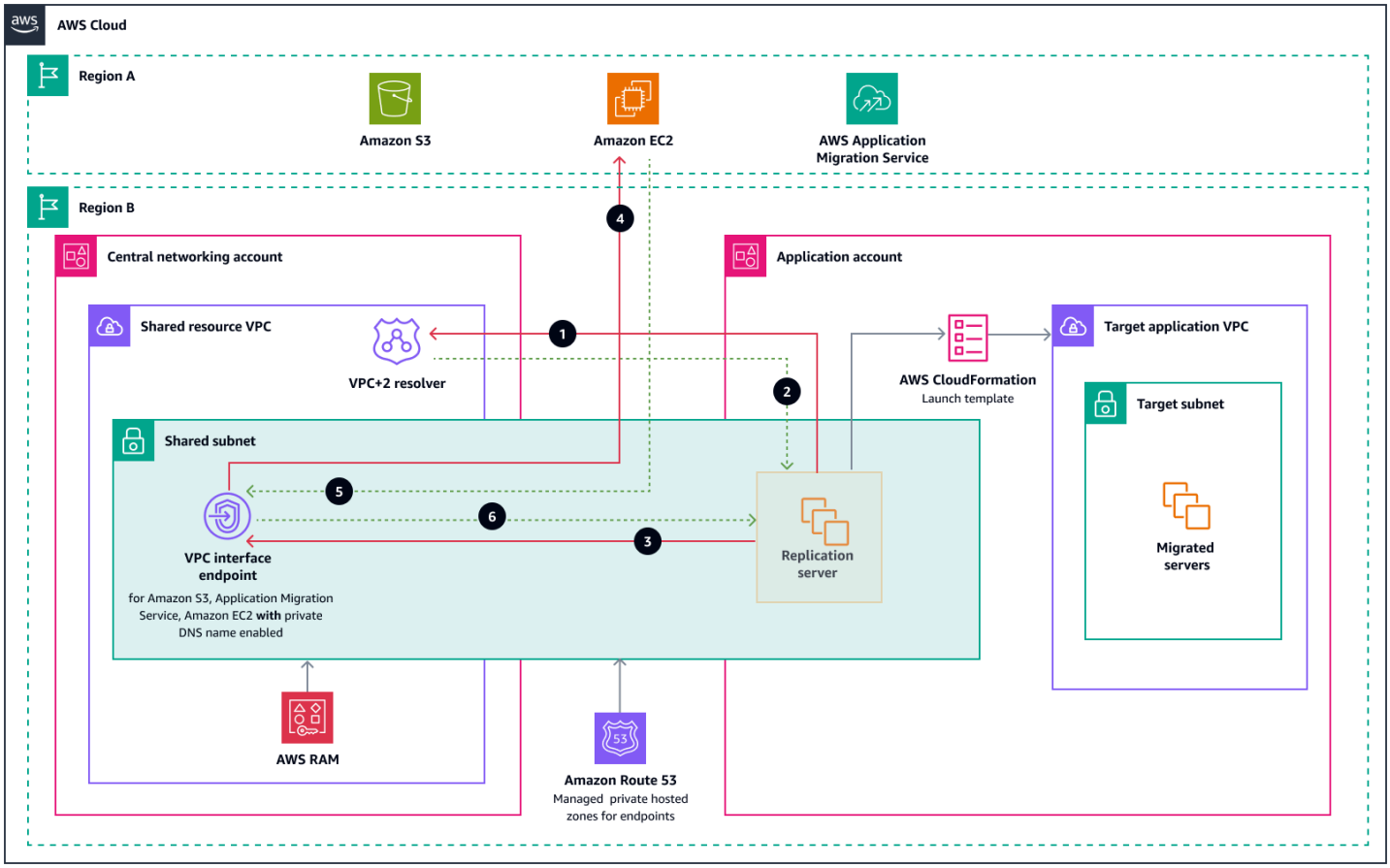
Mehrere Workload-Konten erhöhen sowohl den Verwaltungsaufwand als auch die Kosten für einzelne VPC-Schnittstellenendpunkte in jedem Konto. Daher sollten Sie möglicherweise weniger Staging-VPCs für MGN haben und das Routing für die Staging-VPCs zentral verwalten, um Kosten und Verwaltungsaufwand zu reduzieren.

Lösung

Geben Sie VPC-Endpunkte gemeinsam, indem Sie ein gemeinsames Staging-Bereich-Subnetz verwenden, und. AWS Organizations AWS RAM Weitere Informationen zur VPC-Sharing finden Sie in der Amazon VPC-Dokumentation.

Architektur

Das folgende Diagramm veranschaulicht die Architektur dieser Lösung.



Das Diagramm veranschaulicht den folgenden Verkehrsfluss:

1. Der MGN-Replikationsserver fragt das VPC+2-DNS ab, um den API-Endpunkt für MGN, Amazon EC2 oder Amazon S3 aufzulösen.

2. Das VPC+2 DNS löst die private IP des Endpunkts mithilfe von AWS verwalteten privaten gehosteten Zonen auf und reagiert auf den MGN-Replikationsserver.

3-6. Der Replikationsserver verwendet diese IP, um über den Schnittstellenendpunkt für den Dienst eine Verbindung zur AWS-Service API herzustellen.

Implementierungsschritte

1. Erstellen Sie im zentralen Netzwerkkonto die Staging-VPC und das Subnetz für MGN.
2. Erstellen Sie Endpunkte für MGN, Amazon EC2 oder Amazon S3 mit aktivierten privaten DNS-Namen. Dadurch wird eine AWS verwaltete private gehostete Zone erstellt und sie der Staging-VPC zugeordnet.

3. Teilen Sie das Staging-Subnetz mit Zielanwendungskonten in derselben Organisation und. AWS AWS-Region
4. Verwenden Sie für hybride Konnektivität zwischen AWS und Ihrem lokalen Rechenzentrum (im vorherigen Diagramm nicht dargestellt) Transit Gateway Direct Connect oder AWS Site-to-Site VPN mit Route 53 Resolver-Endpunkten, wie in Lösung 1 und Lösung 2 gezeigt.

Einschränkungen

- Die VPCs AWS-Konten für die Teilnehmer und die Eigentümer-VPC müssen Teil derselben Organisation sein. AWS Organizations
- Eine Liste der gemeinsam nutzbaren Ressourcen finden Sie in der Amazon VPC-Dokumentation.
- Informationen zu den Einschränkungen der VPC-Sharing finden Sie in der Amazon VPC-Dokumentation.

Designüberlegungen

- Um Ihren Betriebsaufwand zu reduzieren, erstellen Sie einmal eine Ressource und verwenden Sie sie dann, AWS RAM um diese Ressource mit anderen Konten zu teilen. Dadurch entfällt die Notwendigkeit, in jedem Konto doppelte Ressourcen bereitzustellen, und der Betriebsaufwand wird reduziert.
- Vereinfachen Sie das Sicherheitsmanagement für Ihre gemeinsam genutzten Ressourcen, indem Sie einen einzigen Satz von Richtlinien und Berechtigungen verwenden. Wenn Sie doppelte Ressourcen in Ihren separaten Konten erstellen, müssen Sie identische Richtlinien und Berechtigungen implementieren und diese für alle Konten synchronisieren. Stattdessen können Sie alle Benutzer, die eine AWS RAM Ressource gemeinsam nutzen, über einen einzigen Satz von Richtlinien und Berechtigungen verwalten. AWS RAM bietet ein einheitliches Erlebnis für die gemeinsame Nutzung verschiedener Arten von AWS Ressourcen.
- Sorgen Sie für Transparenz und Überprüfbarkeit. Zeigen Sie die Nutzungsdetails für Ihre gemeinsam genutzten Ressourcen an, indem Sie sie in Amazon integrieren AWS RAM CloudWatch und AWS CloudTrail. Weitere Informationen finden Sie AWS CloudTrail in der AWS RAM Dokumentation AWS RAM unter Überwachung EventBridge und Protokollierung von AWS RAM API-Aufrufen mit.

Häufig gestellte Fragen

F: Mit wem kann ich Ressourcen teilen?

A: Sie können Ressourcen mit jedem teilen AWS-Konto. Wenn Sie Teil einer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, können Sie Ressourcen auch mit Organisationseinheiten (OUs) oder mit Ihrer gesamten Organisation teilen. Bei unterstützten Ressourcentypen können Sie Ressourcen auch mit AWS Identity and Access Management (IAM-) Rollen und IAM-Benutzern teilen. Wenn Sie Ressourcen mit Konten teilen, die sich außerhalb Ihrer Organisation befinden, erhalten diese Konten eine Einladung, der Ressourcenfreigabe beizutreten. Nachdem sie die Einladung angenommen haben, können sie beginnen, die gemeinsam genutzten Ressourcen zu nutzen.

F: Fallen Gebühren an, wenn ich meine Ressourcen mit anderen AWS-Konten teile?

A: Nein. Sie können Ressourcen ohne zusätzliche Kosten gemeinsam nutzen.

F: Kann ich die gemeinsame Nutzung einer Ressource beenden?

A: Ja. Um die gemeinsame Nutzung einer Ressource zu beenden, entfernen Sie sie aus der Ressourcenfreigabe oder löschen Sie die Ressourcenfreigabe.

F: Wie kann ich die Sicherheit gewährleisten AWS RAM?

A: Sicherheit ist eine gemeinsame Verantwortung zwischen Ihnen AWS und Ihnen. Das Modell der gemeinsamen Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud. Weitere Informationen finden Sie AWS RAM in der AWS RAM Dokumentation unter Sicherheit.

Bewährte Methoden

- Vermeiden Sie einzelne Fehlerquellen. Verwenden Sie für VPC-Endpunkte und Route 53 Resolver-Endpunkte zwei oder mehr Availability Zones für hohe Verfügbarkeit.
- Verwenden Sie Route 53 Resolver-Endpunkte nicht, um DNS-Abfragen zwischen diesen weiterzuleiten. VPCs Wir empfehlen dringend, den Amazon DNS-Server (.2-Resolver) als DNS-Resolver für alle Instances innerhalb von Amazon zu verwenden. EC2 Dieser Resolver bietet ein Höchstmaß an Verfügbarkeit und Skalierbarkeit bei geringster Latenz.
- Weitere bewährte Methoden finden Sie unter Bewährte Methoden für Resolver in der Route 53-Dokumentation.

Ressourcen

- Zugriff und AWS-Service Verwendung eines VPC-Endpunkts mit einer Schnittstelle (Amazon VPC-Dokumentation)
- Teilen Sie Ihre VPC-Subnetze mit anderen Konten (Amazon VPC-Dokumentation)
- Gemeinsam nutzbare Amazon VPC-Ressourcen (Dokumentation)AWS RAM
- Integration AWS Transit Gateway mit AWS PrivateLink und Amazon Route 53 Resolver (AWS Blogbeitrag)
- Zentralisierung von VPC-Endpunkten mit AWS Transit Gateway(Referenzarchitektur)AWS
- Stellen Sie über ein privates Netzwerk eine Connect zu MGN-Daten- und Steuerungsebenen her (AWS Prescriptive Guidance)

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	18. Februar 2025

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.