Réhébergement de vos applications dans une architecture multi-comptes en utilisant des points de AWS terminaison d'interface VPC

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Réhébergement de vos applications dans une architecture multi-comptes en utilisant des points de AWS terminaison d'interface VPC

Table of Contents

Réhébergement de vos applications dans une architecture multi-comptes sur AWS en utilisant les points de terminaison de l'interface VPC

Dipin Jain et Saurabh Shankar, Amazon Web Services

Février 2025 (historique du document)

De nombreuses entreprises réhébergent (transfèrent et transfèrent) leurs applications AWS vers des environnements réseau isolés ou semi-isolés, y compris des centres de données sur site et d'autres infrastructures cloud ou hybrides, en utilisant. AWS Transform MGN Ces réseaux isolés n'autorisent généralement aucun trafic de sortie vers les points de terminaison publics décrits dans les exigences réseau pour MGN. Vous pouvez remédier à cette limitation en utilisant des points de terminaison d'interface de cloud privé virtuel (VPC), comme indiqué dans le modèle de guidage AWS prescriptif Connect to MGN data and control planes via un réseau privé.

De nombreuses organisations utilisent également une architecture de zone d'atterrissage multi-comptes (MALZ) pour l'isolation, la sécurité et les avantages de facturation par compte. Pour permettre la migration « lift-and-shift » en utilisant le MGN sur un réseau sécurisé vers plusieurs cibles Comptes AWS, vous devez créer des points de terminaison d'interface VPC sur chaque cible. Compte AWS Cela augmente le coût et la complexité de la gestion de ces ressources.

Ce guide décrit les options de centralisation des points de terminaison de l'interface VPC afin de réhéberger vos applications dans une architecture multi-comptes sur. AWS Ces options simplifient l'architecture et réduisent les coûts associés à de tels cas d'utilisation.

Résultats commerciaux ciblés

Ce guide propose des solutions pour trois cas d'utilisation du réhébergement. Il met l'accent sur la réduction des coûts et des frais opérationnels, ainsi que sur l'amélioration de la sécurité et de l'utilisation des ressources.

Cas d'utilisation :

- Vos applications sont mappées à différentes unités commerciales, et vous souhaitez les migrer vers différents comptes AWS cibles en même temps Région AWS afin de simplifier la facturation et l'isolation.

  La solution à ce scénario consiste à créer des points de terminaison VPC dans un compte AWS réseau central et à les utiliser AWS Transit Gateway pour se connecter à des comptes d'applications cibles.
- Vous souhaitez migrer vos applications vers différents comptes AWS cibles en plusieurs fois Régions AWS afin de garder vos applications proches de vos utilisateurs ou de faciliter la reprise après sinistre. Il s'agit d'une extension du premier cas d'utilisation.

  La solution à ce scénario consiste à créer des points de terminaison VPC pour chacun d'entre eux Région AWS dans un compte réseau AWS central et à permettre l'accès entre comptes à l'aide d'une passerelle de transit pair et d'Amazon Route 53.
- Vos applications sont mappées à différentes unités commerciales et vous souhaitez les migrer vers différents comptes AWS cibles de la même manière à des Région AWS fins de facturation et d'isolation. Vous souhaitez également utiliser moins de VPC pour le transfert MGN et gérer de manière centralisée le routage des VPC intermédiaires afin de réduire les coûts et les frais administratifs.

  La solution à ce scénario implique le partage des points de terminaison VPC à l'aide d'un sous-réseau de zone de transit partagé, avec AWS Organizations and (). AWS Resource Access Manager AWS RAM

Public visé

Ce guide s'adresse aux consultants en migration, aux architectes d'applications, aux architectes d'infrastructure et aux propriétaires d'applications qui recherchent des solutions pour ces cas d'utilisation.

Solution 1 : créer des points de terminaison VPC dans un compte réseau central pour une seule région

Cas d’utilisation

Vos applications sont mappées à différentes unités commerciales et vous souhaitez les migrer vers différents comptes AWS cibles de la même manière à des Région AWS fins de facturation et d'isolation.

Défis

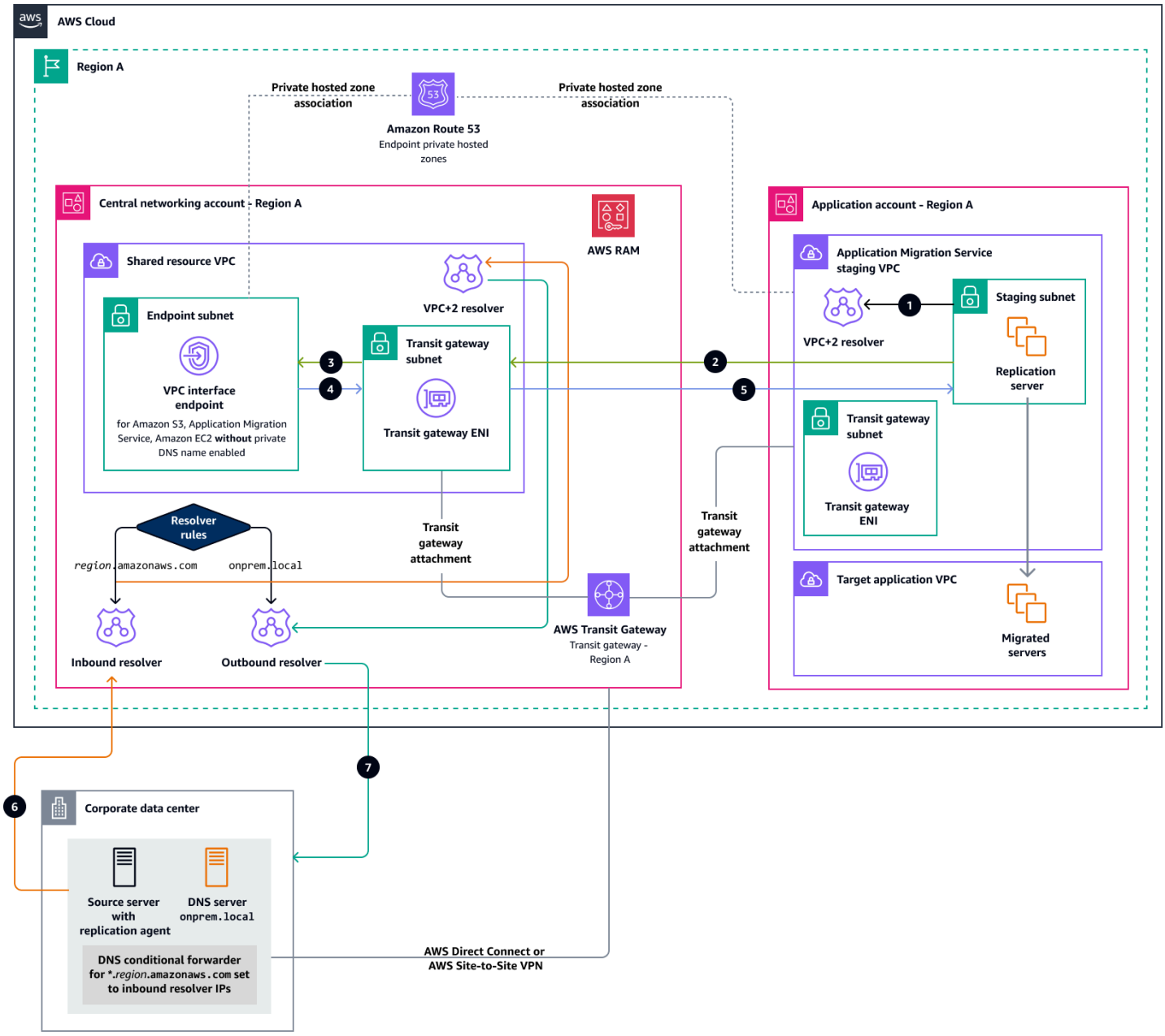
Pour y parvenir via un réseau privé, vous devez créer plusieurs points de terminaison d'interface VPC dans chaque compte cible. Cela augmente les frais administratifs et les coûts liés à la maintenance des terminaux. (Voir AWS PrivateLink les tarifs.)

Solution

Créez des points de terminaison VPC dans un compte AWS réseau central et utilisez Transit Gateway pour vous connecter aux comptes d'applications cibles.

Architecture

Le schéma suivant illustre l'architecture de cette solution.



Dans le diagramme, les chiffres représentent le flux de trafic suivant :

1. L'instance Amazon Elastic Compute Cloud (Amazon EC2) ou le serveur de réplication MGN qui doit se connecter à Amazon Simple Storage Service (Amazon S3), MGN ou Amazon EC2 via un point de terminaison d'interface situé dans le compte réseau central VPC doit d'abord résoudre le nom de domaine en interrogeant le résolveur VPC+2. La zone hébergée privée du point de terminaison est associée au VPC intermédiaire MGN dans la même région pour terminer la résolution du domaine.

> **Note**
>
> Pour chaque zone hébergée privée que vous associez à un VPC, le résolveur crée une règle et l'associe au VPC. Si vous associez la zone hébergée privée à plusieurs VPC, le résolveur associe la règle à tous les VPC.

2. Lorsque l'instance connaît l'adresse IP privée à laquelle se connecter, elle envoie le trafic à la passerelle de transit ENI. Le trafic est envoyé à la passerelle de transit et transféré au VPC de ressources partagées, en fonction de la table de routage de la passerelle de transit.
3. La passerelle de transit ENI du VPC à ressources partagées transmet le trafic au point de terminaison d'interface correspondant.
4. Le point de terminaison VPC renvoie la réponse à la passerelle de transit ENI.
5. Le trafic est redirigé vers la passerelle de transit. Comme indiqué dans la table de routage de la passerelle de transit, le trafic est envoyé au VPC intermédiaire MGN en étoile. La réponse est envoyée par la passerelle de transit ENI à la destination, c'est-à-dire à l'instance EC2 ou au serveur de réplication MGN.
6. Une application cliente située dans le centre de données de l'entreprise résout un nom de domaine sous la forme `<aws_service>.<aws_region>.amazonaws.com` (par exemple,`mgn.us-east-1.amazonaws.com`). Il envoie la requête à son résolveur DNS préconfiguré. Le résolveur DNS du centre de données de l'entreprise dispose d'une règle de transfert qui dirige toute requête DNS pour des `amazonaws.com` domaines vers le point de terminaison entrant Route 53 Resolver. Transit Gateway transmet la requête au VPC de ressources partagées, qui transmet la requête DNS au point de terminaison entrant Route 53 Resolver.

   Le point de terminaison entrant Route 53 Resolver utilise le résolveur VPC+2. La zone hébergée privée du point de terminaison associée à la ressource partagée VPC contient les enregistrements DNS pour lesquels `amazonaws.com` Route 53 Resolver peut résoudre la requête.
7. Le point de terminaison sortant Route 53 Resolver renvoie la réponse à la requête DNS à l'application cliente locale.

Étapes d’implémentation

Pour configurer l'architecture illustrée dans le schéma précédent, procédez comme suit :

1. Connectez le centre de données de votre entreprise au compte réseau central AWS via AWS Direct Connect ou AWS Site-to-Site VPN.
2. Dans le compte réseau, utilisez Transit Gateway pour assurer la connectivité entre les VPC. La passerelle de transit est partagée entre Comptes AWS en utilisant AWS RAM et en outre connectée au sous-réseau intermédiaire du compte de l'application cible via une pièce jointe VPC.

> **Note**
>
> Il Comptes AWS n'est pas nécessaire que Target fasse partie de la même AWS organisation. Pour plus d'informations, consultez la section Ressources partageables dans la AWS RAM documentation.

3. Créez des points de terminaison d'interface VPC pour Amazon EC2, MGN et Amazon S3 dans le compte réseau central sans activer de nom DNS privé.

> **Note**
>
> Lorsque vous créez un point de terminaison VPC pour un Service AWS, vous pouvez activer le DNS privé. Lorsqu'il est activé, le paramètre crée pour vous une zone hébergée privée gérée de Route 53. Cette zone gérée résout le nom DNS au sein d'un VPC. Cependant, cela ne fonctionne pas en dehors du VPC. C'est la raison pour laquelle vous utilisez le partage de zone hébergé privé et Route 53 Resolver pour obtenir une résolution de nom unifiée pour les points de terminaison VPC partagés.

4. Créez une zone hébergée privée pour chaque point de terminaison (MGN, Amazon EC2, Amazon S3). Par exemple, pour MGN dans la `us-east-1` région :
   - Créez une zone hébergée privée avec le nom de domaine`mgn.us-east-1.amazonaws.com`.
   - Créez un enregistrement d'hôte de type A qui pointe le nom de domaine vers les adresses IP des terminaux.
5. Créez des règles entrantes et sortantes de Route 53 Resolver pour faciliter la résolution DNS hybride, et partagez les règles avec les personnes requises Compte AWS dans la même région.

Solution 2 : créer des points de terminaison VPC dans un compte réseau central pour plusieurs régions

Cas d’utilisation

Vous souhaitez migrer plusieurs fois vos applications ou serveurs vers différents comptes AWS cibles Régions AWS, afin de les garder proches de vos utilisateurs ou de garantir la continuité des activités dans des scénarios de reprise après sinistre. Il s'agit d'une extension du premier cas d'utilisation.

Défis

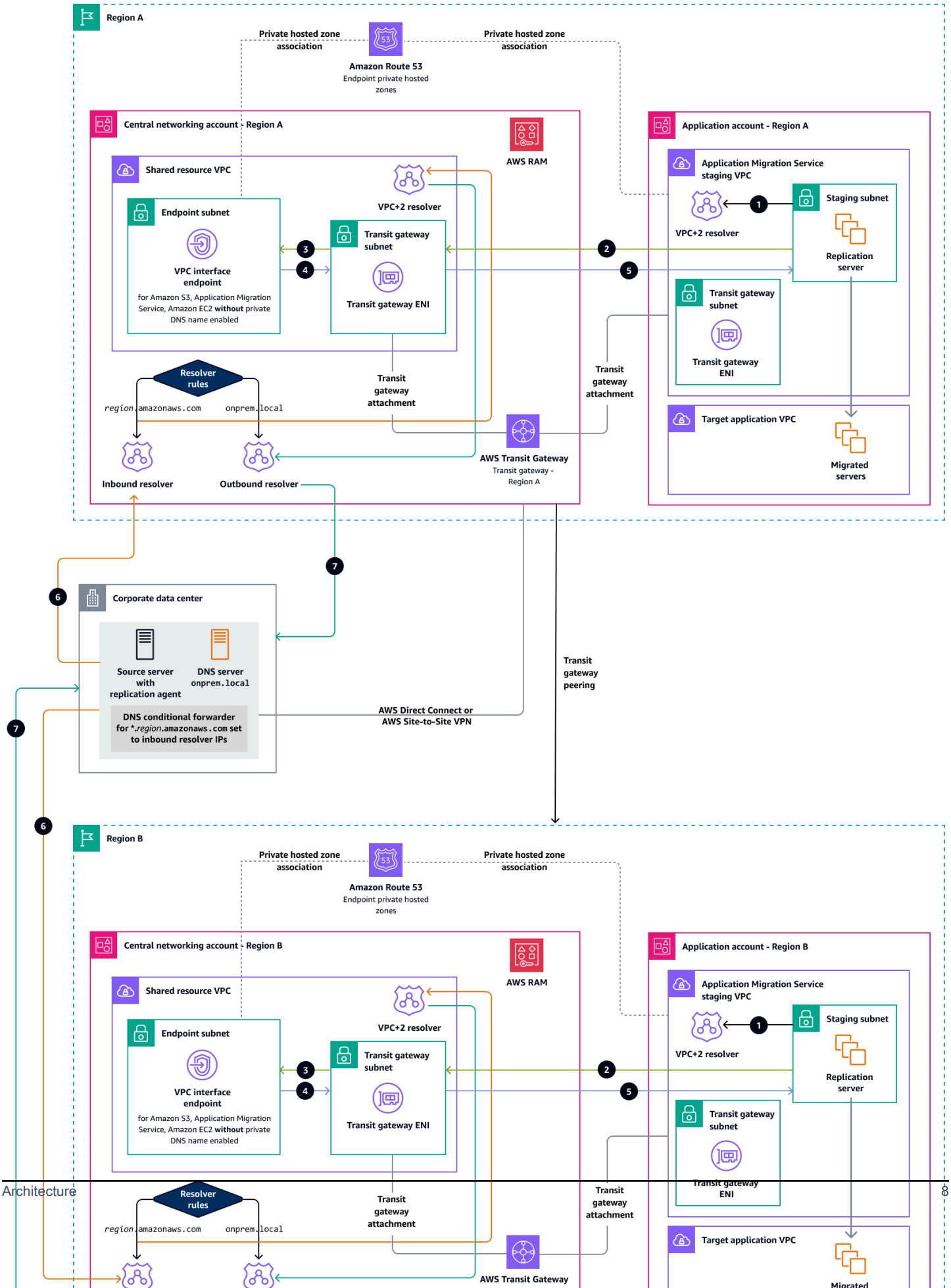
Pour y parvenir via un réseau privé, vous devez créer plusieurs points de terminaison d'interface VPC dans chaque compte cible. Cela devient encore plus complexe dans un scénario multirégional et augmente les frais administratifs et les coûts liés à la maintenance de plusieurs points de terminaison. (Voir AWS PrivateLink les tarifs.)

Solution

Créez des points de terminaison VPC pour chaque région dans un compte réseau central et activez l'accès entre comptes en utilisant une passerelle de transit pair et la Route 53.

Architecture

Le schéma suivant illustre l'architecture de cette solution.


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

Le flux de trafic est le même que dans la solution 1, sauf que les comptes des deux régions sont connectés par le biais d'une passerelle de transit peering.

Étapes d’implémentation

1. Dans le compte réseau central, créez un point de terminaison d'interface VPC pour chaque cible. Région AWS
2. Dans le compte réseau central, créez une zone hébergée privée pour chaque point de terminaison de chaque région et associez la zone aux VPC de l'application cible dans la même région.
3. Dans le compte réseau central, créez une passerelle de transit pour chaque région cible et partagez la passerelle avec les comptes cibles de la même région en utilisant AWS RAM.
4. Connectez les passerelles de transport en commun entre les régions à l'aide de l'appairage des passerelles de transit et mettez à jour les tables de routage des passerelles de transport en commun selon les besoins.
5. Dans le compte réseau central, créez des règles de résolution pour chaque région cible et partagez ces règles avec les comptes cibles de la même région en utilisant AWS RAM.

Solution 3 : partage des points de terminaison de l'interface VPC

Cas d’utilisation

Vos applications sont mappées à différentes unités commerciales et vous souhaitez les migrer vers différents comptes AWS cibles dans la même région à des fins de facturation et d'isolation.

Défis

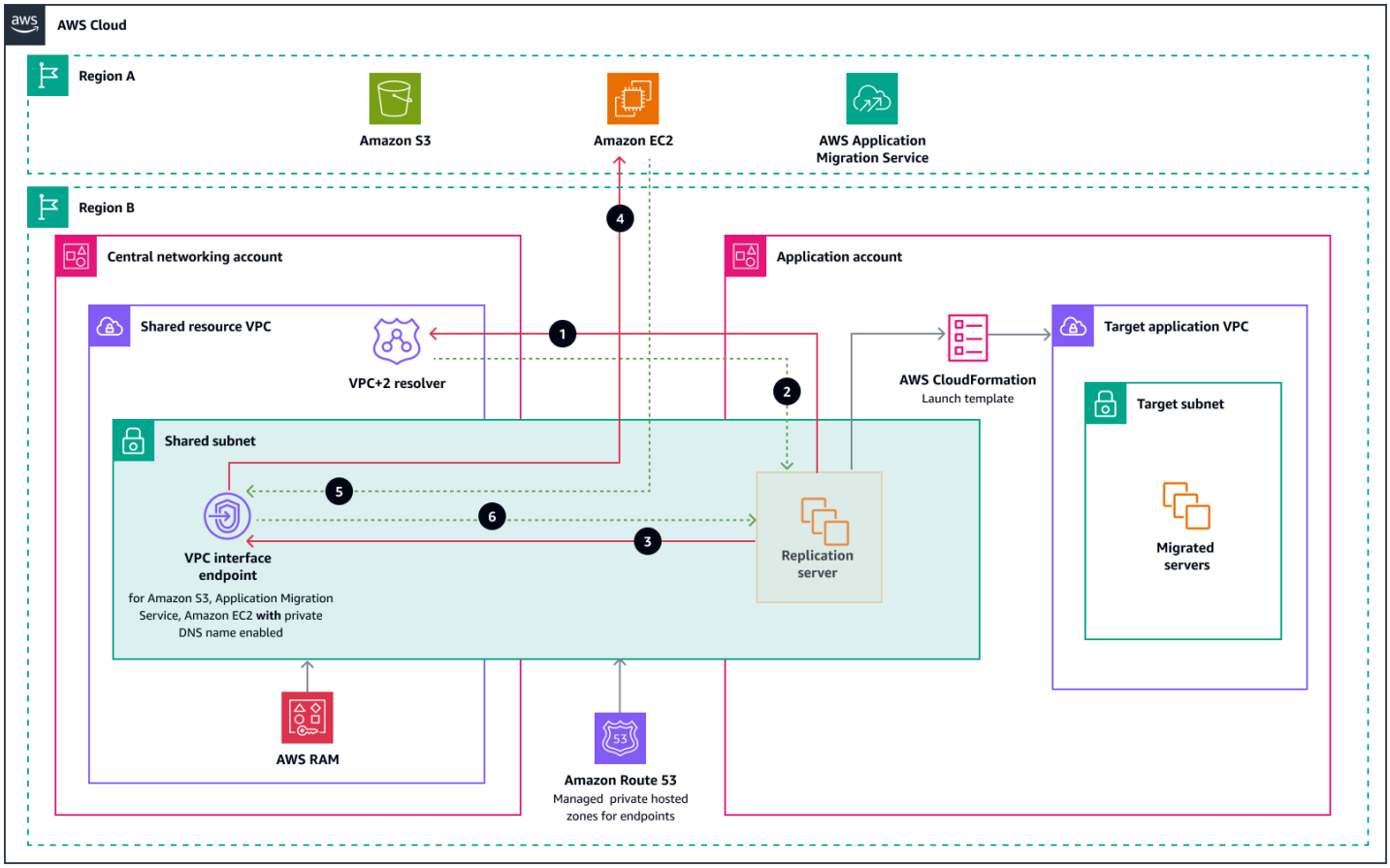
Les comptes de charge de travail multiples augmentent à la fois les frais administratifs et le coût des points de terminaison d'interface VPC individuels dans chaque compte. Par conséquent, vous souhaiterez peut-être avoir moins de VPC intermédiaires pour MGN et gérer le routage de manière centralisée pour les VPC intermédiaires afin de réduire les coûts et les frais administratifs.

Solution

Partagez les points de terminaison VPC à l'aide d'un sous-réseau de zone de transit partagé, et. AWS Organizations AWS RAM Pour plus d'informations sur le partage VPC, consultez la documentation Amazon VPC.

Architecture

Le schéma suivant illustre l'architecture de cette solution.



Le diagramme illustre le flux de trafic suivant :

1. Le serveur de réplication MGN interroge le DNS VPC+2 pour résoudre le point de terminaison de l'API pour MGN, Amazon EC2 ou Amazon S3.

2. Le DNS VPC+2 résout l'adresse IP privée du point de terminaison à l'aide de zones hébergées privées AWS gérées et répond au serveur de réplication MGN.

3-6. Le serveur de réplication utilise cette adresse IP pour se connecter à l' Service AWS API via le point de terminaison de l'interface du service.

Étapes d’implémentation

1. Dans le compte réseau central, créez le VPC intermédiaire et le sous-réseau pour MGN.
2. Créez des points de terminaison pour MGN, Amazon EC2 ou Amazon S3 avec les noms DNS privés activés. Cela crée une zone hébergée privée AWS gérée et l'associe au VPC intermédiaire.

3. Partagez le sous-réseau intermédiaire avec les comptes d'applications cibles de la même AWS organisation et Région AWS.
4. Pour une connectivité hybride entre AWS et votre centre de données sur site (non illustré dans le schéma précédent), utilisez Transit Gateway Direct Connect ou AWS Site-to-Site VPN avec les points de terminaison Route 53 Resolver, comme indiqué dans les solutions 1 et 2.

Limitations

- Le VPC Comptes AWS pour les participants et le VPC propriétaire doivent faire partie de la même organisation dans. AWS Organizations
- Pour obtenir la liste des ressources partageables, consultez la documentation Amazon VPC.
- Pour connaître les limites du partage VPC, consultez la documentation Amazon VPC.

Considérations relatives à la conception

- Pour réduire vos frais d'exploitation, créez une ressource une seule fois, puis AWS RAM utilisez-la pour la partager avec d'autres comptes. Cela élimine le besoin de fournir des ressources dupliquées dans chaque compte et réduit les frais d'exploitation.
- Simplifiez la gestion de la sécurité de vos ressources partagées en utilisant un ensemble unique de politiques et d'autorisations. Si vous créez des ressources dupliquées dans vos comptes distincts, vous devez mettre en œuvre des politiques et des autorisations identiques et les synchroniser sur tous les comptes. Au lieu de cela, vous pouvez gérer tous les utilisateurs qui partagent une AWS RAM ressource par le biais d'un ensemble unique de politiques et d'autorisations. AWS RAM offre une expérience cohérente pour le partage de différents types de AWS ressources.
- Offrez de la visibilité et de l'auditabilité. Consultez les détails d'utilisation de vos ressources partagées en les AWS RAM intégrant à Amazon CloudWatch et AWS CloudTrail. Pour plus d'informations, consultez la section Surveillance de AWS RAM l'utilisation EventBridge et journalisation des appels d' AWS RAM API AWS CloudTrail dans la AWS RAM documentation.

FAQ

Q : Avec qui puis-je partager des ressources ?

R : Vous pouvez partager des ressources avec n'importe qui Compte AWS. Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, vous pouvez également partager des ressources avec des unités organisationnelles (OUs) ou avec l'ensemble de votre organisation. Pour les types de ressources pris en charge, vous pouvez également partager des ressources avec des rôles Gestion des identités et des accès AWS (IAM) et des utilisateurs IAM. Si vous partagez des ressources avec des comptes extérieurs à votre organisation, ces comptes reçoivent une invitation à rejoindre le partage des ressources. Après avoir accepté l'invitation, ils peuvent commencer à utiliser les ressources partagées.

Q : Est-ce que je devrai payer des frais pour partager mes ressources avec d'autres ? Comptes AWS

R : Non. Vous pouvez partager des ressources sans frais supplémentaires.

Q : Puis-je arrêter de partager une ressource ?

R : Oui. Pour arrêter de partager une ressource, supprimez-la du partage de ressources ou supprimez le partage de ressources.

Q : Comment puis-je garantir la sécurité AWS RAM ?

R : La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud. Pour plus d'informations, consultez la section Sécurité AWS RAM dans la AWS RAM documentation.

Bonnes pratiques

- Évitez les points de défaillance uniques. Pour les points de terminaison VPC et les points de terminaison Route 53 Resolver, utilisez au moins deux zones de disponibilité pour une haute disponibilité.
- N'utilisez pas les points de terminaison Route 53 Resolver pour transférer des requêtes DNS entre eux. VPCs Nous vous recommandons vivement d'utiliser le serveur DNS Amazon (résolveur .2) comme résolveur DNS pour toutes les instances d'Amazon. EC2 Ce résolveur fournit le plus haut niveau de disponibilité et d'évolutivité avec la latence la plus faible.
- Pour connaître les meilleures pratiques supplémentaires, consultez la section Meilleures pratiques pour Resolver dans la documentation de Route 53.

Ressources

- Accès et Service AWS utilisation d'un point de terminaison VPC d'interface (documentation Amazon VPC)
- Partagez vos sous-réseaux VPC avec d'autres comptes (documentation Amazon VPC)
- Ressources AWS RAM Amazon VPC partageables (documentation)
- Intégration AWS Transit Gateway avec AWS PrivateLink et Amazon Route 53 Resolver (article de AWS blog)
- Centralisation des points de terminaison VPC AWS Transit Gateway avec AWS (architecture de référence)
- Connectez-vous aux données MGN et aux plans de contrôle via un réseau privé (directivesAWS prescriptives)

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Publication initiale	—	18 février 2025

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.