VPC インターフェイスエンドポイント AWS を使用して、 のマルチアカウントアーキテクチャでアプリケーションをリホストする

AWS 規範ガイダンス

AWS 規範ガイダンス: VPC インターフェイスエンドポイント AWS を使用して、 のマルチアカウントアーキテクチャでアプリケーションをリホストする

Table of Contents

VPC インターフェイスエンドポイント AWS を使用した でのマルチアカウントアーキテクチャでのアプリケーションのリホスト

Dipin Jain and Saurabh Shankar、Amazon Web Services

2025 年 2 月 (ドキュメント履歴)

多くの組織は、 を使用して、オンプレミスのデータセンターやその他のクラウドインフラストラクチャやハイブリッドインフラストラクチャなど、隔離または半隔離されたネットワーク環境 AWS から にアプリケーションをリホスト (リフトアンドシフト) しますAWS Transform MGN。これらの分離されたネットワークは通常、MGN のネットワーク要件で説明されているパブリックエンドポイントへの出力トラフィックを許可しません。この制限に対処するには、 AWS 「規範ガイダンスパターン プライベートネットワーク経由で MGN データおよびコントロールプレーンに接続する」で説明されているように、仮想プライベートクラウド (VPC) インターフェイスエンドポイントを使用します。

多くの組織では、分離、セキュリティ、アカウントごとの請求上の利点のために、マルチアカウントランディングゾーン (MALZ) アーキテクチャも使用しています。保護されたネットワーク経由で MGN を使用してlift-and-shift移行を複数のターゲットに有効にするには AWS アカウント、すべてのターゲットに VPC インターフェイスエンドポイントを作成する必要があります AWS アカウント。これにより、これらのリソースを管理するコストと複雑さが増します。

このガイドでは、アプリケーションをマルチアカウントアーキテクチャでリホストするための VPC インターフェイスエンドポイントを一元化するためのオプションについて説明します AWS。これらのオプションにより、アーキテクチャが簡素化され、このようなユースケースのコストを削減できます。

ターゲットを絞ったビジネス成果

このガイドでは、3 つのリホストユースケースのソリューションを提供します。コスト削減と運用オーバーヘッドの削減、セキュリティとリソース使用率の向上に焦点を当てています。

ユースケース:

- アプリケーションは異なるビジネスユニットにマッピングされ、請求と分離を簡素化 AWS リージョン するために、同じ 内の異なる AWS ターゲットアカウントに移行する必要があります。

このシナリオの解決策は、中央 AWS ネットワークアカウントに VPC エンドポイントを作成し、AWS Transit Gateway を使用してターゲットアプリケーションアカウントに接続することです。

- アプリケーションを複数の の異なる AWS ターゲットアカウントに移行 AWS リージョン して、アプリケーションをユーザーに近づけたり、ディザスタリカバリを容易にしたりしたい。これは、最初のユースケースの拡張機能です。

  このシナリオの解決策には、 AWS 中央ネットワークアカウント AWS リージョン 内の各 の VPC エンドポイントを作成し、ピア接続されたトランジットゲートウェイと Amazon Route 53 を使用してクロスアカウントアクセスを有効にすることが含まれます。
- アプリケーションは異なるビジネスユニットにマッピングされ、請求と分離 AWS リージョン の目的で、同じ 内の異なる AWS ターゲットアカウントに移行します。また、MGN ステージングに使用する VPCs の数を減らし、ステージング VPCs のルーティングを一元管理してコストと管理オーバーヘッドを削減することもできます。

  このシナリオのソリューションでは、 AWS Organizations および AWS Resource Access Manager () で共有ステージングエリアサブネットを使用して VPC エンドポイントを共有します AWS RAM。

対象者

このガイドは、これらのユースケースのソリューションを探している移行コンサルタント、アプリケーションアーキテクト、インフラストラクチャアーキテクト、アプリケーション所有者を対象としています。

解決策 1: 1 つのリージョンの中央ネットワークアカウントに VPC エンドポイントを作成する

ユースケース

アプリケーションは異なるビジネスユニットにマッピングされ、請求と分離 AWS リージョン の目的で、同じ 内の異なる AWS ターゲットアカウントに移行します。

チャレンジ

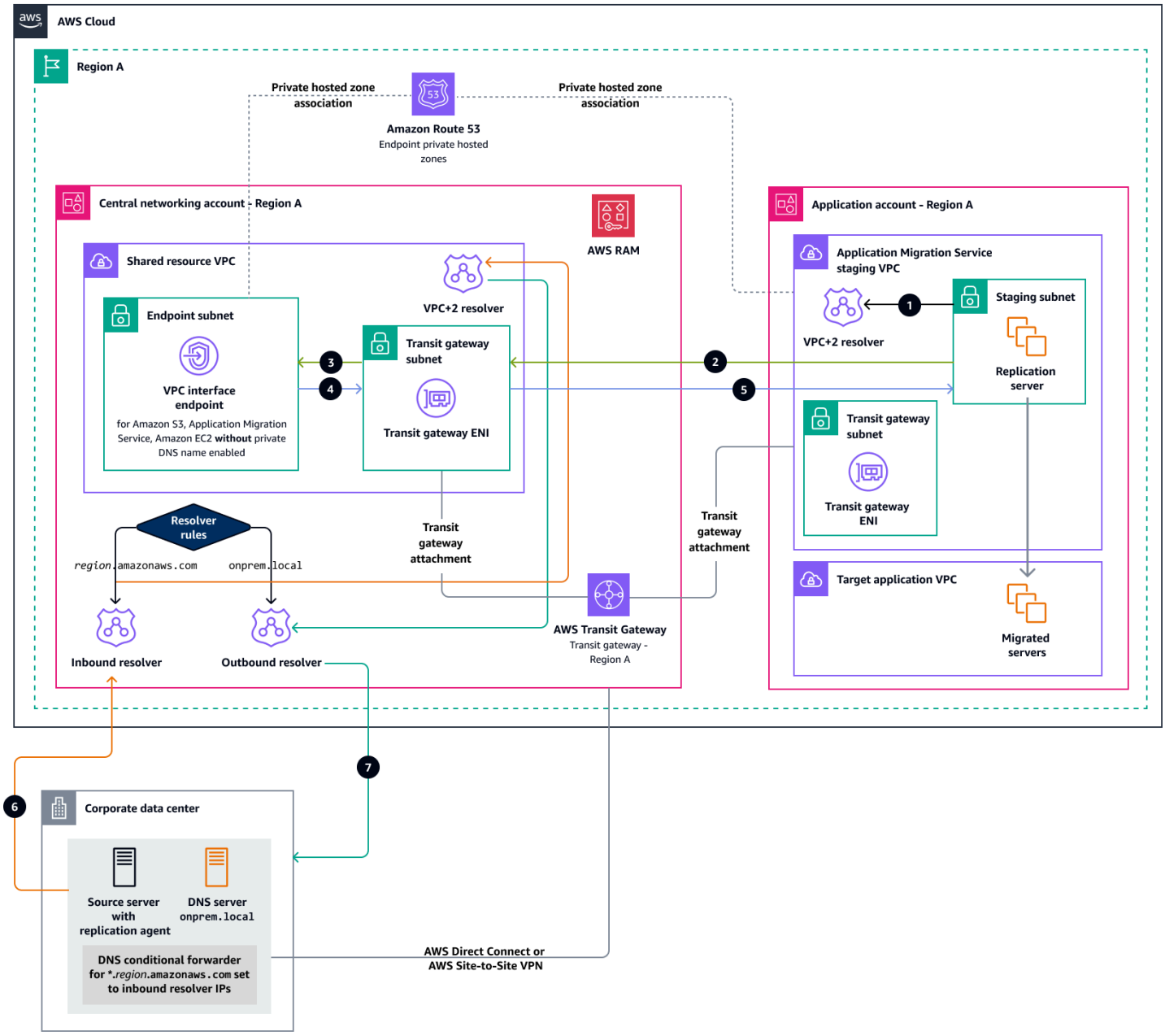
プライベートネットワーク経由でこれを実現するには、すべてのターゲットアカウントに複数の VPC インターフェイスエンドポイントを作成する必要があります。これにより、エンドポイントを維持するための管理上のオーバーヘッドとコストが増加します。(「AWS PrivateLink の料金」を参照してください)。

ソリューション

中央 AWS ネットワークアカウントに VPC エンドポイントを作成し、Transit Gateway を使用してターゲットアプリケーションアカウントに接続します。

アーキテクチャ

次の図は、このソリューションのアーキテクチャを示しています。



この図では、数字は次のトラフィックフローを表しています。

1. 中央ネットワークアカウント VPC にあるインターフェイスエンドポイントを介して Amazon Simple Storage Service (Amazon EC2 Amazon S3、MGN、または Amazon EC2 に接続する必要がある Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは MGN レプリケーションサーバーは、まず VPC+2 リゾルバーにクエリを実行してドメイン名を解決する必要があります。エンドポイントのプライベートホストゾーンは、ドメイン解決を完了するために、同じリージョンの MGN ステージング VPC に関連付けられます。

> **Note**
>
> VPC に関連付けるプライベートホストゾーンごとに、リゾルバーはルールを作成し、VPC に関連付けます。プライベートホストゾーンを複数の VPCs に関連付けると、リゾルバーはルールをすべての VPCs。

2. インスタンスは、接続先のプライベート IP を知ると、トラフィックをトランジットゲートウェイ ENI に送信します。トラフィックはトランジットゲートウェイに送信され、トランジットゲートウェイルートテーブルに基づいて共有リソース VPC に転送されます。
3. 共有リソース VPC のトランジットゲートウェイ ENI は、トラフィックを対応するインターフェイスエンドポイントに転送します。
4. VPC エンドポイントは、トランジットゲートウェイ ENI にレスポンスを返します。
5. トラフィックはトランジットゲートウェイに転送されます。トランジットゲートウェイルートテーブルで指定されているように、トラフィックはスポーク MGN ステージング VPC に送信されます。レスポンスは、トランジットゲートウェイ ENI によって送信先、つまり EC2 インスタンスまたは MGN レプリケーションサーバーに送信されます。
6. 企業データセンターにあるクライアントアプリケーションは、ドメイン名を 形式で解決します `<aws_service>.<aws_region>.amazonaws.com` (例: `mgn.us-east-1.amazonaws.com`)。事前設定された DNS リゾルバーにクエリを送信します。企業データセンターの DNS リゾルバーには、`amazonaws.com`ドメインの DNS クエリを Route 53 Resolver インバウンドエンドポイントにポイントする転送ルールがあります。Transit Gateway は、クエリを共有リソース VPC に転送します。これにより、Route 53 Resolver インバウンドエンドポイントで DNS クエリが転送されます。

   Route 53 Resolver インバウンドエンドポイントは VPC+2 リゾルバーを使用します。共有リソース VPC に関連付けられているエンドポイントプライベートホストゾーンは、 の DNS レコードを保持するため`amazonaws.com`、Route 53 Resolver はクエリを解決できます。
7. Route 53 Resolver アウトバウンドエンドポイントは、オンプレミスクライアントアプリケーションに DNS クエリレスポンスを返します。

実装手順

前の図に示すアーキテクチャを設定するには、次の手順に従います。

1. AWS Direct Connect または を使用して、企業のデータセンターを の中央ネットワークアカウント AWS に接続します AWS Site-to-Site VPN。
2. ネットワークアカウントで、Transit Gateway を使用して VPCs間の接続を提供します。トランジットゲートウェイは、 AWS アカウント を使用して 間で共有され AWS RAM、VPC アタッチメントを介してターゲットアプリケーションアカウントのステージングサブネットにさらに接続します。

> **Note**
>
> ターゲットは同じ AWS 組織の一部である AWS アカウント 必要はありません。詳細については、 AWS RAM ドキュメントの「共有可能なリソース」を参照してください。

3. プライベート DNS 名を有効にせずに、中央ネットワークアカウントに Amazon EC2、MGN、Amazon S3 の VPC インターフェイスエンドポイントを作成します。

> **Note**
>
> への VPC エンドポイントを作成するときに AWS のサービス、プライベート DNS を有効にできます。有効にすると、 設定によってマネージド Route 53 プライベートホストゾーンが作成されます。 このマネージドゾーンは VPC 内の DNS 名を解決します。ただし、VPC の外部では機能しません。これは、プライベートホストゾーン共有と Route 53 Resolver を使用して、共有 VPC エンドポイントの統合名解決に役立つ理由です。

4. エンドポイント (MGN、Amazon EC2、Amazon S3) ごとにプライベートホストゾーンを作成します。たとえば、 `us-east-1`リージョンの MGN の場合:
   - ドメイン名 を使用してプライベートホストゾーンを作成します`mgn.us-east-1.amazonaws.com`。
   - ドメイン名をエンドポイント IPs を指すタイプ A のホストレコードを作成します。
5. Route 53 Resolver のインバウンドルールとアウトバウンドルールを作成してハイブリッド DNS 解決を容易にし、同じリージョン AWS アカウント で必要な とルールを共有します。

解決策 2: 複数のリージョンの中央ネットワークアカウントに VPC エンドポイントを作成する

ユースケース

アプリケーションまたはサーバーを複数の異なる AWS ターゲットアカウントに移行し AWS リージョン、ユーザーの近くに保持したり、ディザスタリカバリシナリオでビジネス継続性を実現したりできます。これは、最初のユースケースの拡張機能です。

チャレンジ

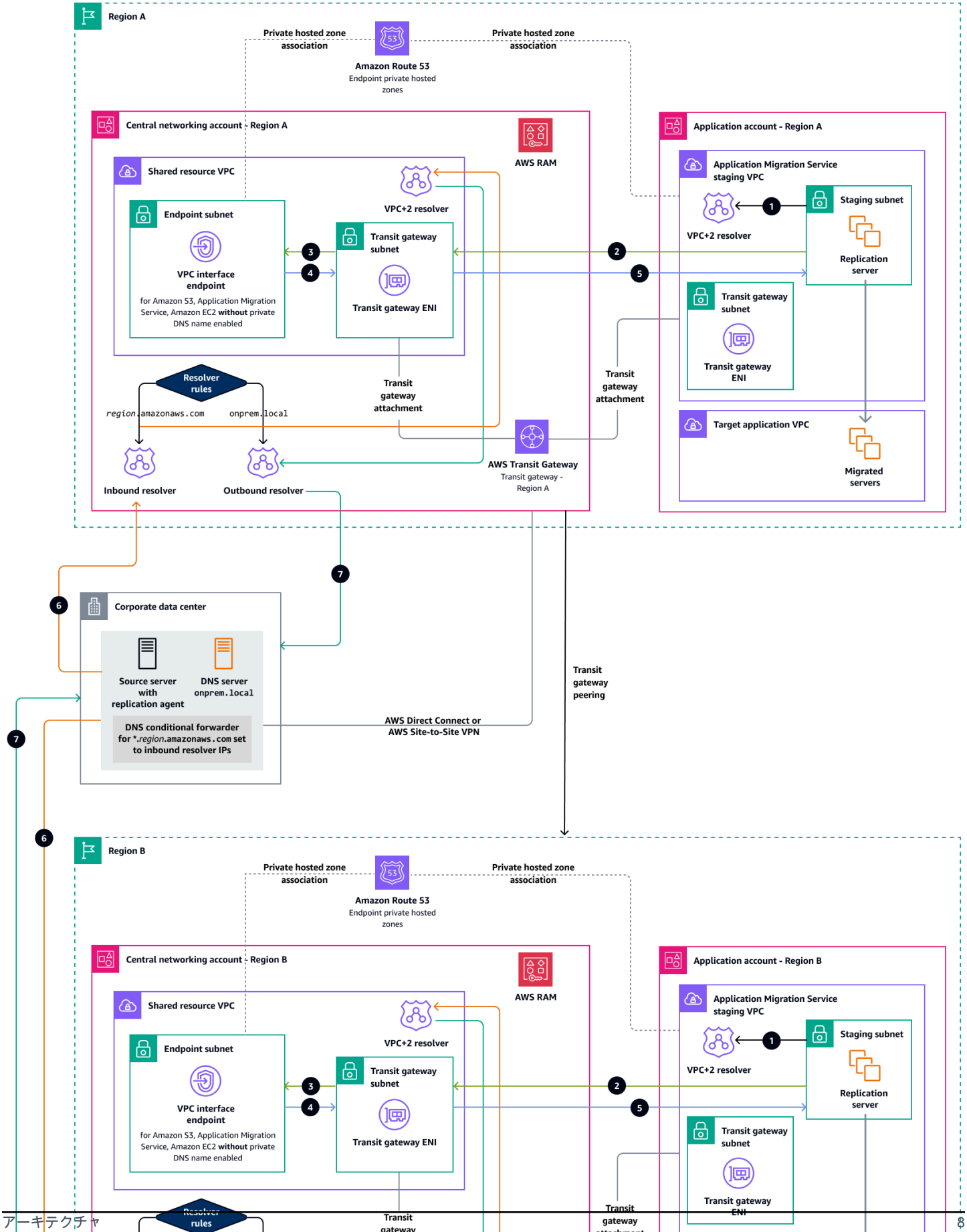
プライベートネットワーク経由でこれを実現するには、すべてのターゲットアカウントに複数の VPC インターフェイスエンドポイントを作成する必要があります。これは、マルチリージョンシナリオではさらに複雑になり、複数のエンドポイントを維持するための管理オーバーヘッドとコストが増加します。(「 AWS PrivateLink の料金」を参照してください)。

ソリューション

中央ネットワークアカウントでリージョンごとに VPC エンドポイントを作成し、ピア接続されたトランジットゲートウェイと Route 53 を使用してクロスアカウントアクセスを有効にします。

アーキテクチャ

次の図は、このソリューションのアーキテクチャを示しています。


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 -

トラフィックフローは、2 つのリージョンのアカウントがトランジットゲートウェイピアリングによって接続されていることを除いて、ソリューション 1 と同じです。

実装手順

1. 中央ネットワークアカウントで、ターゲットごとに VPC インターフェイスエンドポイントを作成します AWS リージョン。
2. 中央ネットワークアカウントで、各リージョンのエンドポイントごとにプライベートホストゾーンを作成し、そのゾーンを同じリージョンのターゲットアプリケーション VPCs に関連付けます。
3. 中央ネットワークアカウントで、ターゲットリージョンごとにトランジットゲートウェイを作成し、 を使用して同じリージョンのターゲットアカウントとゲートウェイを共有します AWS RAM。
4. トランジットゲートウェイピアリングを使用してリージョン間でトランジットゲートウェイを接続し、必要に応じてトランジットゲートウェイルートテーブルを更新します。
5. 中央ネットワークアカウントで、ターゲットリージョンごとにリゾルバールールを作成し、 を使用してこれらのルールを同じリージョンのターゲットアカウントと共有します AWS RAM。

解決策 3: VPC インターフェイスエンドポイントの共有

ユースケース

アプリケーションは異なるビジネスユニットにマッピングされ、請求と分離の目的で、同じリージョン内の異なる AWS ターゲットアカウントに移行します。

チャレンジ

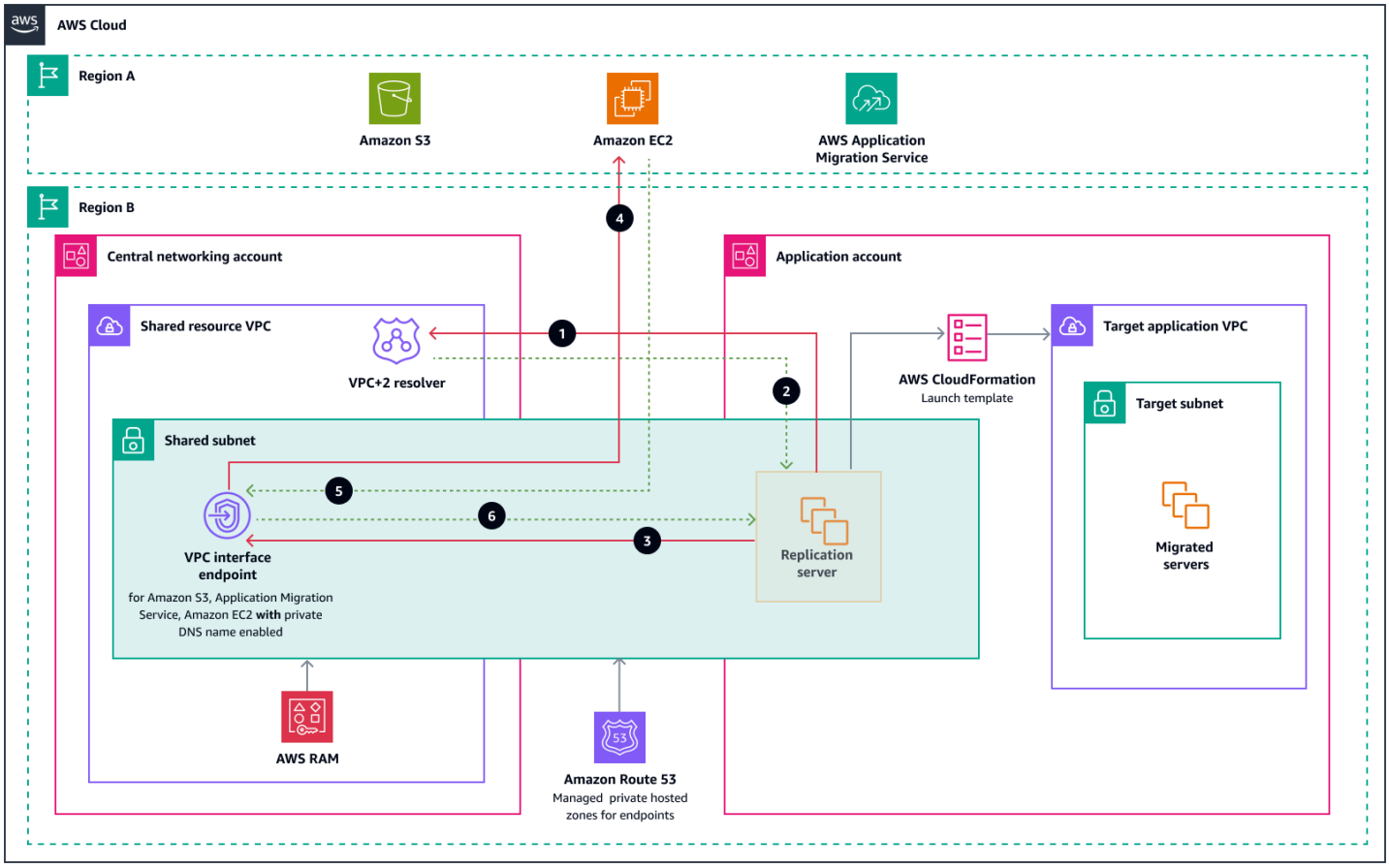
複数のワークロードアカウントでは、管理オーバーヘッドと各アカウントの個々の VPC インターフェイスエンドポイントのコストの両方が増加します。したがって、MGN VPCs を減らし、ステージング VPCs のルーティングを一元管理して、コストと管理オーバーヘッドを削減できます。

ソリューション

共有ステージングエリアサブネット、 AWS Organizationsおよび を使用して VPC エンドポイントを共有します AWS RAM。VPC 共有の詳細については、Amazon VPC ドキュメントを参照してください。

アーキテクチャ

次の図は、このソリューションのアーキテクチャを示しています。



この図は、次のトラフィックフローを示しています。

1. MGN レプリケーションサーバーは VPC+2 DNS をクエリして、MGN、Amazon EC2、または Amazon S3 の API エンドポイントを解決します。

2. VPC+2 DNS は、マネージドプライベートホストゾーンの AWS 助けを借りてエンドポイントのプライベート IP を解決し、MGN レプリケーションサーバーに応答します。

3～6。レプリケーションサーバーは、その IP を使用して、サービスのインターフェイスエンドポイントを介して AWS のサービス API に接続します。

実装手順

1. 中央ネットワークアカウントで、MGN のステージング VPC とサブネットを作成します。
2. プライベート DNS 名を有効にして、MGN、Amazon EC2、または Amazon S3 のエンドポイントを作成します。これにより、 AWS マネージドプライベートホストゾーンが作成され、ステージング VPC に関連付けられます。

3. ステージングサブネットを同じ AWS 組織内のターゲットアプリケーションアカウントと共有します AWS リージョン。
4. AWS とオンプレミスデータセンター間のハイブリッド接続 (前の図に示されていない) には、ソリューション 1 とソリューション 2 に示すように、Transit Gateway、 Direct Connect または AWS Site-to-Site VPN Route 53 Resolver エンドポイントを使用します。

制限事項

- AWS アカウント 参加者 VPCsと所有者 VPC の は、同じ組織に属する必要があります AWS Organizations。
- 共有可能なリソースのリストについては、Amazon VPC ドキュメントを参照してください。
- VPC 共有の制限については、Amazon VPC ドキュメントを参照してください。

設計上の考慮事項

- 運用オーバーヘッドを減らすには、リソースを 1 回作成し、 を使用してそのリソース AWS RAM を他のアカウントと共有します。これにより、すべてのアカウントに重複するリソースをプロビジョニングする必要がなくなり、運用上のオーバーヘッドが軽減されます。
- 単一のポリシーとアクセス許可のセットを使用して、共有リソースのセキュリティ管理を簡素化します。個別のアカウントに重複するリソースを作成する場合は、同じポリシーとアクセス許可を実装し、すべてのアカウント間で同期を維持する必要があります。代わりに、単一のポリシーとアクセス許可セットを使用して AWS RAM リソースを共有するすべてのユーザーを管理できます。は、さまざまなタイプの AWS リソースを共有するための一貫したエクスペリエンス AWS RAM を提供します。
- 可視性と監査可能性を提供します。Amazon CloudWatch および AWS RAM と統合して、共有リソースの使用状況の詳細を表示します AWS CloudTrail。詳細については、 AWS RAM ドキュメントのEventBridge AWS RAM を使用したモニタリング」と「 を使用した AWS RAM API コールのログ記録 AWS CloudTrail」を参照してください。

よくある質問

Q: リソースは誰と共有できますか？

A: リソースは任意の と共有できます AWS アカウント。の組織に属 AWS Organizations していて、組織内での共有が有効になっている場合は、組織単位 (OUs) または組織全体とリソースを共有することもできます。サポートされているリソースタイプでは、 AWS Identity and Access Management (IAM) ロールおよび IAM ユーザーとリソースを共有することもできます。組織外のアカウントとリソースを共有すると、それらのアカウントはリソース共有に参加するための招待を受け取ります。招待を受け入れたら、共有リソースの使用を開始できます。

Q: 他の とリソースを共有した場合、料金が発生しますか AWS アカウント？

A: いいえ。リソースは追加料金なしで共有できます。

Q: リソースの共有を停止できますか？

A: はい。リソースの共有を停止するには、リソース共有から削除するか、リソース共有を削除します。

Q: でセキュリティを確保するにはどうすればよいですか AWS RAM？

A: セキュリティはお客様と AWS お客様の責任です。責任共有モデルでは、これをクラウドのセキュリティとクラウド内のセキュリティと定義しています。詳細については、 AWS RAM ドキュメントの「 のセキュリティ AWS RAM」を参照してください。

ベストプラクティス

- 単一障害点を回避します。VPC エンドポイントと Route 53 Resolver エンドポイントでは、高可用性のために 2 つ以上のアベイラビリティーゾーンを使用します。
- Route 53 Resolver エンドポイントを使用して VPCs 間で DNS クエリを転送しないでください。Amazon EC2 内のすべてのAmazon EC2 リゾルバー) を使用することを強くお勧めします。このリゾルバーは、レイテンシーを最小限に抑えながら、最高レベルの可用性とスケーラビリティを提供します。
- その他のベストプラクティスについては、Route 53 ドキュメントの「リゾルバーのベストプラクティス」を参照してください。

リソース

- インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする (Amazon VPC ドキュメント)
- VPC サブネットを他のアカウントと共有する (Amazon VPC ドキュメント)
- 共有可能な Amazon VPC リソース (AWS RAM ドキュメント)
- AWS Transit GatewayAWS PrivateLink と の統合 Amazon Route 53 Resolver (AWS ブログ記事)
- を使用した VPC エンドポイントの一元化 AWS Transit Gateway (AWS リファレンスアーキテクチャ)
- プライベートネットワーク経由で MGN データおよびコントロールプレーンに接続する (AWS 規範ガイダンス)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
初版発行	—	2025 年 2 月 18 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。