AWS 使用 VPC 介面端點在 上的多帳戶架構中重新託管應用程式

AWS 方案指引

AWS 方案指引: AWS 使用 VPC 介面端點在 上的多帳戶架構中重新託管應用程式

Table of Contents

AWS 使用 VPC 介面端點在 上的多帳戶架構中重新託管應用程式

Dipin Jain 和 Saurabh Shankar，Amazon Web Services

2025 年 2 月 (文件歷史記錄)

許多組織使用 AWS 從隔離或半隔離的網路環境重新託管 （提升和轉移） 應用程式至 ，包括內部部署資料中心和其他雲端或混合基礎設施AWS Transform MGN。這些隔離的網路通常不允許 MGN 網路需求中所述的公有端點的任何輸出流量。您可以使用虛擬私有雲端 (VPC) 介面端點來解決此限制，如透過私有網路連線至 MGN 資料和控制平面 AWS 的規範指引模式所述。

許多組織也使用多帳戶登陸區域 (MALZ) 架構來實現隔離、安全和每個帳戶計費優勢。若要透過安全網路對多個目標使用 MGN 來啟用lift-and-shift AWS 帳戶，您必須在每個目標中建立 VPC 介面端點 AWS 帳戶。這會增加管理這些資源的成本和複雜性。

本指南討論在多帳戶架構中集中 VPC 介面端點以重新託管應用程式的選項 AWS。這些選項可簡化架構，並降低此類使用案例的成本。

目標業務成果

本指南提供三種重新託管使用案例的解決方案。它專注於降低成本和營運開銷，並改善安全性和資源使用率。

使用案例：

- 您的應用程式會映射到不同的業務單位，而且您想要將它們遷移到相同 中的不同 AWS 目標帳戶， AWS 區域 以簡化計費和隔離。

  此案例的解決方案包括在中央 AWS 聯網帳戶中建立 VPC 端點，並使用 AWS Transit Gateway 連線到目標應用程式帳戶。
- 您想要將應用程式遷移到多個 中的不同 AWS 目標帳戶 AWS 區域 ，讓您的應用程式靠近您的使用者或促進災難復原。這是第一個使用案例的延伸。

  此案例的解決方案包括為 AWS 區域 AWS 中央聯網帳戶中的每個 建立 VPC 端點，以及使用對等傳輸閘道和 Amazon Route 53 啟用跨帳戶存取。

- 您的應用程式會映射到不同的業務單位，而且您想要將它們遷移到相同 中的不同 AWS 目標帳戶，AWS 區域 以用於計費和隔離。您也想要針對 MGN 預備使用較少VPCs，而且想要集中管理預備VPCs的路由，以降低成本和管理開銷。

  此案例的解決方案涉及使用共用預備區域子網路與 AWS Organizations 和 AWS Resource Access Manager () 共用 VPC 端點AWS RAM。

目標對象

本指南適用於為這些使用案例尋找解決方案的遷移顧問、應用程式架構師、基礎設施架構師和應用程式擁有者。

解決方案 1：在單一區域的中央聯網帳戶中建立 VPC 端點

使用案例

您的應用程式會映射到不同的業務單位，而且您想要將它們遷移到相同 中的不同 AWS 目標帳戶，AWS 區域 以用於計費和隔離。

挑戰

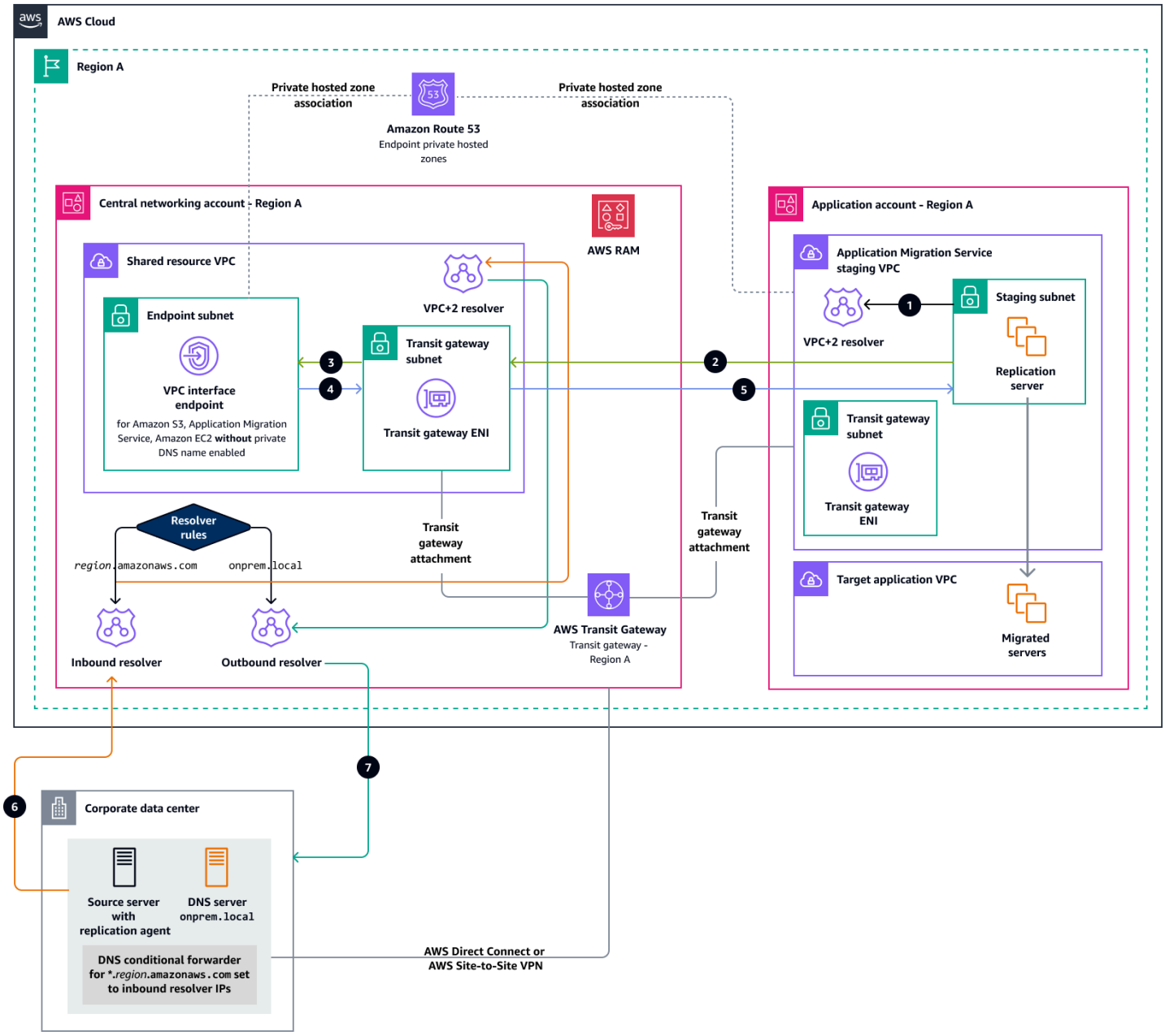
若要透過私有網路達成此目的，您必須在每個目標帳戶中建立多個 VPC 介面端點。這會增加管理開銷和維護端點的成本。（請參閱 AWS PrivateLink 定價。）

解決方案

在中央 AWS 聯網帳戶中建立 VPC 端點，並使用 Transit Gateway 連線到目標應用程式帳戶。

Architecture

下圖說明此解決方案的架構。



在圖表中，數字代表下列流量流程：

1. Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 MGN 複寫伺服器需要透過位於中央聯網帳戶 VPC 中的介面端點連線至 Amazon Simple Storage Service (Amazon S3)、MDN 或 Amazon EC2，首先需要透過查詢 VPC+2 解析程式來解析網域名稱。端點私有託管區域與相同區域中的 MGN 預備 VPC 相關聯，以完成網域解析。

> **Note**
>
> 對於與 VPC 建立關聯的每個私有託管區域，解析程式會建立規則並將其與 VPC 建立關聯。如果您將私有託管區域與多個 VPCs建立關聯，解析程式會將規則與所有 VPCs建立關聯。

2. 當執行個體知道要連線的私有 IP 時，它會將流量傳送至傳輸閘道 ENI。流量會傳送至傳輸閘道，並根據傳輸閘道路由表轉送至共用資源 VPC。
3. 共用資源 VPC 中的傳輸閘道 ENI 會將流量轉送至對應的介面端點。
4. VPC 端點會將回應傳回至傳輸閘道 ENI。
5. 流量會轉送至傳輸閘道。如傳輸閘道路由表中所指定，流量會傳送至輻式 MGN 預備 VPC。回應由傳輸閘道 ENI 傳送至目的地，也就是 EC2 執行個體或 MGN 複寫伺服器。
6. 位於公司資料中心的用戶端應用程式會以 格式解析網域名稱 `<aws_service>.<aws_region>.amazonaws.com` (例如 `mgn.us-east-1.amazonaws.com`)。它會將查詢傳送至其預先設定的 DNS 解析程式。公司資料中心的 DNS 解析程式具有轉送規則，可將`amazonaws.com`網域的任何 DNS 查詢指向 Route 53 Resolver 傳入端點。Transit Gateway 會將查詢轉送至共用資源 VPC，其會將 DNS 查詢轉送至 Route 53 Resolver 傳入端點。

   Route 53 Resolver 傳入端點使用 VPC+2 解析程式。與共用資源 VPC 相關聯的端點私有託管區域會保留 的 DNS 記錄`amazonaws.com`，因此 Route 53 Resolver 可以解析查詢。
7. Route 53 Resolver 傳出端點會將 DNS 查詢回應傳回至內部部署用戶端應用程式。

實作步驟

若要設定上圖中顯示的架構，請依照下列步驟進行：

1. 透過 AWS Direct Connect 或 將公司資料中心連線到中央聯網帳戶 AWS AWS Site-to-Site VPN。
2. 在聯網帳戶中，使用 Transit Gateway 提供 VPCs之間的連線。傳輸閘道是 AWS 帳戶 使用 在 之間共用 AWS RAM，並透過 VPC 連接進一步連接到目標應用程式帳戶預備子網路。

> **Note**
>
> 目標 AWS 帳戶 不必是同一 AWS 組織的一部分。如需詳細資訊，請參閱 AWS RAM 文件中的可共用資源。

3. 在中央網路帳戶中為 Amazon EC2、MDN 和 Amazon S3 建立 VPC 介面端點，而不啟用私有 DNS 名稱。

> **Note**
>
> 當您建立 VPC 端點至 時 AWS 服務，您可以啟用私有 DNS。啟用時，設定會為您建立受管 Route 53 私有託管區域。 此受管區域會解析 VPC 中的 DNS 名稱。不過，它無法在 VPC 外部運作。這是使用私有託管區域共用和 Route 53 Resolver 協助取得共用 VPC 端點統一名稱解析的原因。

4. 為每個端點 (MGN、Amazon EC2、Amazon S3) 建立私有託管區域。例如，對於 `us-east-1`區域中的 MGN：
   - 建立網域名稱為 的私有託管區域`mgn.us-east-1.amazonaws.com`。
   - 建立類型 A 的主機記錄，將網域名稱指向端點 IPs。
5. 建立 Route 53 Resolver 傳入和傳出規則，以促進混合 DNS 解析，並與相同 AWS 帳戶 區域中所需的 共用規則。

解決方案 2：在多個區域的中央聯網帳戶中建立 VPC 端點

使用案例

您想要將應用程式或伺服器遷移到多個不同的 AWS 目標帳戶 AWS 區域，讓它們靠近您的使用者，或在災難復原案例中實現業務連續性。這是第一個使用案例的延伸。

挑戰

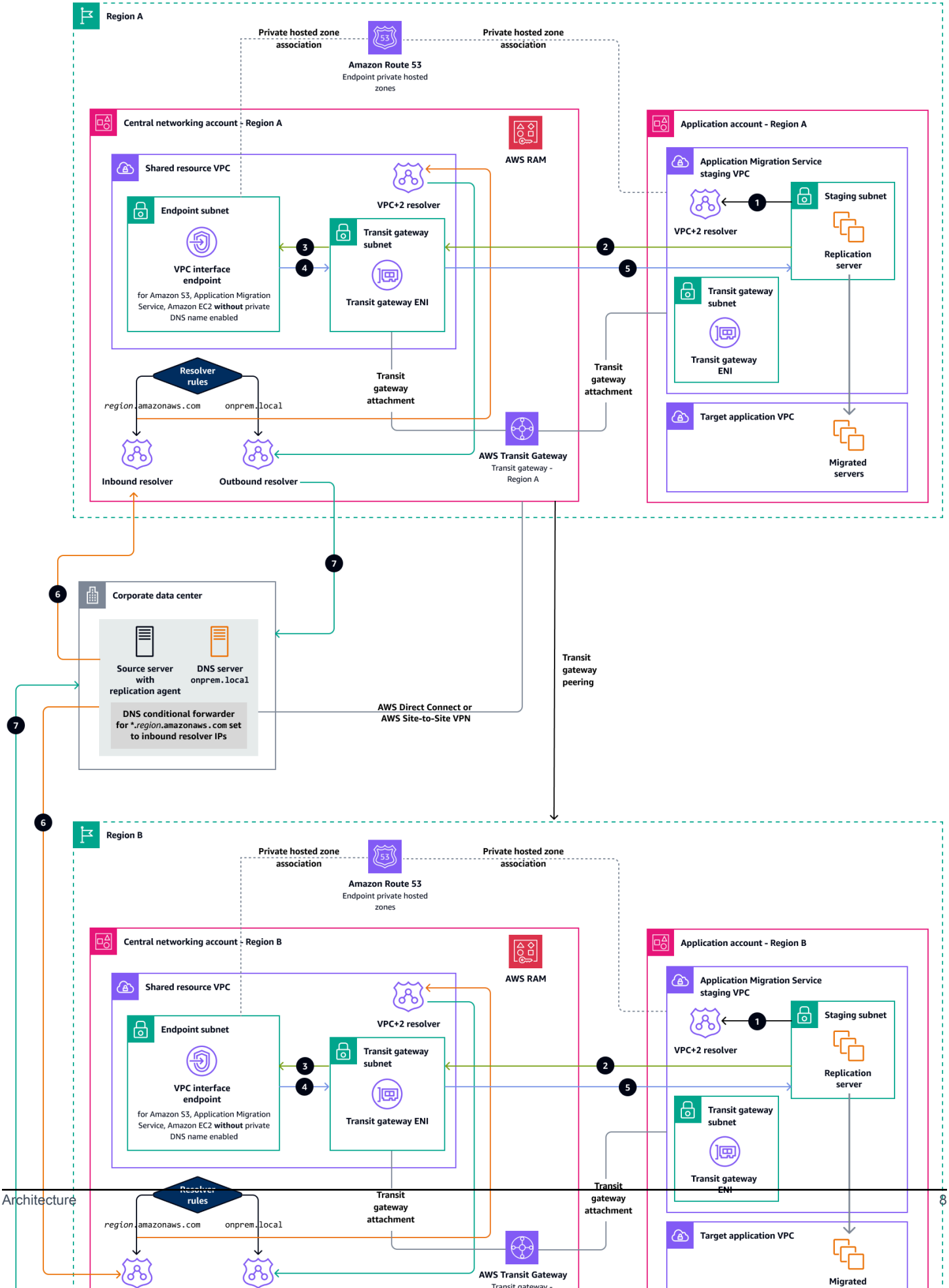
若要透過私有網路達成此目的，您必須在每個目標帳戶中建立多個 VPC 介面端點。這在多區域案例中變得更加複雜，並增加管理開銷和維護多個端點的成本。（請參閱 AWS PrivateLink 定價。）

解決方案

為中央聯網帳戶中的每個區域建立 VPC 端點，並使用對等傳輸閘道和 Route 53 啟用跨帳戶存取。

Architecture

下圖說明此解決方案的架構。


Region A
Private hosted zone association
Amazon Route 53
Endpoint private hosted zones
Private hosted zone association
Central networking account - Region A
AWS RAM
Shared resource VPC
VPC+2 resolver
Endpoint subnet
VPC interface endpoint
for Amazon S3, Application Migration Service, Amazon EC2 without private DNS name enabled
Transit gateway subnet
Transit gateway ENI
Application account - Region A
Application Migration Service staging VPC
Staging subnet
VPC+2 resolver
Replication server
Transit gateway subnet
Transit gateway ENI
Target application VPC
Migrated servers
Resolver rules
region.amazonaws.com
onprem.local
Transit gateway attachment
Transit gateway attachment
AWS Transit Gateway
Transit gateway - Region A
Inbound resolver
Outbound resolver
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
Shared resource VPC
VPC+2 resolver
Endpoint subnet
VPC interface endpoint
for Amazon S3, Application Migration Service, Amazon EC2 without private DNS name enabled
Transit gateway subnet
Transit gateway ENI
Application account - Region B
Application Migration Service staging VPC
Staging subnet
VPC+2 resolver
Replication server
Transit gateway subnet
Transit gateway ENI
Target application VPC
Migrated servers
Resolver rules
region.amazonaws.com
onprem.local
Transit gateway attachment
Transit gateway attachment
AWS Transit Gateway
Transit gateway - Region B

流量流程與解決方案 1 中的流量相同，但兩個區域中的帳戶透過傳輸閘道對等互連。

實作步驟

1. 在中央聯網帳戶中，為每個目標建立 VPC 介面端點 AWS 區域。
2. 在中央聯網帳戶中，為每個區域中的每個端點建立私有託管區域，並將該區域與相同區域中的目標應用程式 VPCs建立關聯。
3. 在中央聯網帳戶中，為每個目標區域建立傳輸閘道，並使用 與相同區域中的目標帳戶共用閘道 AWS RAM。
4. 使用傳輸閘道對等互連跨區域連接傳輸閘道，並視需要更新傳輸閘道路由表。
5. 在中央聯網帳戶中，為每個目標區域建立解析程式規則，並使用 與相同區域中的目標帳戶共用這些規則 AWS RAM。

解決方案 3：共用 VPC 介面端點

使用案例

您的應用程式會映射到不同的業務單位，而且您想要將它們遷移到相同區域中的不同 AWS 目標帳戶，以用於計費和隔離目的。

挑戰

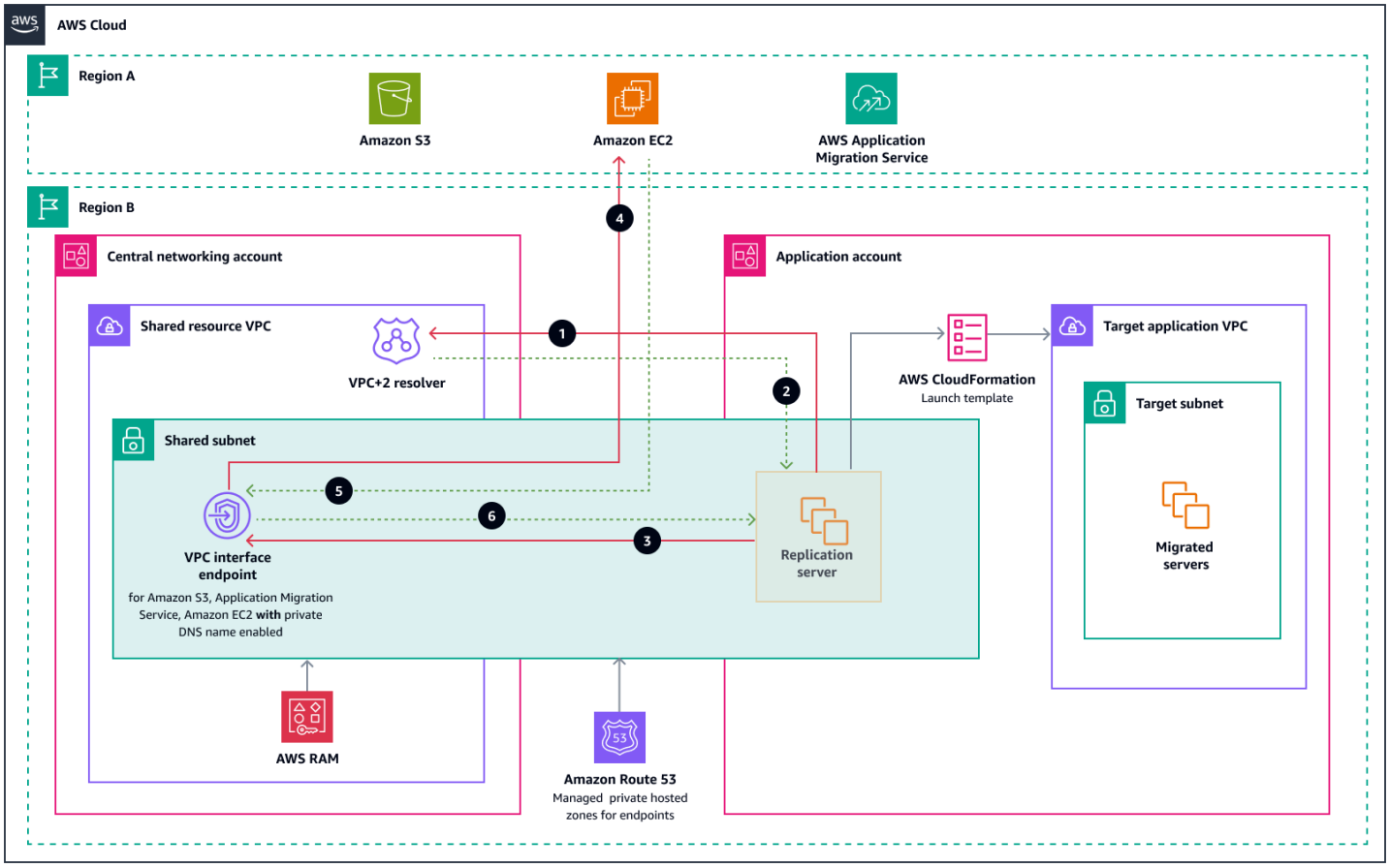
多個工作負載帳戶會增加管理開銷和每個帳戶中個別 VPC 介面端點的成本。因此，您可能想要減少 MGN VPCs，並集中管理預備 VPCs的路由，以降低成本和管理開銷。

解決方案

使用共用暫存區域子網路 AWS Organizations和 共用 VPC 端點 AWS RAM。如需 VPC 共用的詳細資訊，請參閱 Amazon VPC 文件。

Architecture

下圖說明此解決方案的架構。



圖表說明下列流量流程：

1. MGN 複寫伺服器會查詢 VPC+2 DNS，以解析 MGN、Amazon EC2 或 Amazon S3 的 API 端點。

2. VPC+2 DNS 會在受管私有託管區域的協助 AWS 下解析端點的私有 IP，並回應 MGN 複寫伺服器。

3-6. 複寫伺服器使用該 IP 透過 服務的介面端點連線至 AWS 服務 API。

實作步驟

1. 在中央聯網帳戶中，建立 MGN 的預備 VPC 和子網路。
2. 在啟用私有 DNS 名稱的情況下，建立 MGN、Amazon EC2 或 Amazon S3 的端點。這會建立 AWS 受管私有託管區域，並將其與預備 VPC 建立關聯。
3. 與相同 AWS 組織中的目標應用程式帳戶和 共用預備子網路 AWS 區域。
4. 對於 AWS 與內部部署資料中心（上圖未顯示）之間的混合連線，請使用 Transit Gateway Direct Connect 或 AWS Site-to-Site VPN Route 53 Resolver 端點，如解決方案 1 和解決方案 2 所示。

限制

- 參與者 VPCs和擁有者 VPC AWS 帳戶 的 必須是 中相同組織的一部分 AWS Organizations。
- 如需可共用資源的清單，請參閱 Amazon VPC 文件。
- 如需 VPC 共用限制，請參閱 Amazon VPC 文件。

設計考量

- 若要降低營運開銷，請建立資源一次，然後使用 AWS RAM 與其他帳戶共用該資源。這樣就不需要在每個帳戶中佈建重複的資源，並減少營運開銷。
- 使用一組政策和許可，簡化共用資源的安全管理。如果您在個別帳戶中建立重複的資源，您必須實作相同的政策和許可，並在所有帳戶中保持同步。反之，您可以透過一組政策和許可來管理共享 AWS RAM 資源的所有使用者。 AWS RAM 提供一致的經驗，讓您共享不同類型的 AWS 資源。
- 提供可見性和可稽核性。 AWS RAM 與 Amazon CloudWatch 和 整合，以檢視共用資源的使用詳細資訊 AWS CloudTrail。如需詳細資訊，請參閱 AWS RAM 文件中的AWS RAM 使用 EventBridge 監控和使用 記錄 AWS RAM API 呼叫 AWS CloudTrail。

常見問答集

問：我可以與誰共用資源？

答：您可以與任何 共用資源 AWS 帳戶。如果您是 中的組織的一部分， AWS Organizations 且已啟用組織內的共用，您也可以與組織單位 (OUs) 或整個組織共用資源。對於支援的資源類型，您也可以與 AWS Identity and Access Management (IAM) 角色和 IAM 使用者共用資源。如果您與組織外部的帳戶共用資源，這些帳戶會收到加入資源共用的邀請。他們接受邀請後，就可以開始使用共用資源。

問：與其他 共用我的資源會產生任何費用 AWS 帳戶嗎？

答：否。您可以免費共用資源。

問：我可以停止共用資源嗎？

答：是。若要停止共用資源，請將其從資源共用中移除或刪除資源共用。

問：如何確保 的安全性 AWS RAM？

答：安全是 AWS 與您之間的共同責任。共同責任模型將此描述為雲端安全性和雲端安全性。如需詳細資訊，請參閱 AWS RAM 文件中的 中的安全性 AWS RAM。

最佳實務

- 避免單點故障。對於 VPC 端點和 Route 53 Resolver 端點，請使用兩個或多個可用區域以獲得高可用性。
- 請勿使用 Route 53 Resolver 端點在 VPCs 之間轉送 DNS 查詢。我們強烈建議您使用 Amazon DNS Server (.2 解析程式） 做為 Amazon EC2 內所有執行個體的 DNS 解析程式。此解析程式提供最高層級的可用性和可擴展性，以及最低的延遲。
- 如需其他最佳實務，請參閱 Route 53 文件中的解析程式最佳實務。

Resources

- AWS 服務 使用界面 VPC 端點存取 (Amazon VPC 文件）
- 與其他帳戶共用您的 VPC 子網路 (Amazon VPC 文件）
- 可共用的 Amazon VPC 資源 (AWS RAM 文件）
- AWS Transit Gateway 與 AWS PrivateLink 和 整合 Amazon Route 53 Resolver (AWS 部落格文章）
- 使用 集中 VPC 端點 AWS Transit Gateway (AWS 參考架構）
- 透過私有網路連線至 MGN 資料和控制平面 (AWS 方案指引）

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	—	2025 年 2 月 18 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。