使用 VPC 接口终端节点在多账户架构中重新托管您的应用程序 AWS

AWS 规范性指导

AWS 规范性指导: 使用 VPC 接口终端节点在多账户架构中重新托管您的应用程序 AWS

Table of Contents

在多账户架构中重新托管您的应用程序 AWS 通过使用 VPC 接口终端节点

亚马逊 Web Services 的 Dipin Jain 和 Saurabh Shankar

2025 年 2 月（文档历史记录）

许多组织通过使用将其应用程序 AWS 从隔离或半隔离的网络环境中重新托管（提升和转移），包括本地数据中心和其他云或混合基础架构。AWS Transform MGN这些隔离的网络通常不允许向公共端点发送任何出站流量，如 MGN 网络要求中所述。您可以使用虚拟私有云 (VPC) 接口端点来解决此限制，如 AWS 规范性指导模式中所述，通过专用网络连接到 MGN 数据和控制平面。

许多组织还使用多账户 landing zone (MALZ) 架构来实现隔离、安全性和按账户计费的好处。要通过安全网络使用 MGN 实现向多个目标的迁移，您必须在每个目标 AWS 账户中创建 VPC 接口终端节点。AWS 账户这增加了管理这些资源的成本和复杂性。

本指南讨论了集中化 VPC 接口终端节点的选项，以便在上的多账户架构中重新托管您的应用程序。AWS这些选项简化了架构并降低了此类用例的成本。

目标业务成果

本指南为三个再托管用例提供了解决方案。它侧重于降低成本和运营开销，以及提高安全性和资源利用率。

使用案例：

- 您的应用程序映射到不同的业务部门，您希望将它们迁移到同一个业务部门的不同 AWS 目标账户，AWS 区域 以简化计费和隔离。

  此场景的解决方案包括在中央 AWS 网络账户中创建 VPC 终端节点 AWS Transit Gateway ，并使用连接目标应用程序账户。
- 您想将应用程序分成多个迁移到不同的 AWS 目标帐户， AWS 区域 以使应用程序与用户保持距离或便于灾难恢复。这是第一个用例的扩展。

  这种情况的解决方案包括在 AWS 中央网络账户 AWS 区域 中为每个终端节点创建 VPC 终端节点，并使用对等传输网关和 Amazon Route 53 启用跨账户访问。

- 您的应用程序映射到不同的业务部门， AWS 区域 出于计费和隔离目的，您希望将它们迁移到同一个业务部门的不同 AWS 目标账户。您还希望在 MGN 暂存中使用更少的 VPC，并希望集中管理暂存 VPC 的路由，以降低成本和管理开销。

  此场景的解决方案包括使用共享暂存区域子网共享 VPC 终端节点，使用 AWS Organizations 和 AWS Resource Access Manager (AWS RAM)。

目标受众

本指南适用于正在为这些用例寻找解决方案的迁移顾问、应用程序架构师、基础架构师和应用程序所有者。

解决方案 1：在中央网络账户中为单个区域创建 VPC 终端节点

使用案例

您的应用程序映射到不同的业务部门， AWS 区域 出于计费和隔离目的，您希望将它们迁移到同一个业务部门的不同 AWS 目标账户。

挑战

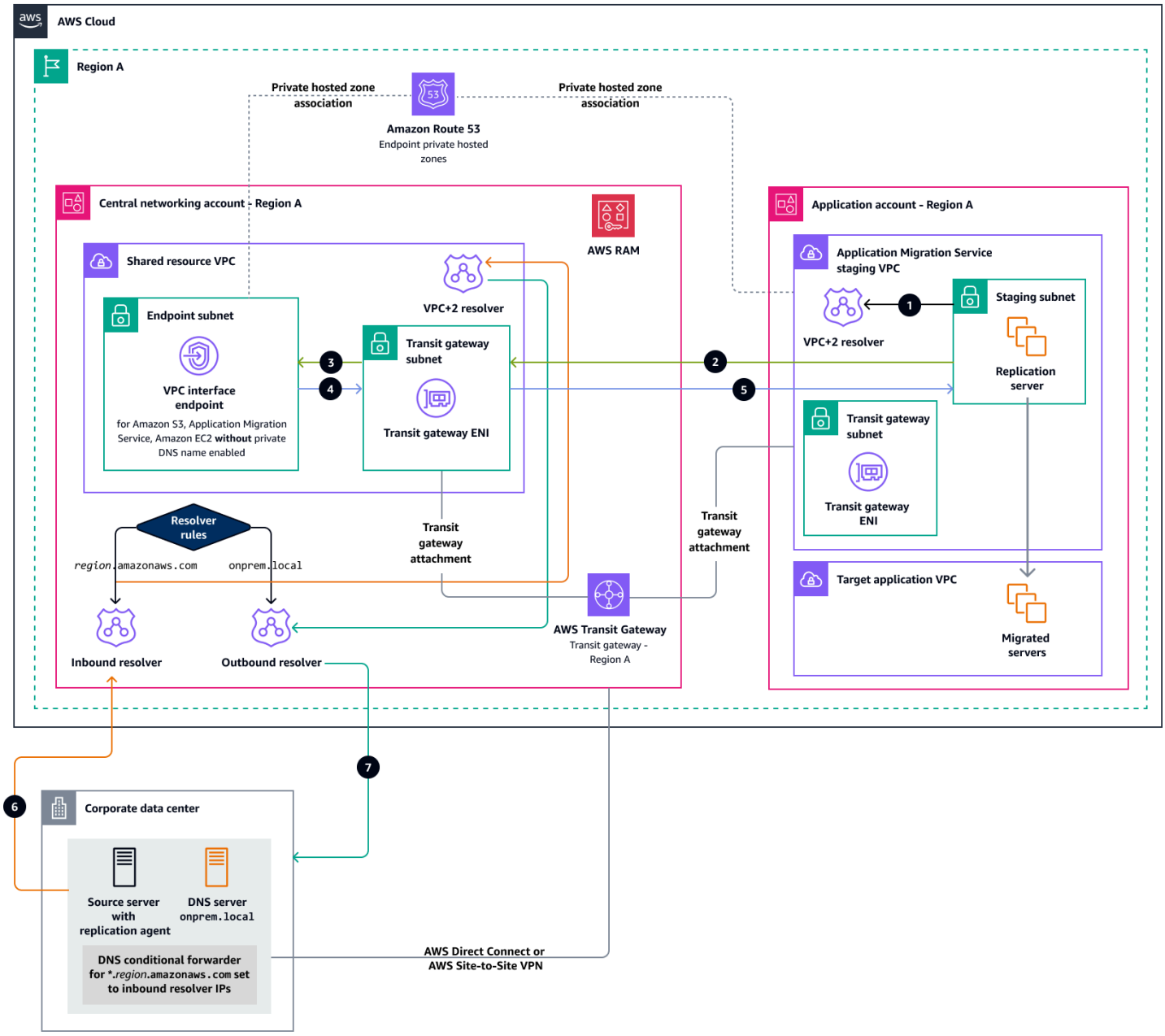
要通过私有网络实现这一目标，您必须在每个目标账户中创建多个 VPC 接口终端节点。这增加了管理开销和维护端点的成本。（参见AWS PrivateLink 定价。）

解决方案

在中央 AWS 网络账户中创建 VPC 终端节点，然后使用 Transit Gateway 连接到目标应用程序账户。

架构

下图说明了此解决方案的架构。



在图中，这些数字表示以下交通流：

1. 需要通过位于中央网络账户 VPC 中的接口终端节点连接到亚马逊简单存储服务 (Amazon S3)、MGN 或 Amazon EC2 的亚马逊弹性计算云 (Amazon EC2) 实例或 MGN 复制服务器首先需要通过查询 VPC+2 解析器来解析域名。终端节点私有托管区域与同一区域中的 MGN 暂存 VPC 关联以完成域解析。

> **Note**
>
> 对于您与 VPC 关联的每个私有托管区域，解析器都会创建一个规则并将其与 VPC 关联。如果您将私有托管区域与多个 VPC 关联，则解析器会将该规则与所有 VPC 关联。

2. 当实例知道要连接的私有 IP 时，它会将流量发送到传输网关 ENI。根据中转网关路由表，流量将发送到中转网关并转发到共享资源 VPC。
3. 共享资源 VPC 中的传输网关 ENI 将流量转发到相应的接口终端节点。
4. VPC 终端节点将响应发送回中转网关 ENI。
5. 流量被转发到中转网关。按照传输网关路由表中的指定，流量将发送到分支 MGN 分段 VPC。响应由传输网关 ENI 发送到目的地，即 EC2 实例或 MGN 复制服务器。
6. 位于公司数据中心的客户端应用程序解析表单中的域名`<aws_service>.<aws_region>.amazonaws.com`（例如，`mgn.us-east-1.amazonaws.com`）。它将查询发送到其预配置的 DNS 解析器。公司数据中心的 DNS 解析器有一个转发规则，该规则将对`amazonaws.com`域的任何 DNS 查询指向 Route 53 解析器入站终端节点。Transit Gateway 将查询转发到共享资源 VPC，后者在 Route 53 解析器入站终端节点上转发 DNS 查询。

   Route 53 解析器入站终端节点使用 VPC+2 解析器。与共享资源 VPC 关联的终端节点私有托管区域保存的 DNS 记录`amazonaws.com`，因此 Route 53 解析器可以解析查询。
7. Route 53 解析器出站终端节点将 DNS 查询响应返回到本地客户端应用程序。

实现步骤

要设置上图所示的架构，请执行以下步骤：

1. AWS 通过 AWS Direct Connect 或将您的公司数据中心连接到中央网络帐户 AWS Site-to-Site VPN。
2. 在网络账户中，使用 Transit Gateway 在 VPC 之间提供连接。传输网关 AWS 账户 由使用共享 AWS RAM，并通过 VPC 连接进一步连接到目标应用程序账户暂存子网。

> **Note**
>
> Target AWS 账户 不必是同一个 AWS 组织的一部分。有关更多信息，请参阅 AWS RAM 文档中的可共享资源。

3. 在中央网络账户中为亚马逊 EC2、MGN 和 Amazon S3 创建 VPC 接口终端节点，无需启用私有 DNS 名称。

> **Note**
>
> 在创建 VPC 终端节点时 AWS 服务，您可以启用私有 DNS。启用后，该设置将为您创建托管 Route 53 私有托管区域。 此托管区域解析 VPC 内的 DNS 名称。但是，它在 VPC 之外不起作用。这就是使用私有托管区域共享和 Route 53 解析器来帮助共享 VPC 终端节点获得统一名称解析的原因。

4. 为每个终端节点（MGN、Amazon EC2、Amazon S3）创建一个私有托管区域。例如，对于该`us-east-1`地区的 MGN：
   - 使用域名创建私有托管区域`mgn.us-east-1.amazonaws.com`。
   - 创建类型为 A 的主机记录，该记录将域名指向端点 IP。
5. 创建 Route 53 Resolver 入站和出站规则以简化混合 DNS 解析，并与同一区域 AWS 账户 的所需规则共享这些规则。

解决方案 2：在中央网络账户中为多个区域创建 VPC 终端节点

使用案例

您想将应用程序或服务器分成多个迁移到不同的 AWS 目标帐户 AWS 区域，以使它们与用户保持亲密关系，或者在灾难恢复场景中实现业务连续性。这是第一个用例的扩展。

挑战

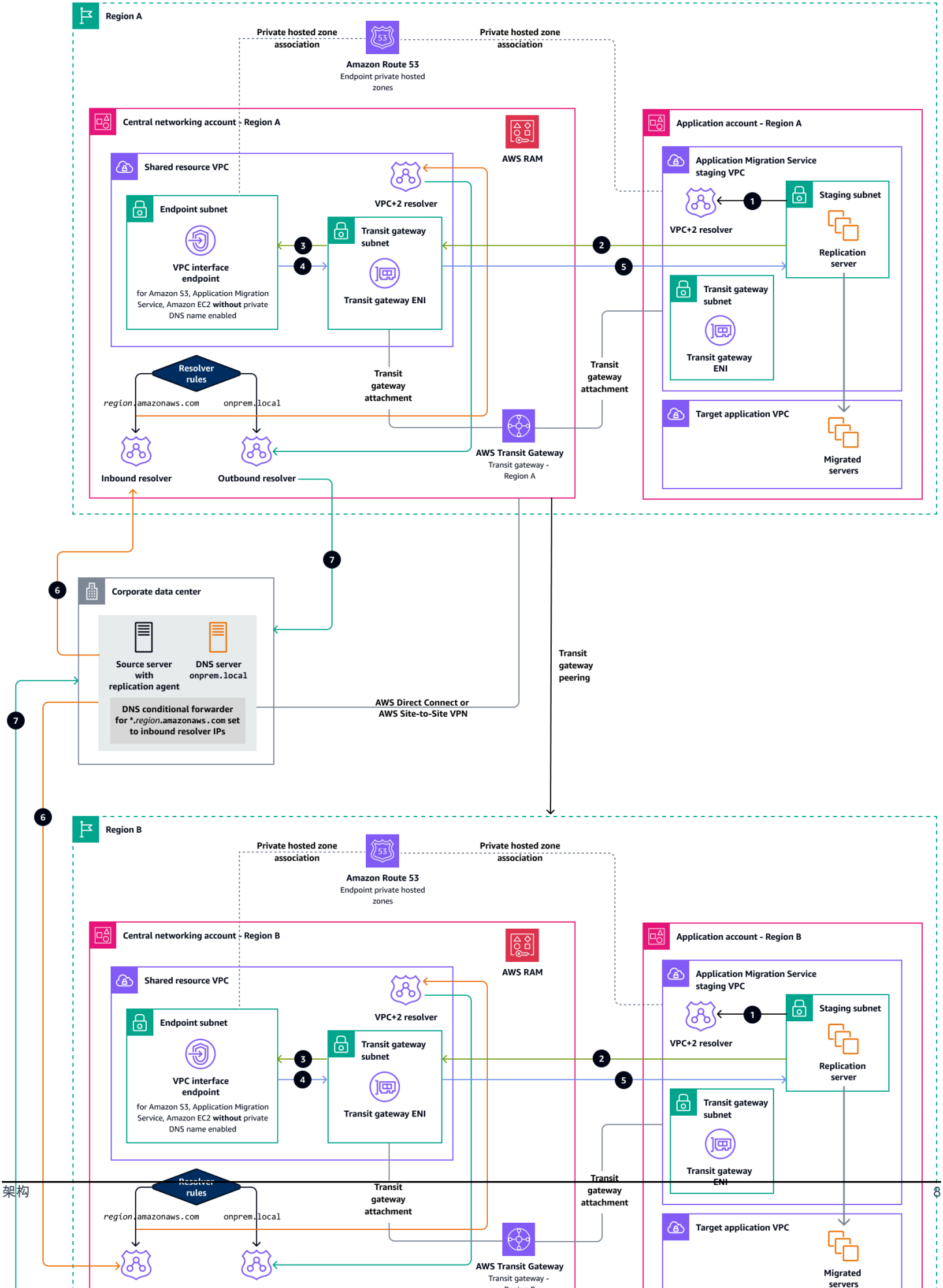
要通过私有网络实现这一目标，您必须在每个目标账户中创建多个 VPC 接口终端节点。在多区域场景中，这会变得更加复杂，并增加了维护多个端点的管理开销和成本。（参见AWS PrivateLink 定价。）

解决方案

在中央网络账户中为每个区域创建 VPC 终端节点，并使用对等传输网关和 Route 53 启用跨账户访问。

架构

下图说明了此解决方案的架构。


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
Transit gateway -
Target application VPC
Migrated servers

流量与解决方案 1 中的相同，唯一的不同是两个区域中的账户通过公交网关对等互连进行连接。

实现步骤

1. 在中央网络账户中，为每个目标创建一个 VPC 接口终端节点 AWS 区域。
2. 在中央网络账户中，为每个区域的每个终端节点创建一个私有托管区域，并将该区域与同一区域中的目标应用程序 VPC 关联。
3. 在中央网络账户中，为每个目标区域创建一个传输网关，然后使用与同一区域中的目标账户共享该网关 AWS RAM。
4. 使用中转网关对等连接跨区域的公交网关，并根据需要更新公交网关路由表。
5. 在中央网络账户中，为每个目标区域创建解析器规则，并使用 AWS RAM与同一区域的目标账户共享这些规则。

解决方案 3：共享 VPC 接口终端节点

使用案例

您的应用程序映射到不同的业务部门，出于计费和隔离目的，您希望将其迁移到同一地区的不同 AWS 目标账户。

挑战

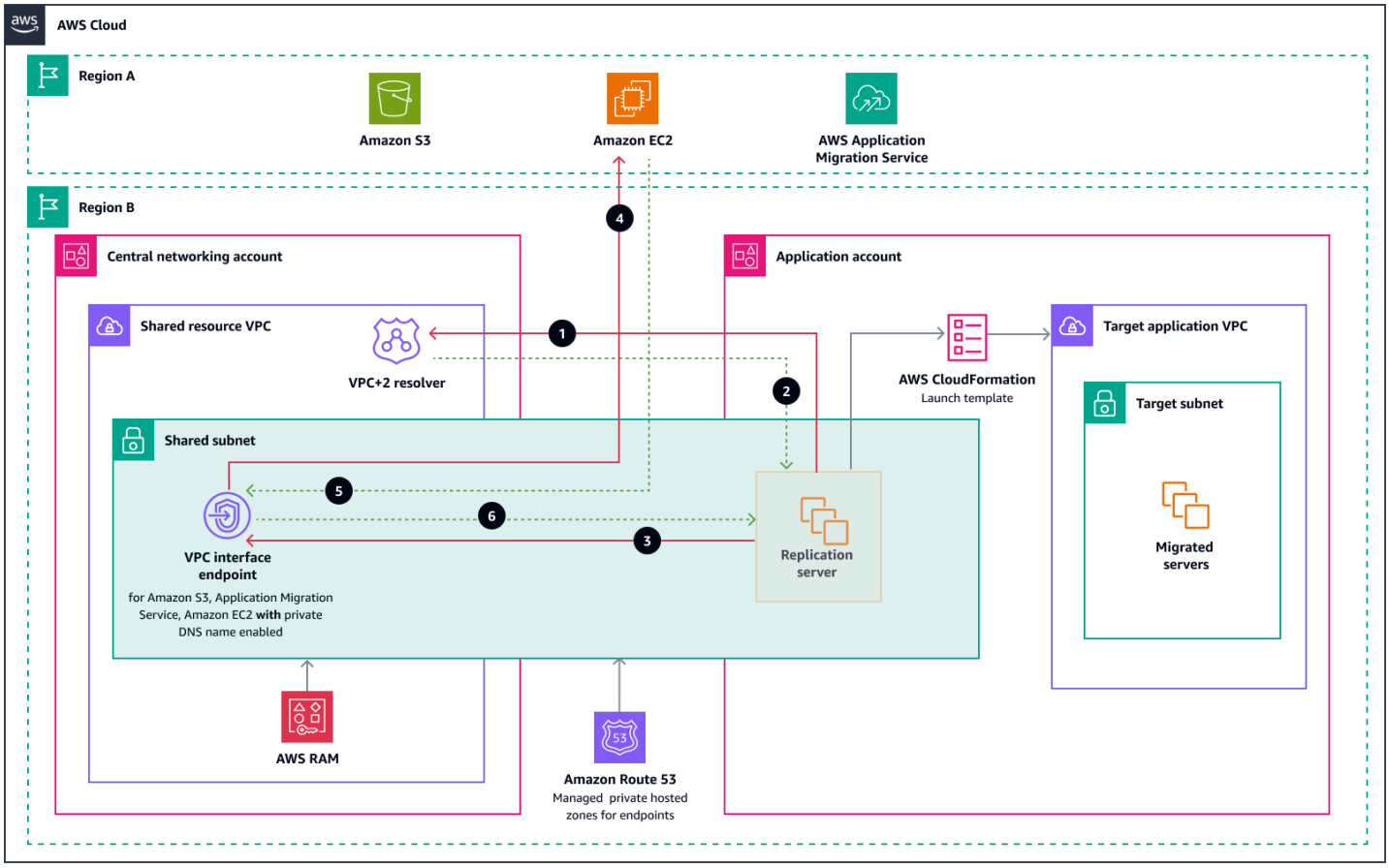
多个工作负载账户会增加每个账户中各个 VPC 接口终端节点的管理开销和成本。因此，您可能希望减少 MGN 的暂存 VPC，并集中管理暂存 VPC 的路由，以降低成本和管理开销。

解决方案

使用共享的中转区域子网共享 VPC 终端节点 AWS Organizations、和。 AWS RAM有关 VPC 共享的更多信息，请参阅 Amazon VPC 文档。

架构

下图说明了此解决方案的架构。



该图说明了以下交通流：

1. MGN 复制服务器查询 VPC+2 DNS 以解析 MGN、Amazon EC2 或 Amazon S3 的 API 终端节点。

2. VPC+2 DNS 借助托管私有 AWS 托管区域解析终端节点的私有 IP，并响应 MGN 复制服务器。

3-6。复制服务器使用该 IP 通过服务的接口端点连接到 AWS 服务 API。

实现步骤

1. 在中央网络账户中，为 MGN 创建暂存 VPC 和子网。
2. 在启用私有 DNS 名称的情况下为 MGN、Amazon EC2 或 Amazon S3 创建终端节点。这将创建一个 AWS 托管私有托管区域并将其与暂存 VPC 关联。
3. 与同一 AWS 组织中的目标应用程序帐户共享暂存子网，以及。 AWS 区域
4. 要实现与您的本地数据中心 AWS 之间的混合连接（上图中未显示），请使用 Transit Gateway，Direct Connect 或者 AWS Site-to-Site VPN 使用 Route 53 解析器终端节点，如解决方案 1 和解决方案 2 所示。

限制

- AWS 账户 对于参与者，VPC 和所有者 VPC 必须属于同一个组织。 AWS Organizations
- 有关可共享资源的列表，请参阅 Amazon VPC 文档。
- 有关 VPC 共享限制，请参阅亚马逊 VPC 文档。

设计注意事项

- 要减少运营开销，请创建一次资源，然后 AWS RAM 使用该资源与其他账户共享。这样就无需在每个账户中配置重复的资源，并减少了运营开销。
- 使用一组策略和权限，简化共享资源的安全管理。如果您在单独的账户中创建重复的资源，则必须实施相同的策略和权限，并使它们在所有账户之间保持同步。相反，您可以通过一组策略和权限来管理共享 AWS RAM 资源的所有用户。 AWS RAM 为共享不同类型的 AWS 资源提供一致的体验。
- 提供可见性和可审计性。通过与 Amazon 集成 AWS RAM ，查看共享资源的使用详情 CloudWatch ，以及 AWS CloudTrail。有关更多信息，请参阅 AWS RAM 文档 AWS CloudTrail中的AWS RAM 使用监控 EventBridge和记录 AWS RAM API 调用。

常见问题解答

问：我可以与谁共享资源？

答：您可以与任何人共享资源 AWS 账户。如果您是组织中的一员， AWS Organizations 并且启用了组织内部共享，则还可以与组织单位 (OUs) 或整个组织共享资源。对于支持的资源类型，您还可以与 AWS Identity and Access Management (IAM) 角色和 IAM 用户共享资源。如果您与组织外部的账户共享资源，则这些账户会收到加入资源共享的邀请。他们接受邀请后，就可以开始使用共享资源了。

问：与其他 AWS 账户人共享我的资源会产生任何费用吗？

答：不是。 您可以共享资源，无需支付额外费用。

问：我能否停止共享资源？

答：是的。要停止共享资源，请将其从资源共享中移除或删除该资源共享。

问：我怎样才能确保安全 AWS RAM？

答：安全是双方共同承担 AWS 的责任。责任共担模型将其描述为云的安全和云中的安全。有关更多信息，请参阅 AWS RAM 文档AWS RAM中的安全性。

最佳实践

- 避免单点故障。对于 VPC 终端节点和 Route 53 解析器终端节点，请使用两个或更多可用区以实现高可用性。
- 请勿使用 Route 53 解析器终端节点在两者之间 VPCs转发 DNS 查询。我们强烈建议您使用亚马逊 DNS 服务器（.2 解析器）作为 Amazon 内部所有实例的 DNS 解析器。 EC2该解析器以最低的延迟提供最高级别的可用性和可扩展性。
- 有关其他最佳实践，请参阅 Route 53 文档中的 Resolver 最佳实践。

资源

- AWS 服务 使用接口 VPC 终端节点（亚马逊 VPC 文档）
- 与其他账户共享您的 VPC 子网（亚马逊 VPC 文档）
- 可共享的 Amazon VPC 资源（AWS RAM 文档）
- AWS Transit Gateway 与 AWS PrivateLink 和集成 Amazon Route 53 Resolver（AWS 博客文章）
- 使用 AWS Transit Gateway（AWS 参考架构）集中化 VPC 终端节点
- 通过@@ 专用网络连接到 MGN 数据和控制平面（AWS 规范性指导）

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
初次发布	—	2025 年 2 月 18 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。