NORDIC™
Global Health and Technology Consulting

NOVEMBER 2023

VIRTUAL PRIVATE CLOUD SHARING

Resource management flexibility

AT A GLANCE

Healthcare organizations continue to realize the myriad benefits of cloud adoption. Whether dipping their toes in or jumping in with both feet, it can be challenging to separate organizational lines of businesses and workflows that could be caused by mergers and acquisitions, service expansion, or strategic partnerships. To fulfill the strategic segmentation of business units or organizations, cloud tools and advancements offer significant advantages.

Over the past several years, Amazon Web Services (AWS) has continued to make advancements to allow for the creation of necessary boundaries and their management, such as consolidated billing and AWS Organizations. To facilitate integration and minimize management overhead, AWS rolled out cross-account role delegation and virtual private cloud (VPC) sharing in 2019. Prior to that, VPCs were connected to a single account. AWS VPC sharing allows a clear separation of duties and shared efficiencies in the cloud space.

Organizations can isolate and manage different lines of business while also enabling resource sharing between them, with each line of business retaining ownership and control of its own resources, accounts, and security. Shared VPCs can be especially useful for highly interconnected needs, such as analytics platforms or applications.

WHAT THIS MEANS FOR YOU

Whether you are new to cloud adoption or continuing to expand your use of AWS, you no longer need to adhere to rigid boundaries. VPCs no longer need to be isolated to one account.

VPC BACKGROUND

VPC is AWS's highest logical network construct that allows users to launch AWS resources, such as compute instances, databases, etc., in a virtual network that the user defines. Each VPC created can be considered a complete and separate network which can then be configured for specific security needs as well as interconnectivity. Interconnecting with the user's on-premises networks or with other VPCs allows AWS VPC to extend these networks.

While each AWS account can have multiple VPCs defined, the main reason organizations create multiple AWS accounts is to allow different lines of business to incorporate their specific needs for management, billing allocation, and security.

However, creating multiple accounts and VPCs also introduces challenges such as the management of these separate accounts, connectivity, and sharing of resources across boundaries.

Over the years, AWS has continued to address these challenges with solutions that include:

- AWS Organizations - AWS Organizations allows for the central management of these multiple accounts from a central/master account. For all joined accounts, AWS Organizations can be used to centrally control access policies, billing preferences, service quotas, etc.
- Cross-account role delegation - Cross-account identity and access management (IAM) role delegation is a process of granting access to AWS resources in one account to users in another account. This can be useful for scenarios where there are multiple AWS accounts for different purposes, such as development, testing, and production. By using IAM roles, administrators can avoid creating and managing individual IAM users in each account. Instead, a trusted relationship is created between the accounts, using temporary security credentials to access the resources.
- VPC sharing - This feature allows users to share subnets from one account (VPC owner) with others (VPC participants) within the same AWS Organization. **VPC sharing can be used** to centrally manage the network configuration of shared VPCs while allowing each account to create their own resources within the shared subnets.

Up until the announcement of VPC sharing in 2019, VPCs had always been considered bound by the account, requiring separate network configurations and resources with connections to these separate networks via Transit Gateway, peering, and/or other means.

USING VPC SHARING

The only requirement for using VPC sharing is enabling resource sharing with AWS Organizations. If an organization is not currently using AWS Organizations, it's advised to consider leveraging it. There is no cost for creating one or many AWS Organizations, and there are many benefits, including security, management, and cost.

CURRENT RELEASE AND LIMITATIONS

Subnets within the shared VPC are managed by their shared participant/account owners, but the participants/account owners cannot change the attributes of the shared subnet or the shared VPC. Responsibilities and permissions for owners and their shared participants/account owners are outlined **in more detail here**. This document will be continuously updated as AWS expands supported services.

VPC SHARING BENEFITS

Sharing VPCs is useful when network isolation between teams does not need to be strictly managed by the VPC owner, but the account level users and permissions must be. With **shared VPC**, multiple AWS accounts create their application resources (such as Amazon EC2 instances) in shared, centrally managed Amazon VPCs. In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants). After a subnet is shared, the participants can view, create, modify, and delete their application resources in the subnets shared with them. Participants cannot view, modify, or delete resources that belong to other participants or the VPC owner. Security between resources in shared VPCs is managed using security groups, network access control lists (NACLs), or through a firewall between the subnets.

VPC sharing benefits:

- Simplified design – No complexity around inter-VPC connectivity
- Fewer managed VPCs
- Segregation of duties between network teams and application owners
- Better IPv4 address utilization
- Lower costs – No data transfer charges between instances belonging to different accounts within the same availability zone. For use of existing VPN, direct connections, and/or other network resources.

Possible use cases:

Healthcare organizations who have OHCA relationships or engage in growing their Community Connect and Regional Connect offerings can create subnets within a shared VPC with resources that can be shared with one or more accounts that can be invited into their AWS Organization. This allows these organizations to focus on their core offerings and the flexibility to extend their offerings/resources as needed.

With the use of shared VPCs, organizations that engage in business-to-business (B2B) lines of business or services that require a high degree of integration can go global without repeating or configuring connectivity between hundreds of VPCs and across regions.

Patterns or designs to apply shared VPCs:

Figure 1 illustrates where underlying networking resources can be created and leveraged by the subnets, as well as other resources created in subnets that can be shared with multiple accounts.

FIG. 1 *Sharing subnets with many VPC participants*

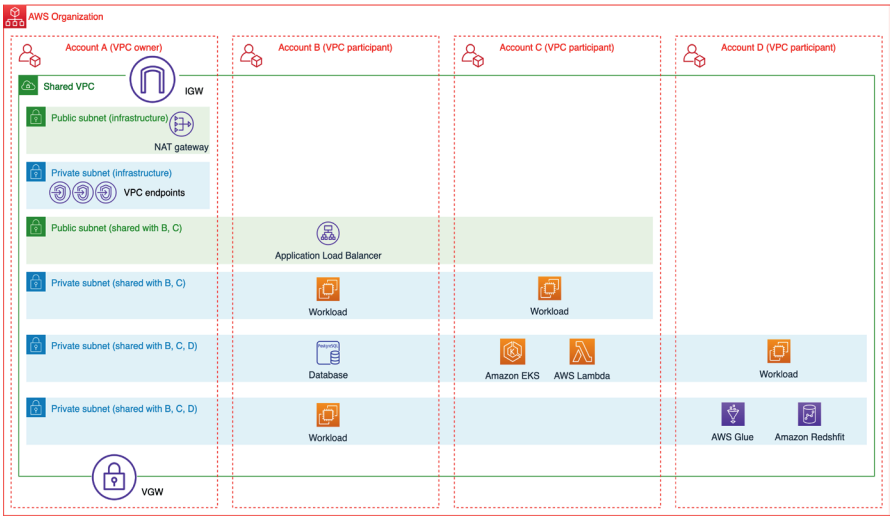
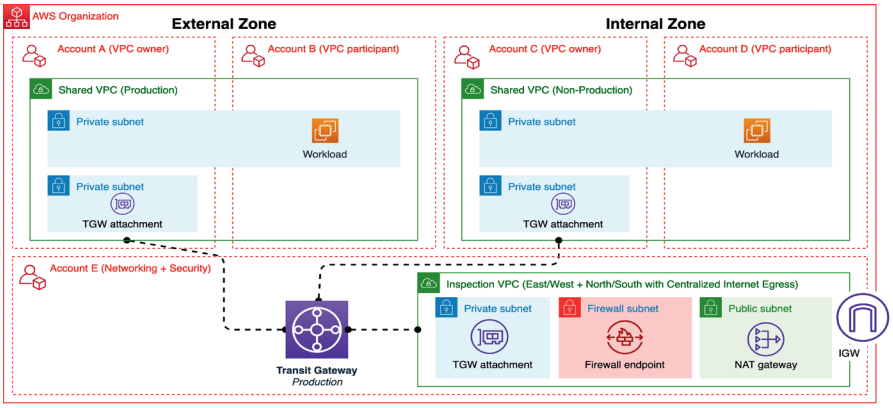


Figure 2 illustrates a central networking account where all traffic can be directed for inspection based on your organization's needs for North/South and/or East/West traffic with a centralized egress or path to the internet. The VPC owner's account is where the shared VPC is. Subnets that house workloads can be shared with other accounts or VPC participants.

FIG. 2 *Single security zone per shared VPC*



SARAVANAN SONAISAMY
Cloud Solutions Lead, Digital Health

KEVIN ERDAL
Practice Leader, Digital Health

CloudPress@NordicGlobal.com

REFERENCES

1. Amazon Web Services. (2023). *Building a scalable and secure multi-VPC AWS network infrastructure* [White paper]. **https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/amazon-vpc-sharing.html**
2. Amazon Web Services. (2023). *Responsibilities and permissions for owners and participants*. **https://docs.aws.amazon.com/vpc/latest/userguide/vpc-sharing.html#vpc-share-limitations**
3. Vaganov, E. (2021, April 16). *VPC sharing: Key considerations and best practices*. Amazon Web Services. **https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-key-considerations-and-best-practices/**
4. Shukla, H. (2020, August 6). *Understanding VPC's*. Medium. **https://medium.com/all-about-aws/understanding-vpcs-ffbebac42af**
5. Amazon Web Services. (2023). *Share your VPC with other accounts*. **https://docs.aws.amazon.com/vpc/latest/userguide/vpc-sharing.html**