## Core Components

* **On-premises network**. The private local-area network running within JPMC.
* **ExpressRoute gateway**. An ExpresssRoute circuit is used to connect the JPMC on-premises network to the Hub VNet.
* **Hub VNet**. An Azure VNet is used as the hub in the hub-spoke topology. The hub is the central point of connectivity to JPMC on-premises network, and a place to host Platform Components that can be consumed by the different workloads hosted in the spoke VNets.
* **Spoke VNets**. One or more Azure VNets that are used as spokes in the hub-spoke topology. Spokes can be used to isolate workloads in their own VNets, managed separately from other spokes. Each workload might include multiple tiers, with multiple subnets connected through Azure load balancers.
* **VNet peering**. Two VNets can be connected using a peering connection. Once peered, the VNets exchange traffic by using the Azure backbone, without the need for a router. In this hub-spoke network topology, VNet peering is used to connect the hub to each spoke. You can peer virtual networks in the same region, or different regions (Global VNet Peering).
* **Inter Spoke Communication (Routable Subnets)**. The spoke VPNs communicate with each other by forwarding their outbound traffic, using User Defined Routes (UDR) , to a Virtual Network Appliance that resides in the Hub VPN, and the Network Appliance then forwards the traffic to its final destination.
* **Platform Components** **(Shared Services) Subnet**. Platform components reside in the Hub VNet and can be shared by the spoke VNets. These are Azure resources like Azure Key Vaults, Azure Pipelines, Data Dog, Azure Automation, Private DNS and Azure Monitors

## Security Considerations

* **Extended & Common Identity**. The JPMC on-premise Active Directory Domain Services (AD DS) environment is extended to Azure using Azure AD Connect that syncs the on-premise AD DS evviroment to an Azure Active Directory Tenant
* **Hub Vnet Domain Controller for Fine Grained Azure Policy**. For Group Policy Objects that need to be controlled separately for Azure and JPMC on-premises environment, there is a Domain Controller in the Hub Vnet.
* **Jump Box**. In case connectivity to the JPMC on-premise network is lost, the Jump Box, which will be the single point of access, will be used to manage the assets in the subscription.
* **Azure Key Vault**. Is used for storage of protected secrets.

## Availability Considerations

* **Domain Controller in Azure Hub Vnet for Outages**. AD Domain Controllers in an availability set will be deployed to the Azure Hub VNet. This will treat the Azure VNet as a stand alone site, and in the event that connectivity is lost to the on-premise site, the authentication and authorization will be local, and will still work.
* **Availability Sets**. Azure Domain Controllers and Network Appliances will be placed in availability sets for high availability.