Azure Services - In-Depth Interview Preparation Notes

1. Virtual Network (VNet)

- **Definition**: Azure Virtual Network (VNet) is your private network in Azure, allowing communication between Azure resources like virtual machines, databases, and services in a secure, isolated manner.
- **Key Features**:
    - **Subnets**: Divide the network into smaller segments, improving organization and security.
    - **Routing**: Control traffic flow between subnets, VNets, and the internet.
    - **Security**: Use Network Security Groups (NSGs) to allow or deny traffic.
- **Use Case**: Connecting on-premises environments to Azure, securely isolating applications within subnets.

2. Subnets

- **Definition**: Subnets are logical subdivisions of a virtual network, where each subnet can be assigned its own IP address range.
- **Key Features**:
    - **Network Segmentation**: Helps manage traffic efficiently by segregating parts of the VNet.
    - **Security Rules**: You can apply different NSGs to subnets to control traffic.
- **Use Case**: Placing front-end and back-end resources in separate subnets to improve security.

3. Network Security Group (NSG)

- **Definition**: NSG is a security layer used to control inbound and outbound traffic at the subnet or network interface level in a VNet.
- **Key Features**:
    - **Security Rules**: Define inbound and outbound rules to control access.
    - **Layer of Protection**: Can be applied to VMs or subnets for greater security.
- **Use Case**: Protecting your web servers from unauthorized access while allowing traffic from specific IPs or ports.

4. Azure Bastion

- **Definition**: A fully managed service that provides secure and seamless RDP and SSH connectivity to your virtual machines directly through the Azure portal without exposing VMs to public IPs.
- **Key Features**:

    - **Secure Access**: No need for public IP on VMs, reducing attack surface.
    - **Direct Portal Access**: Connect to VMs right from the Azure portal.
- **Use Case**: Securely managing your virtual machines in Azure without worrying about direct exposure to the internet.

5. Azure Firewall

- **Definition**: A cloud-based, scalable, and fully managed network security service that provides both inbound and outbound traffic protection for your VNet.
- **Key Features**:
    - **Threat Detection**: Provides built-in threat intelligence.
    - **Application Rules**: Allows or denies traffic based on FQDN.
    - **Network Rules**: Controls inbound and outbound network traffic.
- **Use Case**: Use Azure Firewall to control traffic between different subnets and VNets while ensuring security for cloud-based workloads.

6. VPN Gateway

- **Definition**: Provides secure connectivity between your on-premises network and Azure VNets through IPsec/IKE VPN tunnels.
- **Key Features**:
    - **Point-to-Site**: For individual users to connect securely.
    - **Site-to-Site**: For connecting entire on-premises networks.
    - **VNet-to-VNet**: Securely connects different Azure VNets.
- **Use Case**: Extending your on-premises data center to Azure for hybrid cloud deployments.

7. Azure Kubernetes Service (AKS)

- **Definition**: A managed Kubernetes service that automates the deployment, scaling, and management of containerized applications.
- **Key Features**:
    - **Auto-scaling**: Automatically scale applications based on load.
    - **Managed Kubernetes**: Reduces the operational overhead of running Kubernetes.
    - **Integration**: Easily integrates with Azure services like Azure Monitor, Log Analytics.
- **Use Case**: Deploy containerized applications using Kubernetes while leveraging Azure's security and monitoring features.

8. Application Gateway

- **Definition**: A web traffic load balancer that enables you to manage traffic to your web applications and provides advanced routing features, including SSL termination.
- **Key Features**:
    - **Web Application Firewall (WAF)**: Provides protection against common web vulnerabilities.
    - **SSL Termination**: Offload SSL decryption to reduce load on application servers.
    - **Path-Based Routing**: Route traffic based on URLs.
- **Use Case**: Ensuring that your web applications are protected, load-balanced, and scalable.

9. Azure Front Door

- **Definition**: A global, scalable entry point for web applications, designed for high availability, fast delivery, and security.
- **Key Features**:
    - **Global Load Balancing**: Distributes traffic across multiple regions.
    - **SSL Offloading**: Handle SSL at the edge to reduce the load on backend services.
    - **DDoS Protection**: Automatically provides DDoS protection for your applications.
- **Use Case**: High-performance, globally distributed web applications that need fast delivery with built-in security.

10. Azure Storage Accounts

- **Definition**: Azure Storage provides scalable cloud storage for data objects such as blobs, files, queues, and tables.
- **Key Features**:
    - **Blob Storage**: Stores unstructured data like images and videos.
    - **File Storage**: Provides fully managed file shares.
    - **Replication**: Options include locally-redundant, zone-redundant, geo-redundant, etc.
- **Use Case**: Storing large amounts of unstructured data or providing shared file access to multiple users.

11. Azure Key Vault

- **Definition**: A cloud service for securely storing and accessing secrets, encryption keys, and certificates.
- **Key Features**:
    - **Secret Management**: Store and manage sensitive data like passwords.

    - **Key Management**: Generate and manage encryption keys.
    - **Audit Logs**: Monitor who is accessing your keys and secrets.
- **Use Case**: Storing API keys and database credentials securely in cloud-native applications.

12. Azure Monitor

- **Definition**: A full-stack monitoring solution that provides insights into the performance and health of your applications and infrastructure.
- **Key Features**:
    - **Metrics and Logs**: Collect and analyze data from your resources.
    - **Alerts**: Automatically notify you of issues.
    - **Auto-Healing**: Create automated remediation workflows.
- **Use Case**: Monitoring the performance of cloud applications and automatically responding to performance degradation.

13. Azure App Services

- **Definition**: A fully managed platform for building, deploying, and scaling web apps and APIs.
- **Key Features**:
    - **Multiple Languages**: Supports .NET, Java, Node.js, PHP, Python.
    - **Automatic Scaling**: Scale your application based on demand.
    - **DevOps Integration**: Easily integrate with CI/CD pipelines.
- **Use Case**: Quickly deploying scalable web applications without managing infrastructure.

14. Azure Active Directory (Azure AD)

- **Definition**: A cloud-based identity and access management service that helps your employees sign in and access resources.
- **Key Features**:
    - **Single Sign-On (SSO)**: Users can access all applications with one set of credentials.
    - **Multi-Factor Authentication (MFA)**: Adds an extra layer of security.
    - **Conditional Access**: Define policies for granting access to applications.
- **Use Case**: Managing employee access to applications securely using identity management.

15. Azure Sentinel

- **Definition**: A cloud-native Security Information and Event Management (SIEM) tool for detecting, investigating, and responding to security threats.

- **Key Features**:
    - **Threat Detection**: Uses AI to detect threats quickly.
    - **Automated Response**: Automate threat responses with playbooks.
    - **Integrations**: Integrates with various security tools like firewalls, antivirus solutions.
- **Use Case**: Real-time threat detection and response for enterprise environments.

16. Azure Backup Vaults

- **Definition**: Secure, scalable backup solutions for Azure VMs, SQL databases, and other Azure services.
- **Key Features**:
    - **Automated Backups**: Schedule regular backups with minimal management.
    - **Data Encryption**: Protect your backup data with encryption.
    - **Cost-Effective**: Pay only for what you store, making it a budget-friendly backup option.
- **Use Case**: Ensuring that critical data is backed up regularly with easy recovery options.

17. Azure Container Registry

- **Definition**: A managed, private Docker registry for storing and managing container images.
- **Key Features**:
    - **Integration with AKS**: Simplifies deploying containerized apps.
    - **Geo-Replication**: Ensures availability of images across regions.
    - **Security**: Integrated with Azure AD for role-based access control (RBAC).
- **Use Case**: Storing container images securely and deploying them to Kubernetes.

18. Azure Migrate

- **Definition**: A centralized hub for assessing and migrating on-premises infrastructure to Azure.
- **Key Features**:
    - **Assessment Tools**: Evaluate readiness for migration.
    - **Migration Tools**: Helps move applications, databases, and VMs to Azure.
    - **Hybrid Support**: Works with multi-cloud and on-premise environments.
- **Use Case**: Migrating legacy applications and infrastructure to the cloud.

19. Azure Automation

- **Definition**: A service that automates repetitive tasks and orchestrates frequent actions like scaling, patch management, and compliance.
- **Key Features**:
    - **Runbooks**: Automate tasks using PowerShell or Python scripts.
    - **Desired State Configuration (DSC)**: Ensure systems remain in a desired state.
    - **Scheduling**: Automate jobs on a schedule.
- **Use Case**: Automating cloud management tasks such as stopping/starting VMs or patching systems.

20. ExpressRoute

- **Definition**: A private connection between Azure data centers and on-premise infrastructure, offering better reliability, speed, and lower latency than VPN.
- **Key Features**:
    - **Private Connectivity**: Avoids the public internet for improved security.
    - **High Performance**: Faster and more reliable than traditional VPNs.
    - **Dedicated Bandwidth**: Ensure predictable and high-speed connections.
- **Use Case**: Connecting on-premises datacenters to Azure for a hybrid cloud approach, ensuring secure and reliable connectivity.

21. Azure Policy

- **Definition**: A governance service that allows you to enforce rules and standards on Azure resources.
- **Key Features**:
    - **Policy Definitions**: Apply rules to ensure compliance with organizational standards.
    - **Initiatives**: Group multiple policies into a single unit for easy management.
    - **Auditing**: Monitor compliance and automatically enforce policies.
- **Use Case**: Ensuring all resources comply with corporate security, cost, and management policies.

22. Azure Arc

- **Definition**: A service that allows you to manage resources across on-premises, multi-cloud, and edge environments using Azure management tools.
- **Key Features**:
    - **Unified Management**: Centralized control over your hybrid cloud environments.

    - **Kubernetes Support**: Manage Kubernetes clusters running anywhere.
    - **Security Integration**: Extend Azure security to your hybrid resources.
- **Use Case**: Managing on-premises or multi-cloud resources like Azure resources, ensuring a consistent management and governance approach.

23. DNS Zones

- **Definition**: Azure DNS zones allow you to host your domain names in Azure, managing DNS records using the same credentials, billing, and support as other Azure services.
- **Key Features**:
    - **Managed DNS**: Simplifies DNS management and ensures high availability.
    - **DNS Record Types**: Supports common DNS records (A, CNAME, MX, etc.).
    - **Global Distribution**: Leverages Azure's global infrastructure for fast DNS responses.
- **Use Case**: Hosting your domain names on Azure for fast, reliable DNS management.
