Azure Fundamental Assignment 4

(Durgesh Kumar Shukla)

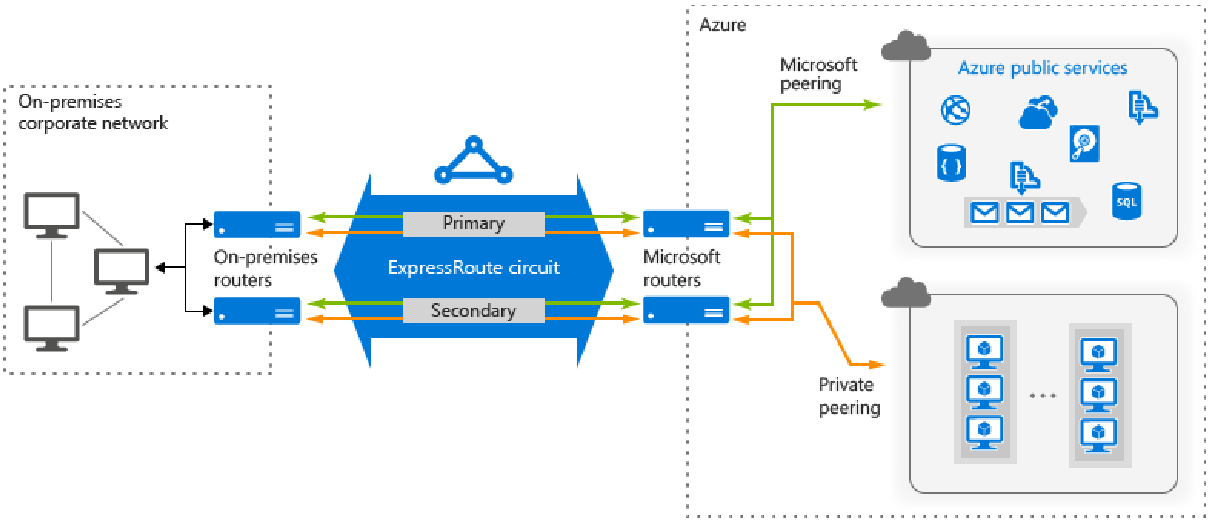
1. List Features and benefits of ExpressRoute.
2. Explain Azure storage account, disc storage and blob storage.
3. List and describe database services that are available on Microsoft Azure.
4. What is the Azure security center?
5. How to detect and respond to security in Azure.
6. What is the Azure key vault? Write its features and advantages.

Question 1.List Features and benefits of ExpressRoute.

Answer:

Express Route

Express route allows a private connection between the local network and the Microsoft cloud. Using express route organisations /users can connect to several Microsoft cloud services (cloud products e.g. Microsoft dynamics 365, Microsoft Azure and Office 365).



Features of Express Route

1.Layer 3 connectivity-Microsoft uses BGP, an industry standard dynamic routing protocol, to exchange routes between your on-premises network, your instances in Azure, and Microsoft public addresses. Establish multiple BGP sessions with your network for different traffic profiles

2.Redundancy-Each Express Route connection includes two Microsoft Enterprise Edge and two-router connections in between the connectivity provider and the local network perimeter. Microsoft ensures there's a BGP connection between the connectivity and the edge of the on-premise network one each allocated for the MSEE router. For the validation of the SLA, there must be a redundant layer 3 configured.

3.Microsoft Cloud services connectivity-Express route enables someone to access the following cloud services:Microsoft Office 365 services, Microsoft Azure services and Microsoft Dynamics 365.

4.Connectivity to all regions of the world-Through the use of Azure express route, organisations can connect to Microsoft in one location and access all services of Microsoft cloud in the whole world.
5.Global connectivity with premium ExpressRoute add-on-You are able to permit the high-quality ExpressRoute add-on feature in order to extend connectivity beyond geopolitical boundaries.
6.Local connectivity with ExpressRoute Local-Transfer data cost-effectively by enabling the Local SKU. With Local SKU, you can bring your data to an ExpressRoute location near the Azure region you want.
7. Across on-premises connectivity with ExpressRoute Global Reach-Can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits.

Benefits of Express Route

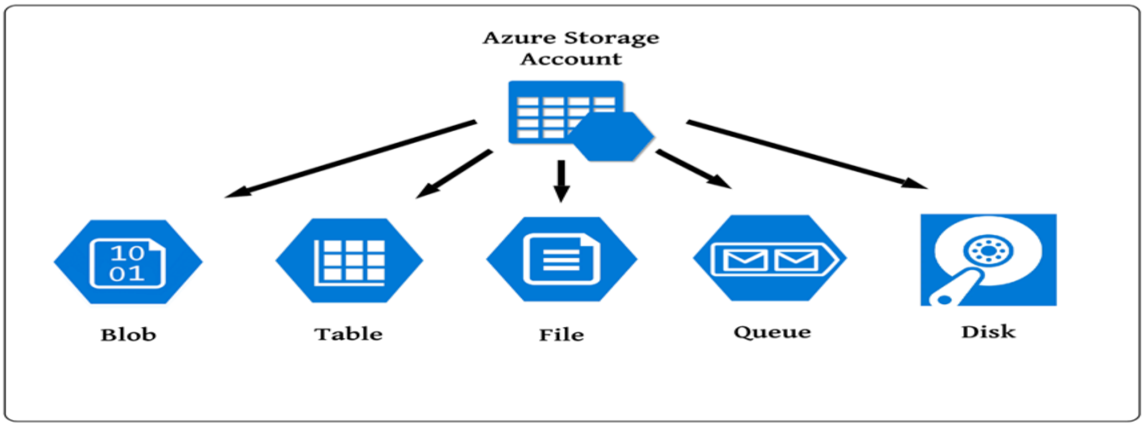
- Express route allows organisations to connect to Microsoft cloud services anywhere in the world.
- Express route provides layer 3 connection between the Azure cloud and the local network.
- Express route increases reliability due to the built-in redundancy.
- Express route improves security and privacy by avoiding sensitive traffic going over the public internet.
- Dynamic routing between your network and Microsoft via BGP.
- Connection uptime SLA.
- QoS support for Skype for Business.

Question 2. Explain Azure storage account, disc storage and blob storage.
Answer:
Azure Storage Account
An Azure storage account contains all of your Azure Storage data objects, including blobs, file shares, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. Data in your storage account is durable and highly available, secure, and massively scalable.

On a broad level, the Azure storage account falls under two bucks -
1.One which is developed with file storage, keeping communication in mind, as it can be accessed by REST API.
2.The second is designed, keeping Virtual Machines (VM) in mind.
Typically there are five different types of storage:

- Queue
- Table
- Blob
- File
- Disk.

Azure Storage allows users to replicate data within the same data centres or inside a data centre located in another zone.



Blob Storage

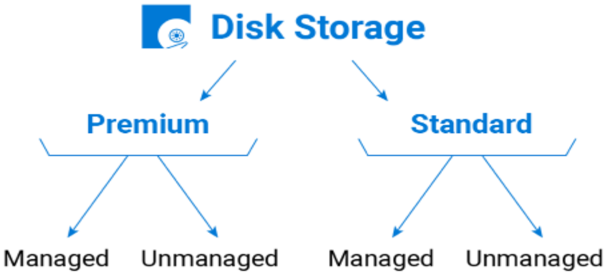
BLOB is an acronym and means Binary Large Object. Blob storage is for unstructured files, such as images, video, music files, backup files, etc. Blobs are stored in a directory-like structure called a "container".

There are three different ways to store Blobs in Microsoft Azure:
Block Blob- good for file storage
Append Blob-good for logs or metadata
Page Blob- designed for storing disk

Disk Storage

Microsoft Azure Disk Storage is based on Page Blobs. It is a service that allows you to create disks for your virtual machines. A disk created in Disk Storage can be accessed from only one virtual machine. In other words - it is your local drive.
Here you can have two options for the speed of your disks:
HDDs that are cheap but slow and called standard storage.
SSDs that are fast but expensive and called premium storage.

And two options for disk management:
Unmanaged disk - you should manage the disk storage and corresponding account yourself
Managed disk - Azure does everything for you. You need to select only the size of the disk and the desired type - standard or premium



Question 3.List and describe database services that are available on Microsoft Azure.
Answer: Azure offers a choice of fully managed relational, NoSQL and in-memory databases, spanning proprietary and open-source engines, to fit the needs of modern app developers. Infrastructure management—including scalability, availability and security—is automated, saving you time and money.

Azure SQL Database-Managed, intelligent SQL in the cloud .
Azure SQL Managed Instance -Managed, always up-to-date SQL instance in the cloud.
SQL Server on Virtual Machines-Migrate your SQL workloads to Azure while maintaining. complete SQL Server compatibility and operating system-level access.
Azure Database for PostgreSQL-Build scalable, secure and fully managed enterprise-ready apps on open-source PostgreSQL, scale out single-node PostgreSQL with high performance or migrate PostgreSQL and Oracle workloads to the cloud.
Azure Database for MySQL -Deliver high availability and elastic scaling to open-source mobile and web apps with a managed community MySQL database service or migrate MySQL workloads to the cloud.
Azure Database for MariaDB-Deliver high availability and elastic scaling to open-source mobile and web apps with a managed community MariaDB database service.
Azure Cosmos DB -Build applications with guaranteed low latency and high availability anywhere, at any scale or migrate Cassandra, MongoDB and other NoSQL workloads to the cloud.
Azure Cache for Redis -Power fast, scalable applications with an open-source-compatible in-memory data store.
Azure Managed Instance -Modernise existing Cassandra data clusters and apps and enjoy flexibility and freedom with managed instance service.

Question 4.What is the Azure security center?
Answer:
Azure Security Centre (*Azure Security Center and Azure Defender are now called Microsoft Defender for Cloud)
Note:Azure Security Center is an advanced, unified security management platform that Microsoft offers all Azure subscribers. Features of the standard offering include security health monitoring for both cloud and on-premises workloads; security threat blocking through access and app controls; adjustable security policies for maintaining regulatory and standards compliance; security vulnerability discovery tools and patches; and advanced threat detection through security alerts and analytics.

Question 5.How to detect and respond to security in Azure.
Answer:
Azure features & resources that help you protect, detect, and respond to security
Azure native security capabilities that organizations can leverage to defeat ransomware attack techniques found in both high-volume, everyday attacks, and sophisticated targeted attacks.
Native Threat Detection: Microsoft Defender for Cloud provides high-0quality threat detection and response capabilities, also called Extended **Detection and Response (XDR).**

This helps you:
Avoid wasting time and talent of scarce security resources to build custom alerts using raw activity logs.Ensure effective security monitoring, which often enables security teams to rapidly approve use of Azure services.
Password-less and Multi-factor authentication: Azure Active Directory MFA, Azure AD Authenticator App, and Windows Hello provide these capabilities. This helps protect accounts against commonly seen password attacks (which account for 99.9% of the volume of identity attacks we see in Azure AD). While no security is perfect, eliminating password-only attack vectors dramatically lowers the ransomware attack risk to Azure resources.
Native Firewall and Network Security: Microsoft built native DDoS attack mitigations, Firewall, Web Application Firewall, and many other controls into Azure. These security 'as a service' help simplify the configuration and implementation of security controls. These give organizations the choice of using native services or virtual appliances versions of familiar vendor capabilities to simplify their Azure security.

Question 6. What is the Azure key vault? Write its features and advantages.
Answer:
Azure Kay Vaults
Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed hardware security module(HSM) pools. Vaults support storing software and HSM-backed keys, secrets, and certificate.

Azure Key Vault Features
Secrets Management - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
Key Management - Azure Key Vault can be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data**.**
Certificate Management - Azure Key Vault lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.
Azure Vault Advantages
Centralize application secrets-Centralizing storage of application secrets in Azure Key Vault allows you to control their distribution. Key Vault greatly reduces the chances that secrets may be accidentally leaked.
Securely store secrets and keys-Access to a key vault requires proper authentication and authorization before a caller (user or application) can get access. Authentication establishes the identity of the caller, while authorization determines the operations that they are allowed to perform.
Monitor access and use-Once you have created a couple of Key Vaults, you will want to monitor how and when your keys and secrets are being accessed. You can monitor activity by enabling logging for your vaults. You can configure Azure Key Vault to:

- Archive to a storage account.
- Stream to an event hub.
- Send the logs to Azure Monitor logs.

*End of the page.