**Azure fundamental assignment 4**

1. *List Features and benefits of ExpressRoute.*

Microsoft Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.

Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility. ExpressRoute connections do not go over the public Internet. This lets ExpressRoute connections offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet. This is beneficial when connection speed and reliability is required for your Azure asset or entire Azure infrastructure. You can create a connection between your on-premises network and the Microsoft cloud in three different ways, Cloud Exchange Co-location, Point-to-point Ethernet Connection, and Any-to-any (IPVPN) Connection.

Key benefits:

* Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
* Connectivity to Microsoft cloud services across all regions in the geopolitical region.
* Global connectivity to Microsoft services across all regions with ExpressRoute premium add-on.
* Dynamic routing between your network and Microsoft over industry standard protocols (BGP).
* Built-in redundancy in every peering location for higher reliability.
* Connection uptime SLA.
* QoS support for Skype for Business.

1. *Explain Azure storage account, disc storage and blob storage.*

Microsoft Azure Cloud offers several types of scalable and with high-availability storage. There are five storage types available in Microsoft Azure divided into two groups.

The first group, which includes Queue Storage, Table Storage, and Blob Storage is designed with file storage, scalability, and communication in mind and is accessible via REST API. The other, which includes File Storage and Disk Storage, is for extending the capabilities of the Microsoft Azure Virtual Machine environment and for access exclusively from VMs.

**Azure storage account** is a container that bands a set of Azure Storage services together. Only data services from Azure Storage can be comprised in a storage account. Integrating data services into a storage account allows the user to manage them as a group. The settings specified while creating the account, or setting that is changed after creation, is applicable everywhere. Once the storage account gets deleted, all the data stored inside gets removed.

**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. Yes, it’s that simple.

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

**Azure Blob Storage**

Azure Blob storage is an object storage solution designed for the cloud. Blob storage gets augmented for storing a massive amount of unstructured data. Unstructured data is data that does not stick to a specific data model or definition, like text or binary data. Blob storage objects can be accessed by the user or client application via HTTP/HTTPS from any part of the world. Azure Storage Rest API, Azure PowerShell, Azure CLI, or an Azure Storage client library is used to access Blob Storage objects. There are three different ways to store Blobs in Microsoft Azure:

* Block Blob - Good for file storage, capable of 4.77 TB per file
* Append Blobs -Good for storing logs or meta-data, can be updated constantly
* Page Blobs - Designed for storing disks

1. *List and describe database services that are available on Microsoft Azure.*

Microsoft Azure offers various services as part of its fully managed services and one of the basic and fundamental building blocks is Azure SQL databases as Azure offers various SQL servers and traditional SQL database tools to make it simple, guide, and automate the database migration using a simple click from Azure portal. Using various database services from the azure users can easily deploy one or more databases to virtual machines or applications as part of its shared elastic pools. Azure database services can migrate the different datasets, schema, and objects from the various sources to the cloud easily.

Azure offers various services to migrate the data from different sources or on-premises SQL server data to the cloud. Database services offer different services tiers and compute size based on the data and have dynamic scalability.

1. **Azure Database Migration Service**

It is a fully managed service that is used for seamless migration from various database sources and on-premises SQL servers to the Azure data platform with fewer user interactions and optimized time with online integration. This service is also used for different existing Azure tools and services to give customers high availability. This service has a premium pricing tier based on this managed instance.

2. **SQL Server Stretch Database Service**

Azure uses the Stretch database to migrate the cold or infrequently accessed data to Azure cloud, It is used to replicate data transparently and securely to the cloud. Stretch database is cost-effective to transfer data and does not require many changes to queries or application whether data is stretched to the cloud or is on on-premises machines. If some data is stored in the specific tables, then the user can migrate the entire table and also it has a filter condition based on data the user can filter out hot and cold data and migrate selected rows only.

3. **SQL Data Sync Service**

It is based on the sync group and SQL data sync service is built on Azure SQL database service and can be used to synchronize the data bi-directionally across various databases both in the cloud or the on-premises machines. To synchronize the data, it uses the hub and spoke topology and hub database is always an Azure SQL database.

4. **Azure Data Factory Service**

Data factory service is a managed ETL (Extract Transform Load) cloud service and integration service. used for extracting the required data and performing the transformation on the data to analyse the logs for data and get more insight into the data. Using data factory users can create data driven ETL pipelines for data movement and transform data at scale.

5. **Azure Cosmos Database**

It is a NoSQL database used to store structure, unstructured or semi-structured data to the azure. Azure Cosmos database is highly available (99.999% available) and dynamically scalable and has very low latency while loading and fetching the data. Cosmos database helps to handle the real-time data with large changes managed by big data technology. It is a globally distributed and multi-modal database and users can enable the cosmos database service using a single button and store data across worldwide regions. It is a NoSQL database hence it does not have schema and index management as the database engine handles the schema inbuilt and hence no application downtime as cosmos DB automatically indexes the data. It has in-built security, and all data is encrypted by default.

6. **Azure Active Directory**

It is used to secure all the services provided as part of database service and integrate all these services. It manages all the users’ Identity and access to the various services.

1. *What is the Azure security center?*

Azure Security Center is a solution that provides unified security management across hybrid cloud workloads. It offers threat protection for data centres within both cloud workloads and on-premises. The platform also works with hybrid clouds that are not part of the Azure ecosystem.

The Azure Security Center is designed to resolve a pressing problem when your organization migrates to the cloud. The cloud customer must take more responsibilities when upgrading to Infrastructure-as-a-Service (IaaS) as compared to cloud solutions like Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), where the cloud service providers take care of most tasks related to securing the network and the services.

Azure Security Center offers a unified platform to secure and manage fast-changing workloads and cope with the challenges of securing your hybrid cloud workloads. The platform helps your organization by:

* Enabling your team to have a clear view of the status of your resources after assessing your environment. Such an assessment gives you an insight into whether your resources are secure
* Generating security alerts and providing threat prevention recommendations. Security Center consciously monitors your workloads to detect security rules violations
* Provisioning services automatically since the Security Center is a native part of the overall Azure solution. This way, you can deploy Security Center seamlessly within your Azure-powered environments

With Azure Security Center, organizations can control the security of an ever-growing number of services under constant threat by a growing number of sophisticated malwares.

1. *How to detect and respond to security in Azure.*

Microsoft Sentinel is a scalable, cloud-native, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Microsoft Sentinel is birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

* Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
* Detect previously undetected threats and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
* Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
* Respond to incidents rapidly with built-in orchestration and automation of common tasks.

1. *What is the Azure key vault? Write its features and advantages.*

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.

Microsoft Azure Key Vault service focuses on the security of the below subjects:

1. Secret Management

The Azure Key Vault service can be used to securely store and control access of secrets, such as authentication keys, storage account keys, passwords, tokens, API keys, .pfx files, and other secrets.

1. Key Management

The Azure Key Vault service can be used to manage the encryption keys for data encryption.

1. Certificate Management

The Azure Key Vault service enables you to provision, manage, and deploy SSL/TLS certificates seamlessly for use with Azure integrated services.

Security being the primary driving force of Azure Key Vault’s existence, Microsoft offers the following tiers based on key protection:

* Standard Tier

Uses Software vaults for storing and managing cryptographic keys, secrets, certificates, and storage account keys. This is compliant with FIPS 140-2 level 2 (vaults).

* Premium Tier

Uses a Managed HSM Pool for storing and managing HSM-backed cryptographic keys. This is compliant with FIPS 140-2 level 3 (managed HSM pools).

Benefits of using Azure Key Vault:

* As the keys saved in vault will be served via URIs, this avoids the risk of accidental exposure and storage of keys in non-secure locations.
* By design, even the vendor (Microsoft) can’t extract or see customer keys, hence, its fully protected at the vendor level too.
* If your organization needs security compliance while requiring the Key Vault, Azure Key Vault is a good option, as the Key Vault service is FIPS 140-2 Level 2 (Vault) / FIPS 140-2 Level 3 (Managed HSM Pools) compliant.
* Key usage details are logged, so the log data can be used for audit purpose in case of any key compromise situation.