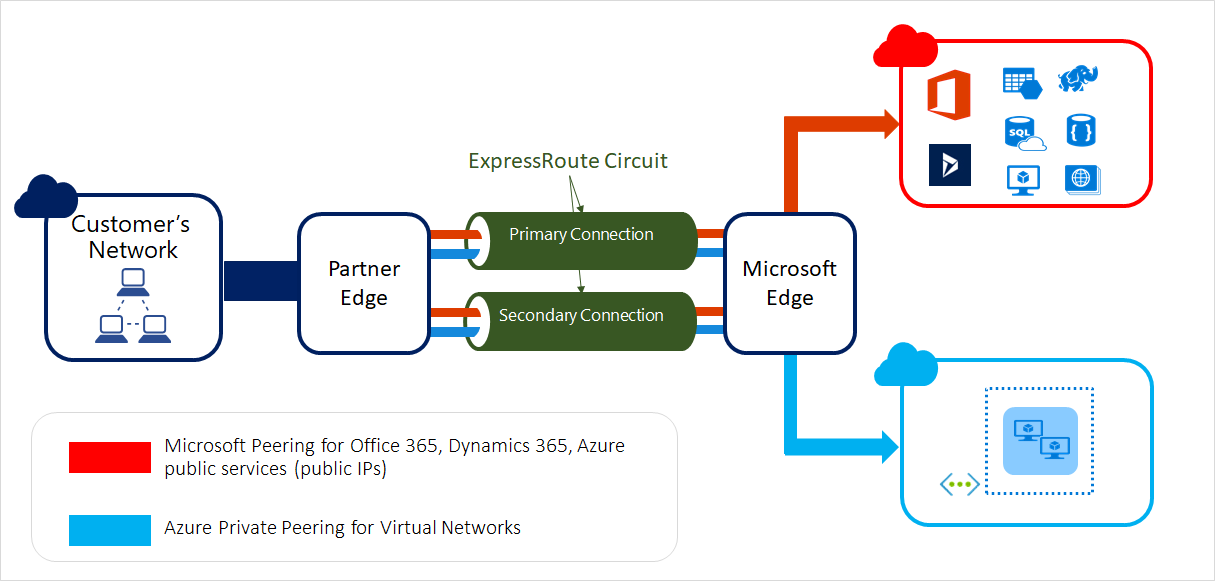
**Azure fundamental assignment 4**

1. List Features and benefits of ExpressRoute.

*With Microsoft Azure ExpressRoute, you can extend your on-premises network to the Microsoft cloud through private connections provided by your connectivity provider. ExpressRoute allows you to connect to Microsoft cloud services such as Microsoft Azure, Office 365, and Dynamics 365.*

*Connections can be obtained from anytoany networks (IPVPNs), point-to-point Ethernet networks, or virtual cross-connects through connectivity providers or colocation facilities. ExpressRoute connections do not go through the public internet. As a result, ExpressRoute connections are more reliable, faster, less delayed, and more secure than regular connections over the Internet. This is useful if you need connection speed and reliability for your Azure resources or your entire Azure infrastructure.*

**

***Features of ExpressRoute***

***Layer 3 Connectivity***

*Azure ExpressRoute uses the BGP dynamic routing protocol to exchange routes between on-premises networks, Azure instances, and public Microsoft IP addresses. Different traffic profiles use multiple BGP sessions.*

***Redundancy***

*The ExpressRoute circuit always has two connections to two Microsoft Enterprise Edge Routers (MSEEs) within the ExpressRoute site. Connection providers use redundant devices to ensure redundancy for connections to Microsoft. A redundant Layer 3 connection configuration is required to enable Microsoft Service Level Agreements (SLA).*

***Connectivity***

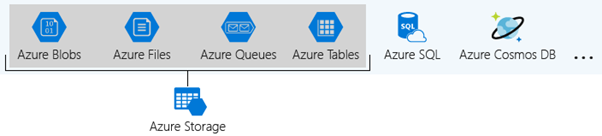
*Azure ExpressRoute offers comprehensive connectivity options for both on-premises networks and regional and global cloud-based Microsoft networks. If you have a valid Azure account and all the prerequisites are met, you can connect to Microsoft Azure and Microsoft 365 services.*

***Benefits of ExpressRoute***

* *Layer 3 connectivity between your on-premises network and the Microsoft cloud through your connectivity provider. The connection can be made over any network (IPVPN), point-to-point Ethernet connection, or virtual cross-connect via Ethernet exchange.*
* *Connections to Microsoft cloud services in all regions of the geopolitical region.*
* *Global connectivity to Microsoft services in all regions using the ExpressRoute premium add-on.*
* *Dynamic routing between the network and Microsoft over industry-standard protocol (BGP).*
* *Redundancy is built into each peering site for reliability.*
* *SLA for connection availability.*
* *QoS support for Skype for Business.*

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

A **storage account** is a container that encapsulates a set of Azure Storage services. Only Azure Storage data services can be included in a storage account. Integrating data services into storage accounts allows users to manage data services as a group. The settings that were set when the account was created, or changed after the account was created, apply to all locations. When a storage account is deleted, all data stored on it will be deleted.



**Types of Azure Storage Accounts**

Azure Storage offers different types of storage accounts. Each type supports its own features and has its own pricing model. Consider these differences before creating a storage account to determine the best account for your application. The types of storage accounts are:

* **General-purpose v2 accounts:** Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.
* **General-purpose v1 accounts:** Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.
* **Block Blob Storage accounts:** Storage accounts with premium performance characteristics for block blobs and appends blobs. It is recommended for scenarios with high transaction rates or scenarios that use smaller objects or require consistently low storage latency.
* **File Storage accounts:** Files-only storage accounts with premium performance characteristics. Recommended for enterprise or high-performance scale applications.
* **Blob Storage accounts:** Legacy Blob-only storage accounts. Use general-purpose v2 accounts instead when possible.

**Azure Disk Storage**

Azure controlled disks are block-stage garage components that are controlled via way of means of Azure and used with Azure Virtual Machines. Managed disks are comparable to a bodily disk in an on-premises server however virtualized. In controlled disks, all you need to do is specify the disk size, type, and provision the disk. Once the disk is provisioned, Azure handles the rest. Each disk can take one of all 3 roles in a digital machine:

|  |  |
| --- | --- |
| **OS disk** | One disk in each virtual machine contains the operating system files. When a user creates a virtual machine, he/she selects a virtual machine image and that fixes the operating system and the OS disk that’s attached to the new machine. The OS disk has a maximum capacity of 2,048 GB. |
| **Data disk** | User can add one or more data virtual disks to each virtual machine to store data. For example, database files, website static content, or custom application code should be stored on data disks. The number of data disks that can be added depends on the virtual machine size. Each data disk has a maximum capacity of 32,767 GB. |
| **Temporary disk** | Each virtual machine contains a single temporary disk, which is used for short-term storage applications such as page files and swap files. The contents of temporary disks are lost during maintenance events, so do not use these disks for critical data. These disks are local to the server and are not stored in a storage account. |

## Blob Storage

Blob storage accounts are specialized in storing blob data and can also be used to choose an **access tier**, which allows you to specify how frequently data in the account is accessed. You can choose an access tier suitable for your storage and which suits your expenses.

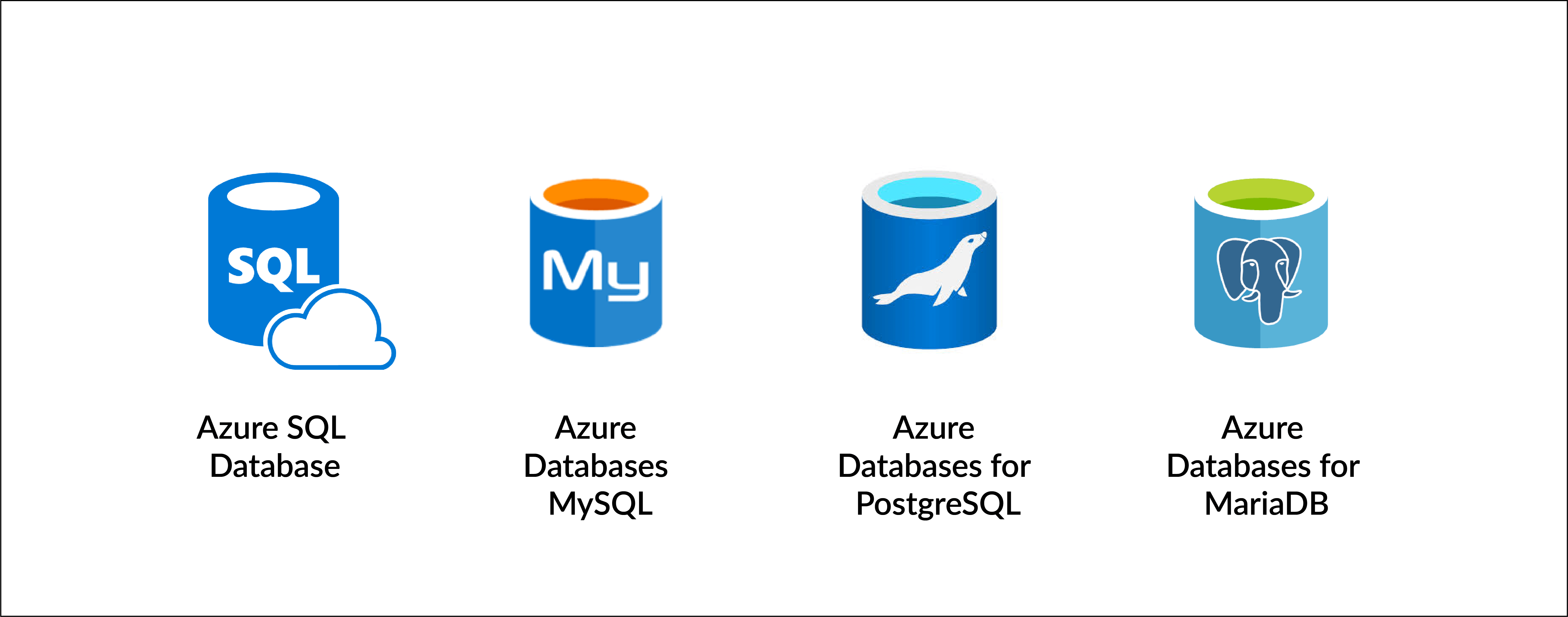
There are two types of access tiers:

**Hot:**This access tier grants us the lowest latency possible. Hence, it should be used with data which is frequently accessed. Naturally, since it offers low latency it is more expensive.

**Cold:**This access tier is less in performance than the “Hot” access tier i.e offers higher latency than the former access tier. That being said, it comes with a lesser price tag and hence can be used for data which is less frequently accessed.

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

Azure offers a choice of fully managed relational, NoSQL, and in-memory databases that span proprietary and open-source engines to meet the needs of modern app developers. Infrastructure management such as scalability, availability, and security is automated, saving time and money. Azure-managed databases focus on building applications while simplifying your work by exposing performance insights through built-in intelligence, unlimited scale, and security threat management.



Azure offers a variety of services for migrating data from different sources or on-premises SQL Server data to the cloud. Database services provide different levels of services and operands based on data, and also 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 onpremise 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 costeffective to transfer data and does not require many changes to queries or application whether data is stretched to the cloud or is on onpremise 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 bidirectionally across various databases both in the cloud or the onpremise 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 analyze 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 structured, unstructured or semistructured 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 multimodal database and users can enable the cosmos database service using a single button and store data across worldwide regions. Since this is a NoSQL database, the database engine handles the built-in schema, so there is no schema and index management. Therefore, Cosmos db automatically indexes the data, so there is no application downtime. It has built-in security and all data is encrypted by default.

**6. Azure Active Directory**

It is used to protect all services provided as part of the database service and to integrate all of these services. Manages identities of all users and access to various services.

1. What is the Azure security centre?

The Microsoft Azure Security Center is a set of tools for monitoring and managing the security of virtual machines and other cloud computing resources in the Microsoft Azure public cloud.

Administrators access the Azure Security Center through the Azure Management Portal. The Security Center has a set of security tools designed to prevent, detect, and respond to potential security threats to your Azure deployment. Your organization needs an Azure subscription to access the Security Center.

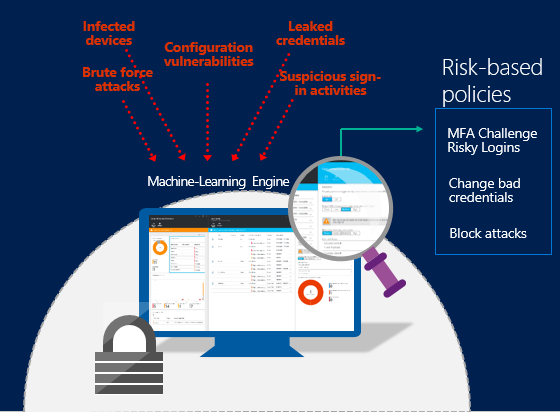
The main features of Azure Security Center are:

* The **policy configuration** allows an administrator to set a set of security-related controls for a particular Azure subscription or resource group. An Azure resource group is a collection of Azure resources. The VM, storage, database, or virtual network needed to run the application.
* **Data collection** collects data about Azure resources to ensure that the policy is applied. The service can also scan VMs daily for potential security threats. The administrator can select the Azure storage account where the collected VM data is stored.
* **Recommendations** provide a list of suggestions for creating an Azure security policy based on the security needs of a particular Azure resource. Possible recommendations include deploying missing system updates, deploying antivirus, and controlling VM traffic using NSGs.
* **Alerts** issue alerts when potential security threats such as compromised VMs and malware are detected. Azure Security Center automatically collects and integrates log data about Azure resources to create alerts.

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

Azure gives constructed in chance safety capability thru offerings inclusive of Azure Active Directory (Azure AD), Azure Monitor logs, and Microsoft Defender for Cloud. This series of protection offerings and abilities offers an easy and speedy manner to apprehend what's taking place inside your Azure deployments.

Azure offers a big range of alternatives to configure and personalize protection to fulfil the necessities of your app deployments. This article discusses a way to meet those necessities.



Examples of some of the ways that Azure Identity Protection can help secure your accounts and identities include:

[**Detecting risk detections and risky accounts**](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection)

* Detect six risk detection types using machine learning and heuristic rules.
* Calculate user risk levels.
* Provide custom recommendations to improve overall security posture by highlighting vulnerabilities.

[**Investigating risk detections**](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection)

* Send notifications for risk detections.
* Investigate risk detections using relevant and contextual information.
* Provide basic workflows to track investigations.
* Provide easy access to remediation actions such as password reset.

[**Risk-based, conditional-access policies**](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection)

* Mitigate risky sign-ins by blocking sign-ins or requiring multi-factor authentication challenges.
* Block or secure risky user accounts.
* Require users to register for multi-factor authentication.

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 something you want to tightly control access to. Such as API key, password, certificate, or encryption key. The Key Vault service supports two types of containers: Vault and managed hardware security module (HSM) pools.

The benefits of Azure Key Vault are mentioned below:

•Organize application secrets in one place

•Keep secrets and keys secure

•Keep an eye on who has access and how they are using it

•Simplified application secret management

•Azure services can be integrated with Key Vault

### Features

### Centralize application secrets

### Securely store secrets and keys

### Monitor access and use

### Simplified administration of application secrets

### Integrate with other Azure services