**Azure fundamental assignment 4**

1. **List Features and benefits of ExpressRoute.**

ExpressRoute is an Azure service that lets you create private connections between Microsoft datacenters and infrastructure that's on your premises or in a colocation facility. ExpressRoute connections don't go over the public Internet, and offer higher security, reliability, and speeds with lower latencies than typical connections over the Internet.

ExpressRoute offers a variety of advanced networking functionalities to expand your on-premises networks in the Microsoft cloud. Some of the core features of Azure ExpressRoute include.

**Layer 3 Connectivity**

Azure ExpressRoute is using the BGP dynamic routing protocol to exchange routes between your on-premises network, your instances in Azure and public Microsoft IP addresses. Different traffic profiles use multiple BGP sessions.

**Redundancy**

n ExpressRoute circuit always has two connections to two Microsoft Enterprise edge routers (MSEEs) at an ExpressRoute Location. Connectivity providers employ redundant devices to ensure redundancy of your connections to Microsoft. You must have a redundant Layer 3 connectivity configuration to make sure Microsoft’s Service Level Agreement (SLA) is valid.

**Connectivity**

Azure ExpressRoute offers rich connectivity options for both your on-premises networks and regional and global Microsoft cloud-based networks. With a valid Azure account and if all requirements are met, you can have connections to the Microsoft Azure and Microsoft 365 services.

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

The Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Core storage services offer a massively scalable object store for data objects, disk storage for Azure virtual machines (VMs), a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store. The services are:

**Disk Types**

Azure offers 2 types of disk storage:

Managed

Managed disk has some advantages over unmanaged disks in the sense that disks will be created and managed for you. This is a IaaS offering.

Unmanaged

With unmanaged disks, you must manage it yourself. Basically, this means that your virtual hard disks are stored in a storage account as page blobs.

And two types of disks:

Premium

Which means your data will be placed on solid state disks

Standard

Where data is placed on regular hard disk drives

**Blob Storage**

The word blob is an acronym which stands for binary large object. Blobs typically include large files that are unstructured, such as images, video, music files, backup files etc.

Blob storage can be divided into two access tiers, a hot access tier for data which is accessed frequently and a cold access tier for data which is not accessed very often.

The cold access tier is cheaper than the hot access tier and as such you can store more data at a lower cost, it is also slightly less available, like 99% as opposed to the 99.9% of the hot storage tier.

It’s also possible to switch between access tiers at any point if you wish to do so.

There are essentially 3 different types of blobs (in a nutshell):

Block blobs

As suggested by the name, block blobs are made of blocks. Each block has a block ID. Blocks can be different sizes, potentially up to a maximum of 4.75TB. Block clients are set to 32MB size block by default, but this can be configured using the SingleBlobUploadThresholdInBytes property.

Block blobs are optimized for data streaming, and has some features which helps you to manage blobs such as an MD5 hash for verification or parallel uploads.

Append blobs

Append blobs are used to append data. Basically, this means that each time you make changes to the blob, the data will be appended at the end of the blob. Data cannot be changed or deleted, only appended.

Page blobs

A page blob consists out of pages. A page is 512 bytes, and the blob can go up to 1 TB in size.

This is typically used for fast read and write operations.

You must choose the type of blob when you create the blob and unfortunately once the blob is created it’s not possible to change it to a different type.

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

|  |  |
| --- | --- |
| Managed, intelligent SQL in the cloud | Azure SQL Database |
| Managed, always up-to-date SQL instance in the cloud | Azure SQL Managed Instance |
| Migrate your SQL workloads to Azure while maintaining complete SQL Server compatibility and operating system-level access | SQL Server on Virtual Machines |
| 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 PostgreSQL |
| 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 MySQL |
| Deliver high availability and elastic scaling to open-source mobile and web apps with a managed community MariaDB database service | Azure Database for MariaDB |
| 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 Cosmos DB |
| Power fast, scalable applications with an open-source-compatible in-memory data store | Azure Cache for Redis |
| Accelerate your transition to the cloud using a simple, self-guided migration process | Azure Database Migration Service |
| Modernise existing Cassandra data clusters and apps and enjoy flexibility and freedom with managed instance service | Azure Managed Instance for Apache Cassandra |

1. **What is the Azure security center?**

Azure Security Center by Microsoft is a solution that provides unified security management across hybrid cloud workloads. It offers threat protection for data centers 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 has to 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.

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

Use the alerts and incidents queues to detect security in Azure.

The response actions you can take on devices include:

Start an automated investigation

Use automated investigation to detect and respond to threats effectively and consistently, at scale. You can use automated investigation to cover multiple devices simultaneously. That's because if a threat is identified across multiple devices, all of those devices will then be included in your automated investigation.

Collect an investigation package

You can use an investigation package, which is a Zip file that contains information about suspicious entities and events on a device. Use investigation packages to understand the present state of the affected device, and to also identify the techniques and tools that an attacker used.

Run antivirus scan

You can also use next-generation protection to remotely start an antivirus scan for your devices to find and address malware on any device.

Restrict app execution

You can restrict specific applications from running on a device. This is a way to prevent attackers from gaining control over your device, and prevent other devices from being compromised through the same app. Users will receive a notification if they attempt to start a restricted app.

Isolate devices

Based on how severe the attack is, and the priority level of the device, it might be necessary to isolate the device from the rest of your network. This is a good way to stop an attacker from gaining more control and performing lateral movement attacks against the rest of your network.

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

Azure Key Vault helps solve the following problems:

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.

**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. When using Key Vault, application developers no longer need to store security information in their application. Not having to store security information in applications eliminates the need to make this information part of the code. For example, an application may need to connect to a database. Instead of storing the connection string in the app's code, you can store it securely in Key Vault.

Your applications can securely access the information they need by using URIs. These URIs allow the applications to retrieve specific versions of a secret. There is no need to write custom code to protect any of the secret information stored in Key Vault.

**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.

Authentication is done via Azure Active Directory. Authorization may be done via Azure role-based access control (Azure RBAC) or Key Vault access policy. Azure RBAC can be used for both management of the vaults and access data stored in a vault, while key vault access policy can only be used when attempting to access data stored in a vault.

Azure Key Vaults may be either software-protected or, with the Azure Key Vault Premium tier, hardware-protected by hardware security modules (HSMs). Software-protected keys, secrets, and certificates are safeguarded by Azure, using industry-standard algorithms and key lengths. For situations where you require added assurance, you can import or generate keys in HSMs that never leave the HSM boundary. Azure Key Vault uses nCipher HSMs, which are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. You can use nCipher tools to move a key from your HSM to Azure Key Vault.

Finally, Azure Key Vault is designed so that Microsoft does not see or extract your data.

**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.

You have control over your logs and you may secure them by restricting access and you may also delete logs that you no longer need.

**Simplified administration of application secrets**

When storing valuable data, you must take several steps. Security information must be secured, it must follow a life cycle, and it must be highly available. Azure Key Vault simplifies the process of meeting these requirements by:

Removing the need for in-house knowledge of Hardware Security Modules.

Scaling up on short notice to meet your organization's usage spikes.

Replicating the contents of your Key Vault within a region and to a secondary region. Data replication ensures high availability and takes away the need of any action from the administrator to trigger the failover.

Providing standard Azure administration options via the portal, Azure CLI and PowerShell.

Automating certain tasks on certificates that you purchase from Public CAs, such as enrollment and renewal.

In addition, Azure Key Vaults allow you to segregate application secrets. Applications may access only the vault that they are allowed to access, and they can be limited to only perform specific operations. You can create an Azure Key Vault per application and restrict the secrets stored in a Key Vault to a specific application and team of developers.

**Integrate with other Azure services**

As a secure store in Azure, Key Vault has been used to simplify scenarios like:

Azure Disk Encryption

The always encrypted and Transparent Data Encryption functionality in SQL server and Azure SQL Database

Azure App Service.

Key Vault itself can integrate with storage accounts, event hubs, and log analytics.