https://www.edureka.co/blog/interview-questions/azure-interview-questions/

https://www.besanttechnologies.com/windows-azure-interview-questions-and-answers

**Blob**

Blobs typically include large files that are unstructured, such as images, video, music files, backup files etc.

**Container**: A container contains a group of blobs in which there can exist an unlimited amount of blobs. A mandatory requirement of a container is that its name should always be lowercase.

**Blob**: A blob is a file of any size and type

**Types of Blob**

**Block Blob**: These blobs are ideal for storing documents and text or binary media files. 50,000 blocks of up to 100 MB, each can be stored in a single block blob, which totals a size of a tad more than 4750 GB or 4.75 TB. (50000\*100MB)

**Append Blob:** Append blobs are similar to Block blobs, but more optimized for appending operations which makes append blobs more suitable to store logging scenarios. What differentiates append blobs from block blobs is storage capacity. This blob can only store up to 4MB of data, unlike 100MB in block blobs. Therefore, append blocks are limited to a storage capacity of a little over 195 GB. (50000\*4 MB).

**Page Blob:** Page blobs can store about **8** TB of data, which makes these extremely efficient for scenarios that require high reading and writing operations. This blob storage option is useful for all Azure virtual machines storage disks including the operating system disk. Within Azure, there are two-page blob categories like Standard, used for virtual machines with an average amount of read/write operations, and Premium, used for virtual machines for intensive read/write operation

**API Management**

* It is fully managed service
* Using APIM we can publish, Maintain and Monitor API’s
* Major drawback for APIs is that one cannot track the utilization of the APIs
* Instead of accessing the API directly, you can register API into APIM. Therefore, user cannot directly access API instead of going APIM. Now APIM take care of authorization, Oauth and Open ID connect and all
* This is not just about authenticating and authorizing access to API’s, it is also about policies like rate limit, quota, XML to JSON conversion etc.
* One can also apply authentication on the API and authorize application to access the API

**Security**

Three ways to secure API in APIM

1. When you register your API to APIM services, you will get primary key and secondary key under subscription. One of these needs to be passed in the header of the request to the APIM. This protects your API from being called by anyone without a subscription key. Request without a key are stopped at the APIM gateway, never reaching your API backend.
2. Another one is Oauth 2.0 – token based authentication
3. Third one is Open ID Connect

**Policies**

* Using policies, it will change the behavior of API through configuration.
* Policies like conversion from XML to JSON and restrict the amount of incoming calls from a developer
* Restrict the incoming call from IP addresses
* <https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-policies>
* <https://docs.microsoft.com/en-us/azure/api-management/set-edit-policies>

**Logic app**

* Used for creating workflows
* It provides a visual designer for configuring the workflows.
* You can define a workflow with connectors and logic creation using inbuilt standard connectors
* Logic Apps is a fully managed IPAAS (Integration platform as a service)

**End Point**

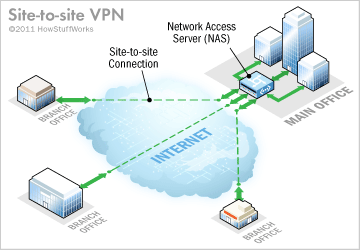
Some of the resources are not able to create under Vnet. Such as Blob storage account

To overcome this problem, we can use end point to connect blob from vnet

**P2S VPN**

* With a Point-to-Site VPN, you can connect a single computer (the point) to your Azure network (the site), and your computer will be authenticated to the VPN using certificates
* If a virtual machine in virtual network needs to be connected with on premise machine, the point-to-site connectivity is needed

**S2S VPN**



* It is used to create secure connection between to end points
* when you need a persistent connection from many on-perm devices and computers to your Azure network
* Site-to-site VPN can be intranet based or extranet based
* Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations
* Extranet-based — When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs

**Deployment models**

Public Cloud, Private Cloud and Hybrid Cloud

**Public cloud**:

* The end users can access the services via public network like internet
* Popular for hosting everyday apps like email, CRM and other business support apps
* more vulnerable to attacks due to high levels of accessibility

**Private Cloud**:

* It provides cloud services and infrastructure exclusively to a single tenant
* The cloud infrastructure can be monitored either by cloud provider or the tenant