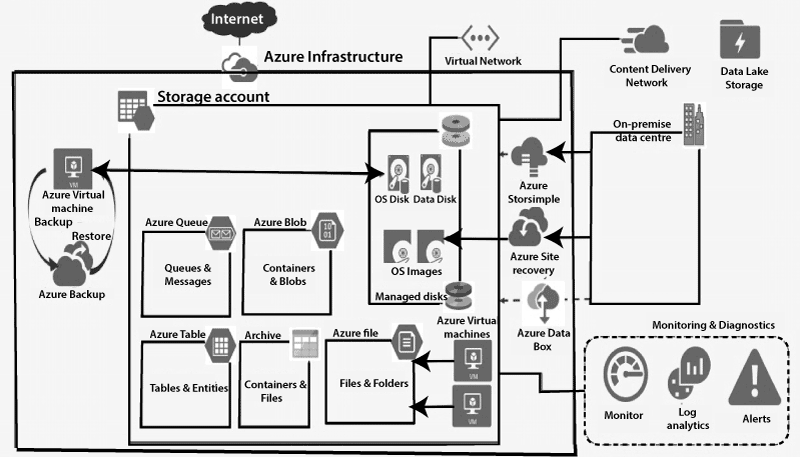
Azure Services list.

1. Compute Service
2. Azure Storage Service
3. Networking Service
4. Database Service
5. Azure DevOps.

Azure Storage Service:

Azure Blob:

* **Azure Blob:** We can have *Azure Blob*storage within the storage account, which is used to store the unstructured data such as media files, documents, etc.



Azure Storage Account

An Azure Storage Account is a secure account, which provides you access to services in Azure Storage.

The storage account is like an administrative container, and within that,

we can have several services like **blobs, files, queues, tables, disks**, etc. And when we create a storage account in Azure, we will get the unique namespace for our storage resources. That unique namespace forms the part of the URL. The storage account name should be unique across all existing storage account name in Azure.

**Access Tiers**

There are four types of access tiers available:

***Premium Storage (preview):*** It provides high-performance hardware for data that is accessed frequently.

***Hot storage:*** It is optimized for storing data that is accessed frequently.

***Cool Storage:*** It is optimized for storing data that is infrequently accessed and stored for at least 30 days.

***Archive Storage:*** It is optimized for storing files that are rarely accessed and stored for a minimum of 180 days with flexible latency needs (on the order of hours).

**Storage account endpoints**

Whenever we create a storage account, we will get an endpoint to access the data within the storage account. So each object that we stored in Azurestorage has an address, which includes your unique account name and the combination of an account name, and service endpoint, which forms the endpoint for your storage account.

For example, if your general-purpose account name is mystorageaccount then generally the default endpoints for different services looks like:

**Azure Blob storage:** <http://mystorageaccount.blob.core.windows.net>.

**Azure Table storage:** <http://mystorageaccount.table.core.windows.net>

**Azure Queues storage:** <http://mystorageaccount.queue.core.windows.net>

**Azure files:** <http://mystorageaccount.file.core.windows.net>

29-05-2023:

The most fundamental building block of **Azure network services** is the virtual network. Using a virtual network, we can deploy our isolated network on Azure. And we can divide the virtual network into multiple parts using subnets.

For example –

Webserver subnet,

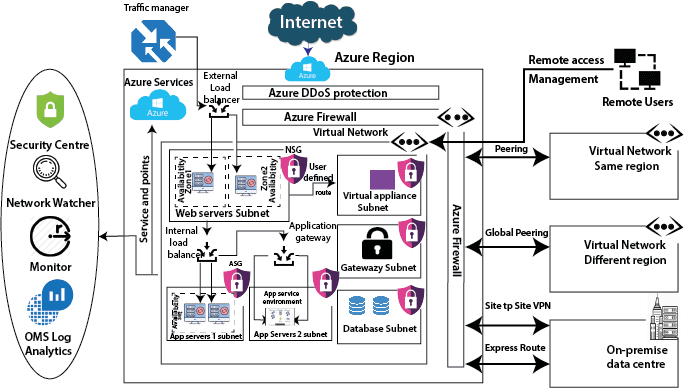
App servers1 subnet,

App servers2 subnet,

Database subnet,

Gateway subnet,

Virtual Appliance subnet, etc.



**Service Protection:** After the deployment of all these services, we need to protect these services. Azure provides several protection strategies.

**DDoS Protection:** The DDoS protection will protect our workload in the virtual network from DDoS attacks. There is a two-tier available in DDoS protection. One is the basic, which is free and enabled automatically. If we need the advance capability, then we can go for the DDoS standard tier.

**Firewall:** When we need network security, we use a firewall. Azure provides a firewall service which you can centrally manage inbound and outbound firewall rules.

We can able to create network firewall rules, application firewall rules, inbound SNAT rules, outbound DNAT rules, etc.

**Network Security Groups:** If you think the firewall is too costly for you, then we can use Network security groups. We can filer the inbound and outbound traffic using network security groups. We can attach the network security group at two levels, one at the subnet level and other we can attach to a virtual machine.

**Application Security Groups:** Microsoft introduces the application security group to put all the server related to one application in one application security group and use that application security group in network security group inbound and outbound rules. The primary purpose of the Application Security Group is to simplify the rule creation in NSG's.

Service Availability

We must make sure that our application is highly available and resilient to regional failures, data center failure, and rack failures. Azure provides some services to make our application highly available; these are:

**Traffic Manager:** Microsoft Azure traffic manager controls the distribution of user traffic for service endpoints in different regions. Service endpoints supported by Traffic Manager include Azure VMs, Web Apps, Cloud services, etc. It uses DNS to direct the client request to the right endpoint based on a traffic-routing method and the health of endpoints.

**Load Balancer:** Load balancer is used to distribute the traffic evenly between a pool of web servers or application servers. There are two types of the load balancer, one is external load balancer which sits outside the virtual network and the second one is an internal load balancer that sits inside the virtual network.

**Application Gateway:** Using the application gateway, we can achieve URL path-based routing, Multi-site hosting, etc.

**Availability Zones:** By deploying our virtual machines into different availability zones, we can route our application traffic to virtual machines that are located in different availability zone in case of failure of datacenter within any region.

**Peering:** To enable communication between two virtual networks, we can establish peering. We can do this peering with virtual networks within the same region. If we have an Azure virtual network in another region, then we can use global peering. And for the on-premises data center, we have two options, and one is the site to site VPN, which will get established over the Internet. But for private connectivity, we have to use the express route.

Virtual Network:

The Azure Virtual Network is a logical representation of the network in the cloud. So, by creating an Azure Virtual Network, we can define our private IP address range on Azure and deploy different kinds of Azure resources. For Example - Azure virtual machine, App service environment, Integration service environment, etc.

**Subnet**

Subnet plays a vital role because many configurations will be done at a subnet level. It is a range of IP addresses in the VNet.

Vnet can be divided into multiple subnets based on different design considerations, for example - we can deploy a virtual machine, App services environment, integration service environment, etc.

VMs & PaaS services deployed to subnets n the same VNet and can communicate with each other without any extra configuration.

Route tables, NSG, Service endpoints, and policies are configured to the subnets.

Azure Concepts:

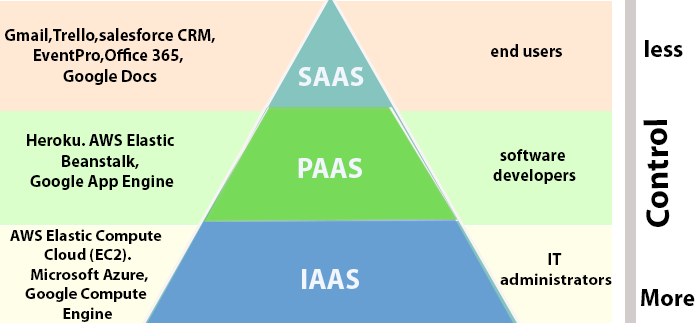
Az-900

Az-203 -development

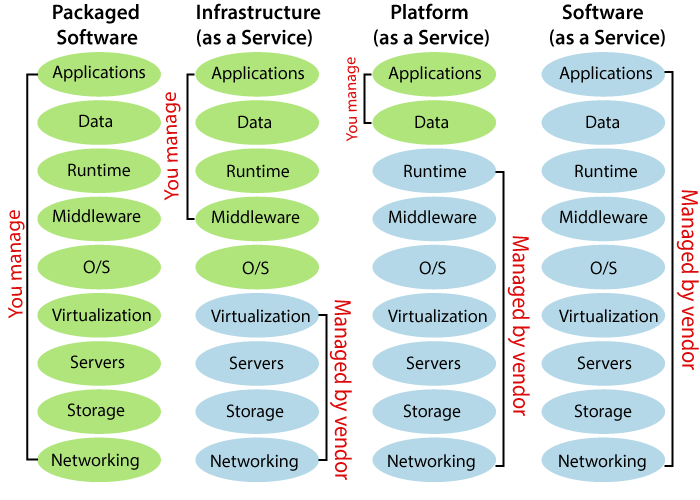
Az-400 solution architecture :

* **Public Cloud:**The cloud resources that are owned and operated by a third-party cloud service provider are termed as public clouds.
* It delivers computing resources such as servers, software, and storage over the internet
* **Private Cloud:**The cloud computing resources that are exclusively used inside a single business or organization are termed as a private cloud.
* A private cloud may physically be located on the company’s on-site datacentre or hosted by a third-party service provider.
* **Hybrid Cloud:**It is the combination of public and private clouds, which is bounded together by technology that allows data applications to be shared between them.
* Hybrid cloud provides flexibility and more deployment options to the business.

Types of Cloud Services



1. **Infrastructure as a Service (IaaS):**In IaaS, we can rent IT infrastructures like servers and virtual machines (VMs), storage, networks, operating systems from a cloud service vendor. We can create VM running Windows or Linux and install anything we want on it. Using IaaS, we don’t need to care about the hardware or virtualization software, but other than that, we do have to manage everything else. Using IaaS, we get maximum flexibility, but still, we need to put more effort into maintenance.
2. **Platform as a Service (PaaS):** This service provides an on-demand environment for developing, testing, delivering, and managing software applications. The developer is responsible for the application, and the PaaS vendor provides the ability to deploy and run it. Using PaaS, the flexibility gets reduce, but the management of the environment is taken care of by the cloud vendors.
3. **Software as a Service (SaaS):** It provides a centrally hosted and managed software services to the end-users. It delivers software over the internet, on-demand, and typically on a subscription basis. E.g., Microsoft One Drive, Dropbox, WordPress, Office 365, and Amazon Kindle. SaaS is used to minimize the operational cost to the maximum extent.



Discussed with suresh on 7-7-23:

VM-----------Virtual machine

In terraform multiple resource creation will be using ---count

VN – vnet peering networking –two subscription communicate.

Like hub and some other hub.

Subnet------- Ip range 10.20.1.9/16, NSG ports inbound and out bound.

Storage – file blob, archive, hit, cool

Firewall ---Security unknow access,

Security –

Null

Local variable

Global variable

Backend file.

Terraform through done

responsible for designing, implementing, and managing Azure cloud solutions