What are all the services Azure offers as PaaS?

**Azure offers five main services of Platform as a Service in which multiple service types host a custom application or a business logic for specific use cases:**

* Web apps. ...
* Mobile apps. ...
* Logic apps. ...
* Functions. ...
* Web jobs.

Azure AD is a highly-available and **highly-scalable identity management service for small and large organizations**. It enables organizations to use their corporate credentials to authenticate to new or existing applications, factoring out the authentication process and eliminating the need for many different identities.

Azure AD B2C is a separate service from [Azure Active Directory (Azure AD)](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis). It is built on the same technology as Azure AD but for a different purpose. It allows businesses to build customer facing applications, and then allow anyone to sign up into those applications with no restrictions on user account. A white-label authentication solution. It acts as an identity provider for two business.

What's Azure security Center?

* Azure Security Center is **a unified security management system offered by Microsoft to Azure customers**. ... Providing visibility and control over the security of Azure resources (like Virtual Machines, Cloud Services, Azure Virtual Networks, and Blob Storage).It gives you secure score dashboard of overall environment. It gives security alerts and recommendations (insights).
* Azure defender is a paid feature of Azure security center, it gives vulnerability assessment, threat detection and etc.
* Regulatory compliance assessment

What is azure monitor for?

**Collect, analyze, and act on telemetry data from your Azure and on-premises**

1. Metrics
2. Logs
3. Alerts

Application Insights:

**What is Azure application Insights**

Azure application insights is a part of  Azure monitor service. It is one of the powerful tools which can help to diagnose, monitor and analyze your application. It can help in identifying anomalies and monitoring the performances of applications deployed anywhere irrespective of their technology.

Why do we use Azure key vault?

Secrets Management - Azure Key Vault can be used **to Securely store and tightly control access to tokens, passwords, certificates, API keys**, and other secrets. ... Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.

Active Directory:

The default protocol used in directory services is LDAP ( Lightweight Directory Access Protocol).

Forest is used to define an assembly of AD domains that share a single schema for the AD.  All DC’s in the forest share this schema and is replicated in a hierarchical fashion among them.

**Major Components of Active Directory are**

* Domain
* Tree
* Forest
* Organizational Unit
* Site

AD is great at managing traditional on-premise infrastructure and applications. Azure AD is great at managing user access to cloud applications.

For Authentication & authorization of all the objects in an organization uses AD, it uses LDAP,NTLM and kerberoes protocols

When compared with AD, here is what Azure AD doesn’t do:

* You can’t join a server to it
* You can’t join a PC to it in the same way – there is Azure AD Join for Windows 10 only (see later)
* There is no Group Policy
* There is no support for LDAP, NTLM or Kerberos
* It is a flat directory structure – no OU’s or Forests

So Azure AD does not replace AD.

Active directory, what is FSMO roles?

FSMO stands for Flexible Single Master Operation

Active directory database follows multiple master model which means changes in active directory database get replicated to all the Domain Controllers in the domain. ... So, these roles are called Flexible Single Master Operation.

Domain Naming Master – Add/remove domain controller to a forest.

Schema master- Maintaining the attributes and classes (user properties) of all the objects in the forest.

RID master – maintaining the RID pools, every object in a domain have a rid number attached.

PDC Emulator- is responsible for time syncing in entire domain

Infrastructure master- It checks the group authorizations in a domain.

What is Azure security group?

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group **contains security rules that allow or deny inbound network traffic to, or outbound network traffic from**, several types of Azure resources.

It is stateful, when we create an inbound or an outbound rule.

Network acls:

Is set of rules for entire subnet.

Security group is for certain IP address

It is stateless, it return traffic must be allowed explicitly.

What is VNet in Azure?

An Azure Virtual Network (VNet) is **a representation of your own network in the cloud**.

Microsoft Azure ExpressRoute is **a connector that uses a connectivity provider to extend your on-premises networks into the Microsoft Azure and Microsoft 365 clouds over a private connection**. Azure ExpressRoute supports any-to-any (IP VPN) network and point-to-point Ethernet networks.

DHCP: Dynamically allocates the IP address

DNS: It is for name resolution

What is an Azure traffic Manager?

Azure Traffic Manager is **a DNS-based traffic load balancer**. This service allows you to distribute traffic to your public facing applications across the global Azure regions. ... The endpoint can be any Internet-facing service hosted inside or outside of Azure.

**Azure Policy:**

Azure Policy is set of rules/plans

It deals with resource properties

There are lot of built in polices.

It is an Azure service helps to manage, assign and governance. Can be applied at subscripton level and resource group.

**How is Azure API Management used?**

It is primarily used to provide a central interface to create, provision and manage API for web and cloud applications and services.  With Azure API Management user can;

* Monitor the health of APIs, identifying errors, configure throttling, rate limits and more on each API.
* Provides insight into the utilization of APIs
* Creating and managing user roles and defining end to end API usage policies
* Provides a central interface to consolidate and manage thousands of API’s across multiple platforms.
* Provide an authentication and access control mechanism to manage and ensure security on API access and utilization

API: Application programming interface.

What is B2C in Azure AD?

Azure AD B2C stands for **Azure Active Directory Business-to-Consumer**. ... Azure AD B2C is a directory service that leverages identity stores outside of your company. It is an authentication service for publicly facing applications.

Azure AD B2C is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks.

Azure AD B2C is a separate service from [Azure Active Directory (Azure AD)](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis). It is built on the same technology as Azure AD but for a different purpose. It allows businesses to build customer facing applications, and then allow anyone to sign up into those applications with no restrictions on user account.

NSG: Design to filter traffic to and from the Azure resources located in the Azure Vnet.

Ability to have multiple inbound and outbound rules

An Initiative is a collection of policy definitions that are tailored towards **achieving a singular overarching goal**. ... Policy is a single rule and when we need to implement multiple rules for a single resource or set of resources create all the policies and then attach them to a single initiative.