

AZ-900 MICROSOFT AZURE FUNDAMENTALS

Infrastructure as a service (IaaS) -Offers necessary compute, storage, and networking assets on demand, on a pay-as-you-go basis.

Platform as a service (PaaS) - Provide complete development and deployment environment in the cloud, with assets that enable to deliver simple cloud-based apps to cloud-enabled enterprise applications. (For web application lifecycle)

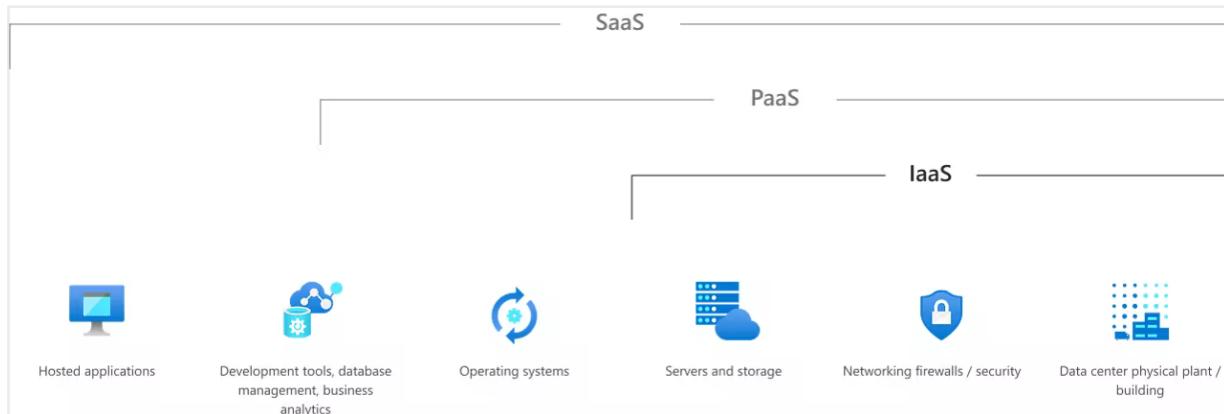
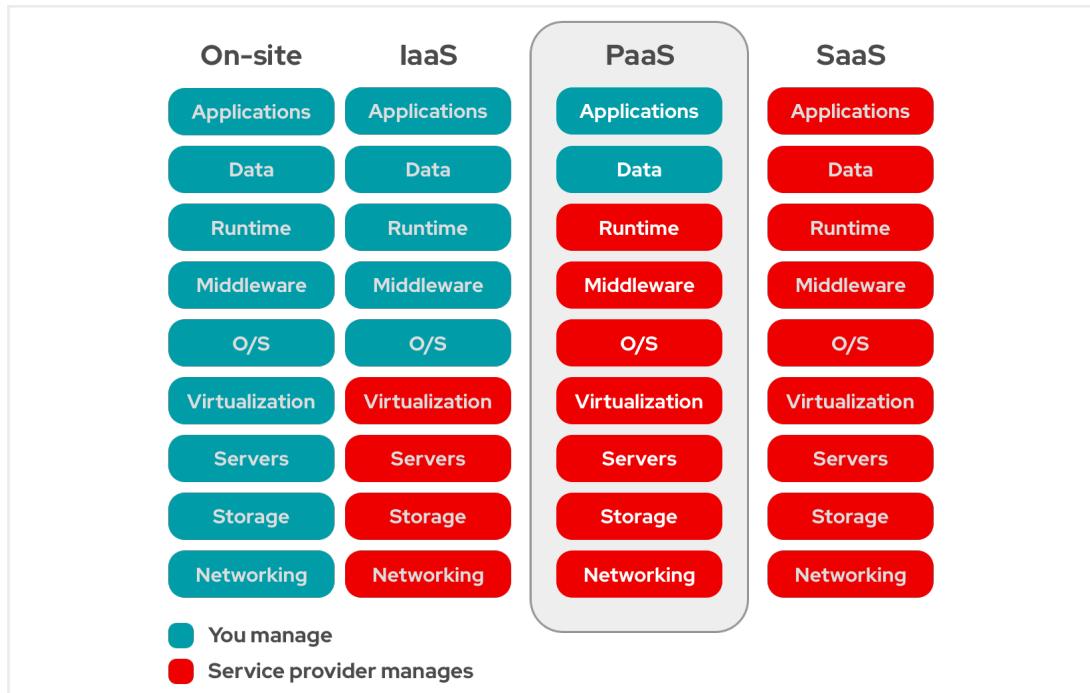
Software as a service (SaaS) -Host and manage the software application and underlying infrastructure.

IaaS - > Azure Virtual Machine ,Azure Storage Account

PaaS -> Azure App service, Azure SQL Database,Azure Cosmos DB,Azure Synapse Analytics

SaaS -> Qutlook email , Calendar , Microsoft Office 365

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Provider	Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider



Expenditure models: OpEX vs CapEX:

OpEX: Pay-as-you-go pricing (Example: Cloud Services)

CapEX: Upfront cost Example (Deploying your own data center)

Virtual Machines Scale Sets:

Create and manage a group of load balanced VMs.

Allows your application to automatically scale as resource demand changes

All VM instances are created from the same base OS image and configuration.

Provides high availability and application resiliency

There is no cost for the scale set itself, you only pay for each VM instance that you create.

VPN gateway

Can connect Azure virtual network with On-premises network
All transferred data is **encrypted** in a private tunnel as it crosses the internet.
Azure VPN Gateway instances are deployed in Azure Virtual Network

- Site-to-Site connection - Connect on-premises datacenters to virtual networks
- Point-to-Site connection - Connect individual devices to virtual network
- Multi-site connection – Connect more than one on-premises network to virtual network
- Network-to-Network connection - Connect virtual networks to other virtual networks

We can also use "Network peering"

Networking peering vs tunnel:

VNet Peering provides a low latency, high bandwidth connection useful in scenarios such as **cross-region data replication and database failover** scenarios. Since traffic is **completely private** and remains on the Microsoft backbone, customers with strict data policies prefer to use VNet Peering as public internet is not involved. Since there is no gateway in the path, there are no extra hops, ensuring low latency connections.

VPN Gateways provide a limited bandwidth connection and is useful in scenarios where **encryption is needed**, but bandwidth restrictions are tolerable. In these scenarios, customers are also not as latency-sensitive.

Application Gateway provides HTTP based load balancing.

Azure CDN: paas

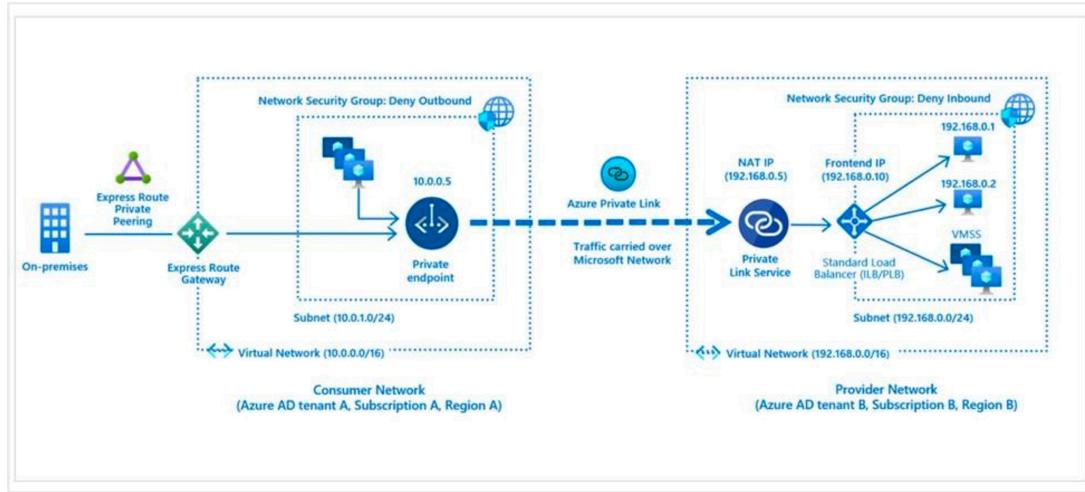
ExpressRoute:

- Use a private, dedicated connection
- Data do not go over the public Internet
- Data is not Encrypted
- Low Latency, faster connection, for high traffic

Expressroute vs von gateway vs vent peering?

Virtual Network service endpoints: provides secure and direct connectivity to Azure services

Private Link: a network interface that uses a private IP address from your virtual network.



Service Endpoint vs Private endpoint:

Service endpoint — It will continue to be a publicly routable IP address, Free.
Private endpoint — It is a private IP in the address space of the virtual network where the private endpoint is configured, cost.

Azure Storage Service

Azure Storage Data Redundancy: Protect your data from hardware failures, network or power outage, and natural disasters

Azure Blob Storage: Binary Large Object

Block Blobs: For large objects that doesn't use random read and write operations, files that are read from beginning to end (media files or image files for websites)

Page Blobs: Optimized for random read and write operations. Provide durable disks for Azure Virtual Machines (Azure VMs)

Append Blobs: Optimized for append operations. e. g. Logs. When you modify an append blob, blocks are added to the end of the blob only Updating or deleting of existing blocks is not supported

Storage Access Tiers: hot, cool, archive

Azure Table Storage: NoSQL key-value Storage, key-value

Azure Queue Storage: Message queuing service to store large numbers of messages.

Azure File Storage: Simple, secure, and serverless enterprise-grade cloud file shares

Disk Storage: High-performance, highly durable block storage for Azure Virtual Machines

Import and export service: Move small amount of data – Internet, AzCopy, Azure Storage Explorer, Large: ship

Azure Migrate: Discover, assess, right-size, and migrate your on-premises virtual machines (VMs) to Azure

Assessment and migration

Databases → Azure SQL Database or Managed Instance

Web Applications → Azure App Service

Virtual Desktops → Azure Virtual Desktop

Servers, databases, and web apps → Azure VM or VMware

Data → Azure Data Box

Authentication techniques:

Password-based authentication

Password-less authentication (Example: send OTP on mobile/email)

Multi-factor authentication (OTP, Security Question, Password)

Single Sign-on

Social Authentication

Authorization Techniques:

Role-based access control

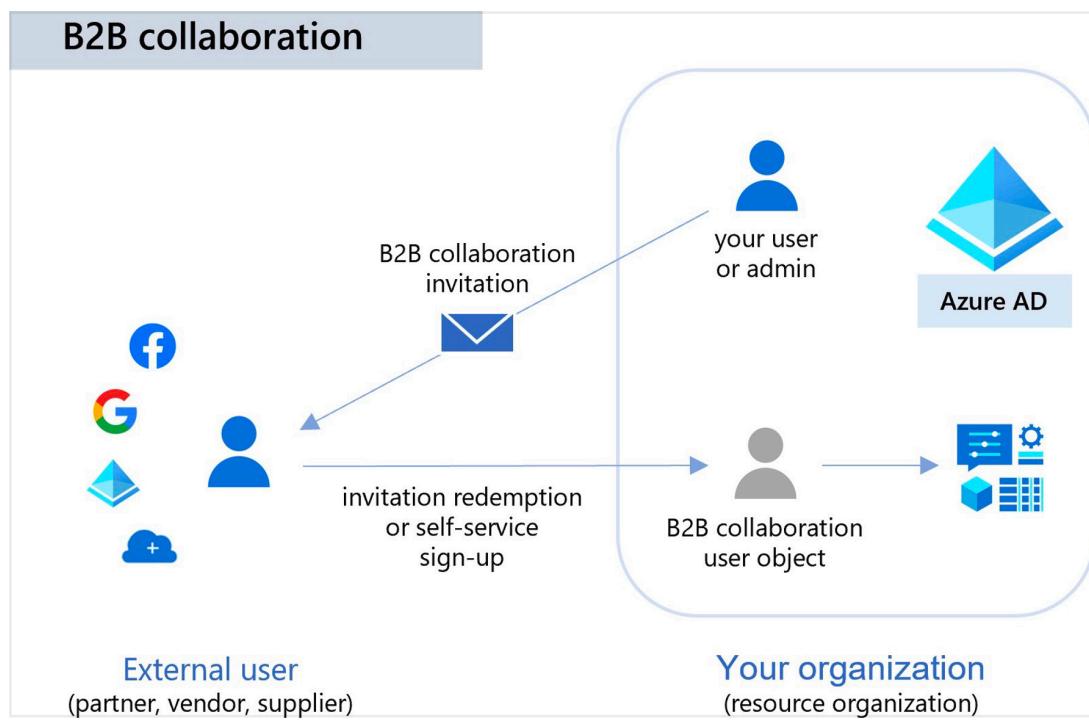
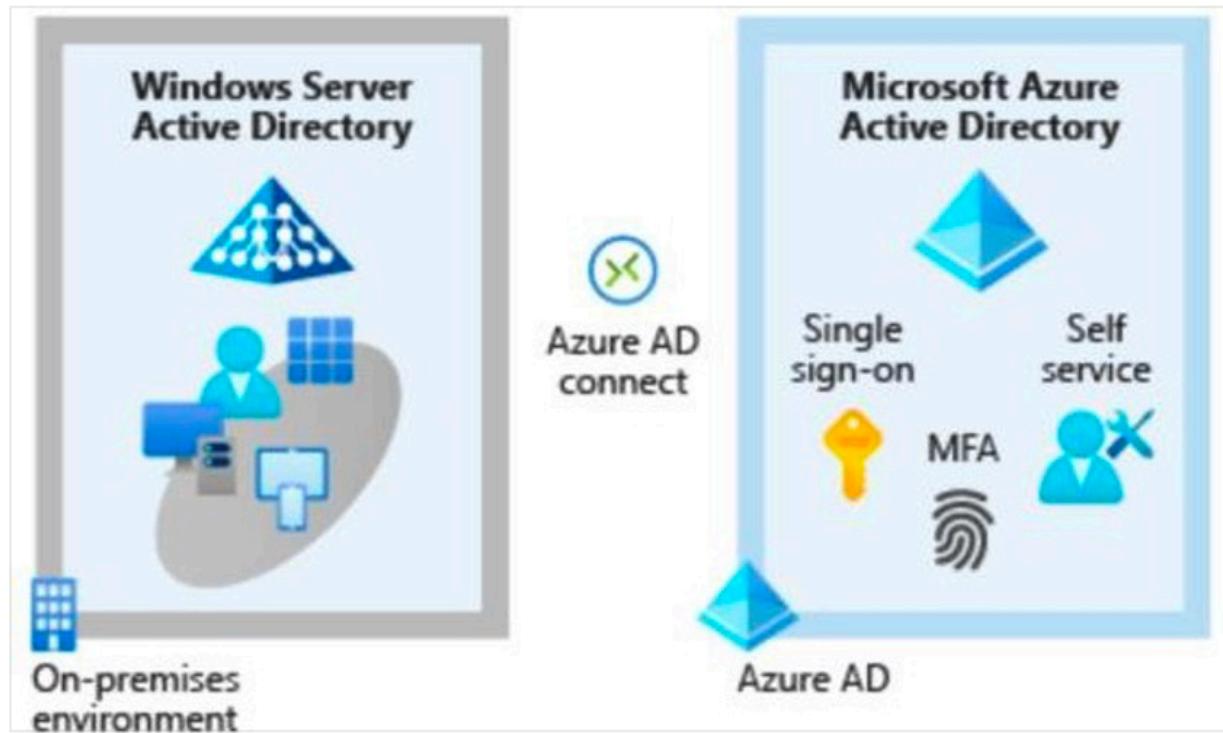
JSON web token

SAML

OpenID authorization

OAuth

Azure Active Directory: Microsoft's cloud-based identity and access management service



Azure AD Roles vs RBAC Roles:

AD: Manage access to Azure Active Directory resources.

RBAC: Manage access to Azure resources.

Multifactor authentication

Conditional Access: Azure Active Directory uses Conditional Access to grant (or deny) resource access based on identity signals. (*Premium P1 or P2 license*)
Passwordless authentication: Windows hello for business, Microsoft Authenticator, FIDO2

Azure RBAC: Role-based access control

	Role				
	Reader	Resource-specific	Custom	Contributor	Owner
Scope	[User icon]				
	Management group				
	[Key icon]	Observers	Users managing resources		Admins
	[Resource group icon]				
	[Resource icon]	Automated processes			

Defense in depth: Protect information and prevent it from being stolen by those who aren't authorized to access it. (**DDOS: Network perimeter**)

Microsoft Defender for Cloud:

Secure score - A single score so that you can tell, at a glance, your current security situation

Recommendation on how to improve score

Defend: detect threats and send alerts

Cost Affecting Factors

Cost Reduction Methods:

Reservations

Save on licensing costs

Spot VM

Azure Service Advisor

Delete unused resources

Migrate from IaaS to PaaS services

Choose Low cost Location and Reservation

Total Cost of Ownership (TCO) Calculator:

Azure Cost Management and Billing: Manage your cloud spending with

confidence

Cost Management: This is a built-in service that gives you a breakdown of the usage and cost of your Azure resources.

Azure Tags: name-value pairs that help to organize the Azure resources

Azure Policy: Achieve real-time cloud compliance at scale with consistent resource governance

Azure Blueprints: Enabling quick, repeatable creation of governed environments

Azure Resource Manager (ARM): Deployment and management service for Azure

Azure Arc: Secure, develop, and operate infrastructure, apps, and Azure services anywhere. Manage your entire environment together by projecting your existing non-Azure and/or on-premises resources into Azure Resource Manager.

Azure Advisor: Your free, personalized guide to Azure best practices

Reliability: Ensures and improves the availability of your mission-critical applications.

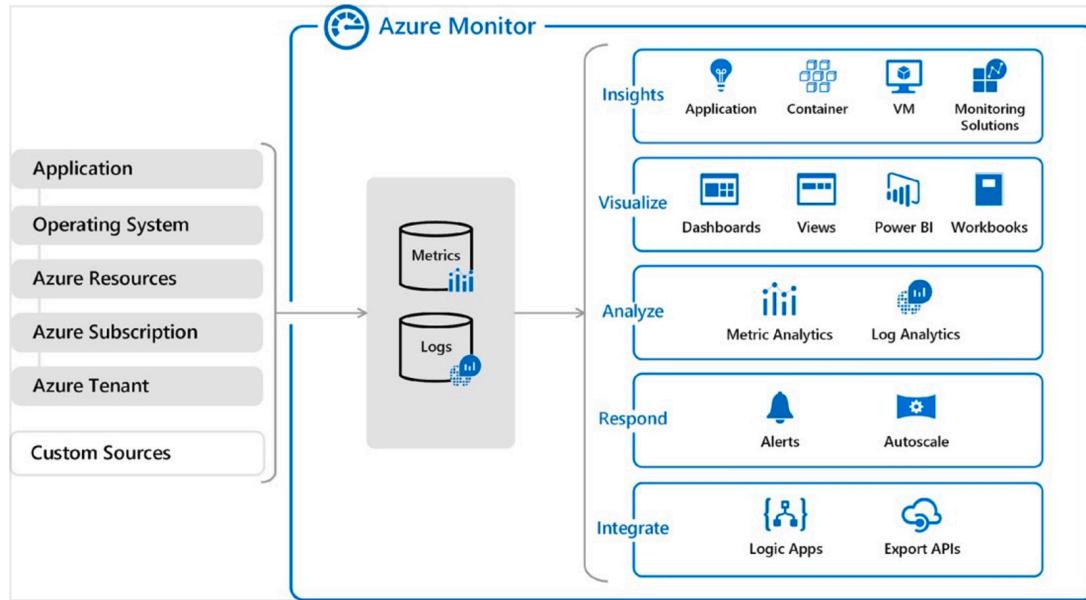
Security: Detect threats and vulnerabilities that might lead to security breaches.

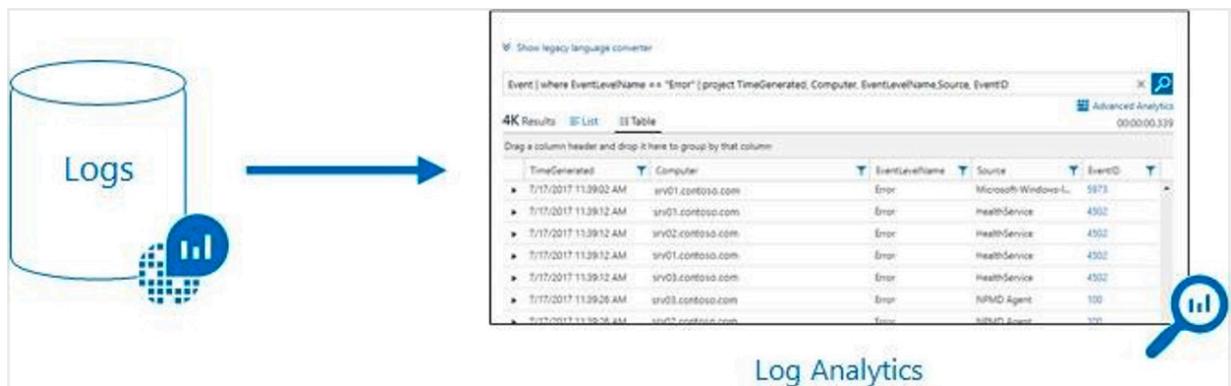
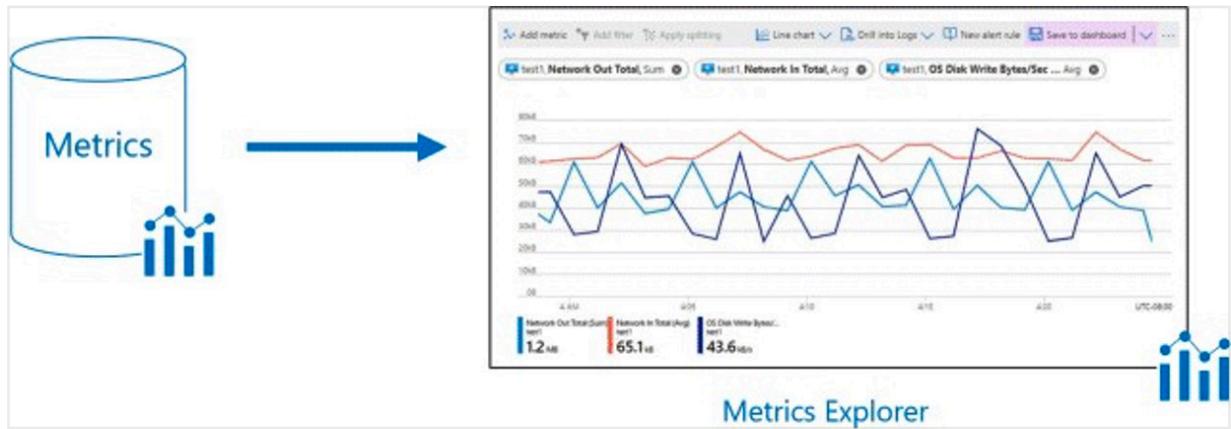
Performance: Improve the speed of your applications.

Cost: Optimize and reduce your overall Azure spending.

Operational Excellence: Help you achieve process and workflow efficiency, resource manageability, and deployment best practices.

Azure Monitor: Full observability into your applications, infrastructure, and network





Azure Service Health: Personalized alerts and guidance for Azure service issues

storage plan:

Free = 1 GB

Shared = 1 GB

Basic = 10 GB

Standard = 50 GB

Premium = 250 GB

Isolated = 1 TB

For all VM that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have VM Connectivity to at least one instance at least **99.99%** of the time.

For all VM that have two or more instances deployed in the same Availability Set or in the same Dedicated Host Group, we guarantee you will have VM Connectivity to at least one instance at least **99.95%** of the time.

For any Single Instance VM using Premium SSD or Ultra Disk for all Operating System Disks and Data Disks, we guarantee you will have VM Connectivity of at least **99.9%**.

For any Single Instance VM using Standard SSD Managed Disks for Operating System Disk and Data Disks, we guarantee you will have VM Connectivity of at

least **99.5%**.

For any Single Instance VM using Standard HDD Managed Disks for Operating System Disks and Data Disks, we guarantee you will have VM Connectivity of at least **95%**.

DevTest Lab

Quickly provision development and test environments
Minimize waste with quotas and policies
Set automated shutdowns to minimize costs
Build Windows and Linux environments

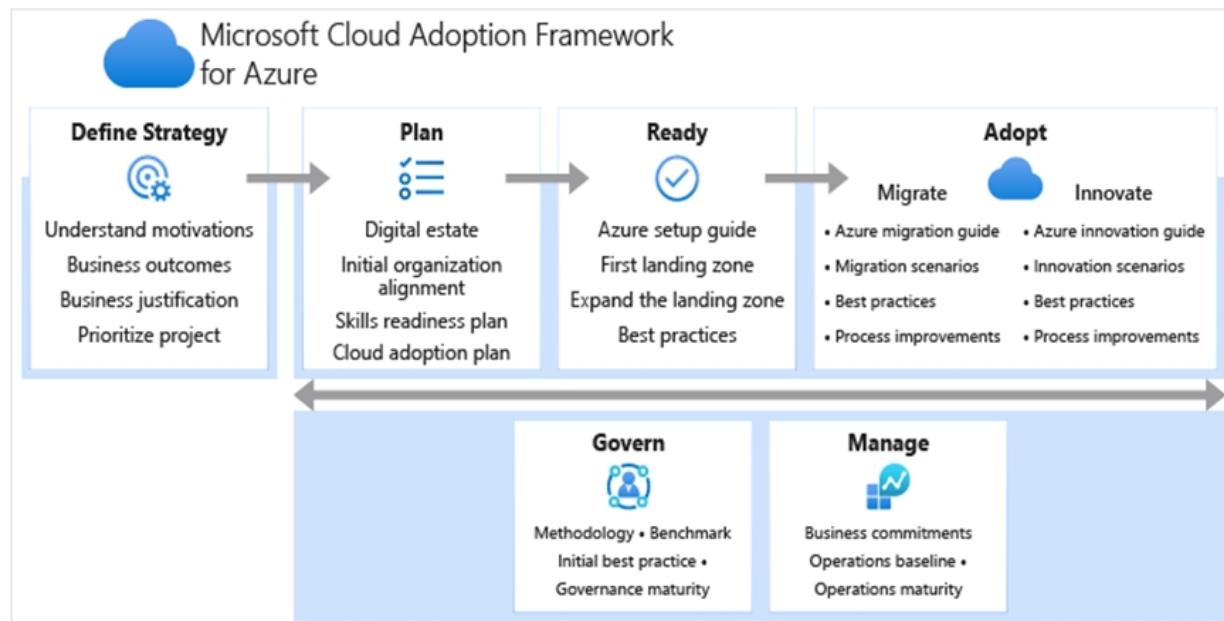
You plan to migrate a web application to Azure. The web application is accessed by external users.

You need to recommend a cloud deployment solution to minimize the amount of administrative effort used to manage the web application.

What should you include in the recommendation?

- B. Platform as a Service (PaaS) **Most Voted**
-

The public cloud is a shared entity whereby multiple corporations each use a portion of the resources in the cloud



Regions > Zones > Datacenters > Availability Sets (Rack)

A Local Network Gateway is an object in Azure that represents your on-premise VPN device, **IP address ranges**. your local holds all configuration information on your local network settings.

A Virtual Network Gateway is the VPN object at the Azure end of the VPN and on-premise.

An Azure AD tenant can have multiple subscriptions but an Azure subscription can only be associated with one Azure AD tenant.

Manage compliance -> azure policy

You can move resources to a **new resource group or subscription**

If you want to raise the limit or quota above the default limit, open an online customer support request at no charge

Availability zones are used to replicate data and applications in the **same** region

Azure containers are the backbone of the virtual disks platform for Azure IaaS.

To create a storage solution in Azure for the planned mapping drive, you should create a **File service in a storage account**.

Tags for Resources are **not** inherited by default from their Resource Group

To read or download a blob in the Archive tier, you must first **rehydrate** it to an online tier, either Hot or Cool.

Availability Zones are unique physical locations within an Azure region.

Redundant Storage (LRS) is the default which maintains three copies of the data in the data center.

Geo-redundant storage (GRS) has cross-regional replication to protect against regional outages. Data is replicated synchronously three times in the primary region, then replicated asynchronously to the secondary region.

One of the benefits of **Azure SQL Data Warehouse** is that high availability is built into the platform.

Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider.

You can use **Power BI** to analyze and visualize data stored in **Azure Data Lake** and **Azure SQL Data Warehouse**.

The computer has **PowerShell Core 6.0**, but it doesn't have the **Azure CLI** installed. You need Azure PowerShell module in addition to PowerShell to run Azure commands, such as New-AzVM.

CosmosDB: mulity region and json

Azure Service Health provides the health/status of Azure service.

Azure Monitor - Provides Health/Status of your application using insights and logs

Azure Advisor does **not** provide recommendations on how to improve the security of an **Azure AD environment**.

Azure Databricks is a fast, easy, and collaborative **Apache Spark-based big data analytics service** designed for data science and data engineering.

You can have a read-only lock **and** a delete lock to the resource.

DDoS Protection Standard

Azure Application Insights vs azure advisor

Feature	Azure Application Insights	Azure Advisor
Purpose	Monitor and diagnose web application performance	Provide personalized recommendations for optimizing Azure resources
Data collected	Application performance data and usage insights	Resource usage patterns and configurations
Recommendations	Issues and performance bottlenecks in web applications	Recommendations for improving performance, security, and cost of Azure resources
Integration with other Azure services	Azure Monitor, Azure DevOps	Azure Security Center, Azure Backup
Target audience	Developers and DevOps teams	Azure administrators and IT teams

What can you associate Azure **Blueprints? Policies, ARM Templates, Role-based access controls**

Compare support plans: <https://azure.microsoft.com/en-us/support/plans/>

When deployed with a web application firewall (WAF), Azure DDoS Protection protects both at the **network layer** (Layer 3 and 4, offered by Azure DDoS Protection) and at the **application layer** (Layer 7, offered by a WAF).

You have a VM and want to encrypt its disks. First: **create key-vault**

A management group tree can support up to **six** levels of depth.

Configure **cloud tiering** so the most frequently accessed files are replicated locally, while infrequently accessed files are kept in the cloud until requested.

You can create custom, or **user-defined(static)**, routes in Azure to override Azure's default system routes, or to add more routes to a subnet's route table.

Azure service bus for messaging

The **Microsoft Azure Data Box** cloud solution lets you send terabytes of data into and out of Azure in a quick, inexpensive, and reliable way.

Azure Service Fabric is a **distributed systems platform** that makes it easy to package, deploy, and manage scalable and reliable microservices and containers.

UDR can Be created before Subnet

Azure Event Hubs — a scalable event ingestion and streaming service for big data and IoT scenarios

Azure Monitor - is a comprehensive monitoring solution for applications and infrastructure

Private preview – During this phase we invite a **few customers** to take part in

early access to new concepts and features. This phase does not include formal support.

Public preview – During this phase we allow **any customer** with the proper Azure AD license to evaluate the new feature.

Azure HDInsight is a managed, full-spectrum, **open-source** analytics service in the cloud for enterprises. With HDInsight, you can use open-source frameworks such as, Apache Spark, Apache Hive, LLAP, Apache Kafka, **Hadoop** and more, in your Azure environment.

Transfer data free if **in same data center**, otherwise free for 5gb.

Services	Answer Area
	IoT Hub A managed service that provides bidirectional communication between IoT devices and Azure
	IoT Central A fully managed software as a service (SaaS) solution to connect, monitor, and manage IoT devices at scale
	Azure Sphere A software and hardware solution that provides communication and security features for IoT devices

hu(b) = (b)idirectional

(c)entral = (c)onnect, monitor

(s)sphere = (s)ecurity

Third part -> market place

Services	Answer Area
	Azure Synapse Analytics A fully managed data warehouse that has integral security at every level of scale at no extra cost.
	Azure Cosmos DB A globally distributed database that supports NoSQL.
	Azure HDInsight Managed Apache Hadoop clusters in the cloud that enable you to process massive amounts of data.

Serverless Solutions

Answer Area

Azure Functions

Executes code:

Azure Functions

Azure Logic Apps

Is always stateful:

Azure Functions

Runs only in the cloud:

Azure Logic Apps

Wrong the second should be logic apps which is always stateful!!!

Answer Options

Answer Area

Azure SQL Database A managed relational cloud database service.

Azure SQL Synapse Analytics A cloud-based service that leverages massively parallel processing (MPP) to quickly run complex queries across petabytes of data in a relational database.

Azure Data Lake Analytics Can run massively parallel data transformation and processing programs across petabytes of data

Azure HDInsight An open-source framework for the distributed processing and analysis of big data sets in clusters

Relational: Sql

Massive MPP: Synapse

Messive PetaByte: Lake

OPen-source: Insight

Identity, governance, privacy, and compliance features

Azure cost management and Service Level Agreements