AZ-900 : Microsoft Certified: Azure Fundamentals

1. Provide the best video playback experience:
   - A **content delivery network (CDN)** is a distributed network of servers that can efficiently deliver web content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.
   - **Azure Content Delivery Network (CDN)** offers developers a global solution for rapidly delivering high bandwidth content to users by caching their content at strategically placed physical nodes across the world.

2. Services
   - ✓ **Azure Repos** - Azure service provides a set of version control tools to manage code
   - ✓ **PowerApps** lets you quickly build business applications with little or no code.
   - ✓ **Azure Databricks** is an Apache Spark-based analytics service.
   - ✓ **Azure Machine Learning**
     - Uses past training to provide predictions that have high probability
     - It should use to build, test and deploy predictive analytics solution
   - ✓ **Serverless Computing:**
     - Azure Logic Apps is a cloud service that helps you schedule, automate, and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations.
     - Azure Functions – Provides serverless computing functionalities
   - ✓ **Firewall:**
     - Azure Firewall
       - It can be used to grant or deny access based on originating IP address
     - network security group (NSG)
   - ✓ **Compliance:**
     - Microsoft Compliance Manager (Preview) is a free workflow-based risk assessment tool that lets you track, assign, and verify regulatory compliance activities related to Microsoft cloud services.

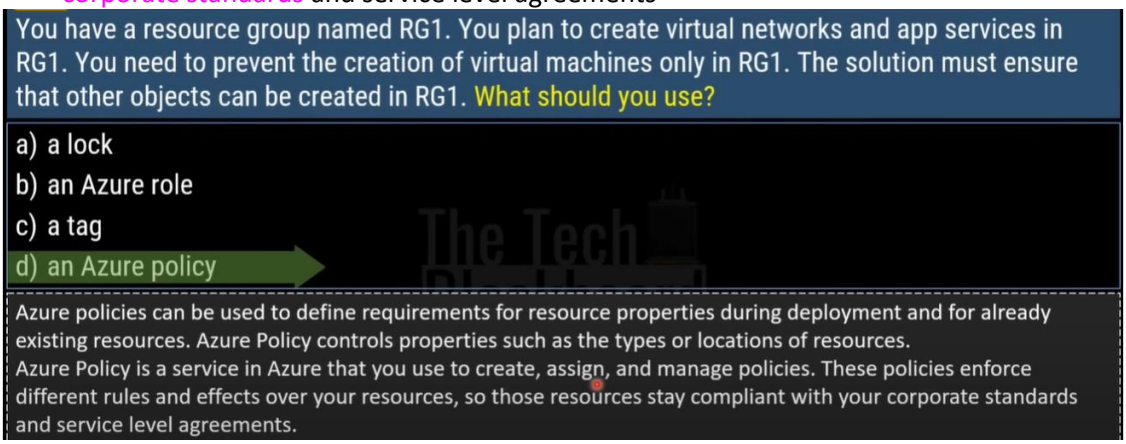
       Compliance Manager is used to meet compliance obligations, such as GDPR, ISO, NIST, and HIPAA.

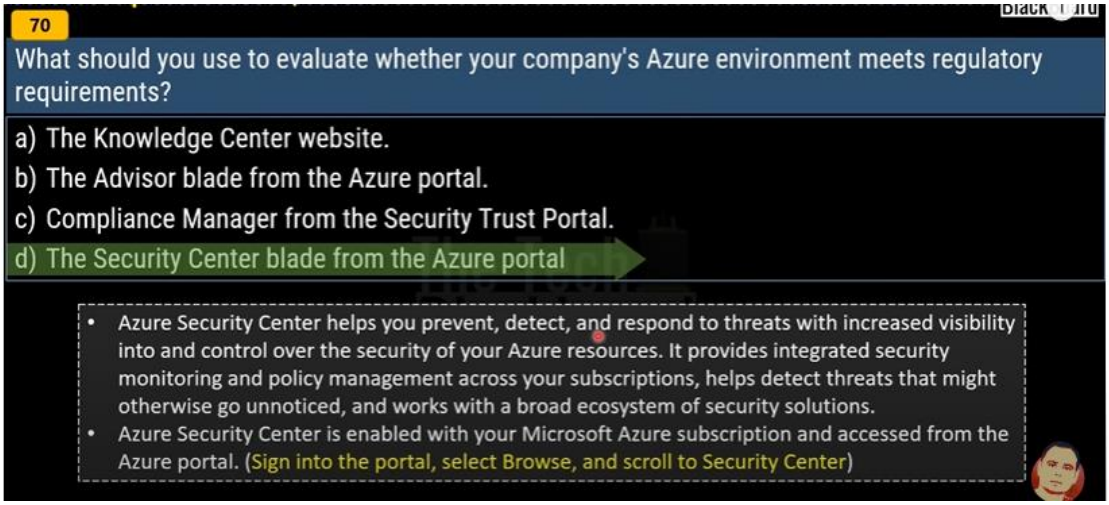
       The Azure Compliance documents provides detailed documentation on Azure legal and regulatory standards and compliance. You can also seen the reference blueprints that can be applied directly to your azure subscription

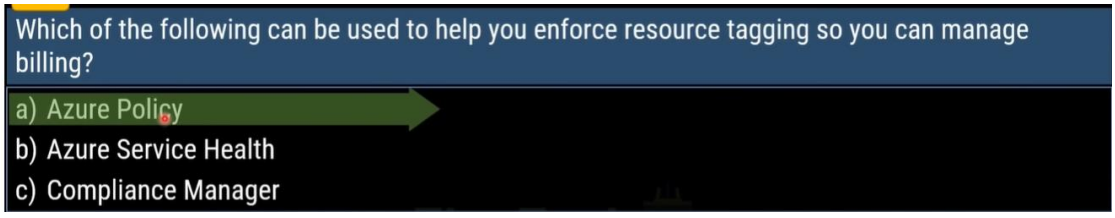
     - Azure Trust Center - whether Azure complies with the company's regional requirements.

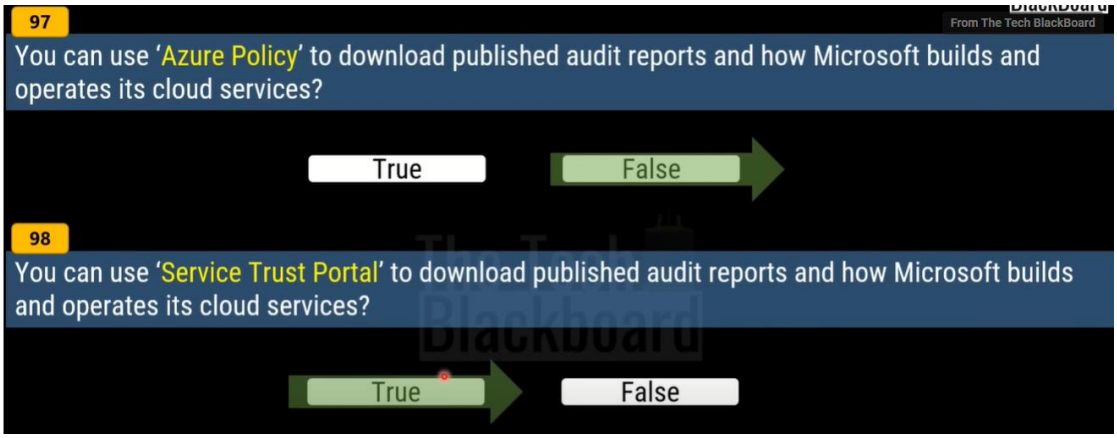
       The Service Trust Portal is a web portal that provides all kinds of content and tools that pertain to Microsoft security, privacy, and compliance practices. The Service Trust Portal also features third-party audits of many of Microsoft's online services, along with information on how Microsoft's services can help you maintain and track compliance with laws, regulations, and other standards.

- Azure Policy - is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements









What is Azure policy initiative?

a) a collection of policy definitions

b) collection of Azure policy definition assignments

c) group of Azure Blue Prints definition

d) group of role based access control (RBAC)?

- ✓ Data from millions of sensors
  - Azure IoT Hub – Process Data from millions of sensors
  - Azure Advanced Threat Protection (ATP) - monitor threats by using sensors
  - Azure Data Lake – It can be used to store data from devices
  - Azure Notification Hubs – It can be use for sending millions of notifications to iOs, Android, Windows, Kindle working on APN(Apple Push Notification service), GSM (Google cloud mobile)

- ✓ Azure Active Directory (AD) Identity Protection -
  - To enforce MFA based on a condition. Azure AD join only applies to Windows 10 devices
  - Azure AD – an application connect to retrieve security tokens
  - Azure AD Identity Protection includes two risk policies: sign-in risk policy and user risk policy. A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.

Azure AD authenticates users and provides access tokens. An access token is a security token that is issued by an authorization server. Security Token is not a Secret. Password, Private Keys, Certificates, etc., are secrets. Tokens are generated when request is made and they change with almost each request and valid for short duration only. So, there is no point in protecting the token by storing it in the vault to use it when needed, it is not a static value.

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in:

- External resources: such as Microsoft Office 365, the Azure portal, and thousands of other SaaS applications.
- Internal resources: such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

- ✓ Azure Information Protection encrypt
  - Documents and email messages. You use Azure Information Protection labels to apply classification to documents and emails
  - It Automatically add a watermark to Microsoft Word documents that contain credit card information

- ✓ General Data Protection Regulation – defines data protection and privacy rules

- ✓ Azure Blueprint –
  - We can add an ARM template to an Azure Blueprint
  - You can use an Azure blueprint to grant permission to a resource

- ✓ Azure Log Analytics – use to correlate events from multiple resources into a centralized repository

- ✓ Edge Computing – It allows customers to run VMs, container and data services at edge locations

✓ DevTest Labs: creates labs consisting of pre-configured bases or Azure Resource Manager templates.
- Quickly provision Windows and Linux environments by using reusable templates and artifacts.
- Easily integrate your deployment pipeline with DevTest Labs to provision on-demand environments.
- Scale up your load testing by provisioning multiple test agents and create pre-provisioned environments for training and demos.

✓ Azure Monitor:
- What can you use to automatically send an alert if an administrator stops an Azure virtual machine? Azure Monitor

Statements	Yes	No
Azure Monitor can monitor the performance of on-premises computers.	○	○
Azure Monitor can send alerts to Azure Active Directory security groups.	○	○
Azure Monitor can trigger alerts based on data in an Azure Log Analytics workspace.	○	○

Statements	Yes	No
You can configure the Azure Active Directory (Azure AD) activity logs to appear in Azure Monitor.	○	○
From Azure Monitor, you can monitor resources across multiple Azure subscriptions.	○	○
From Azure Monitor, you can create alerts.	○	○

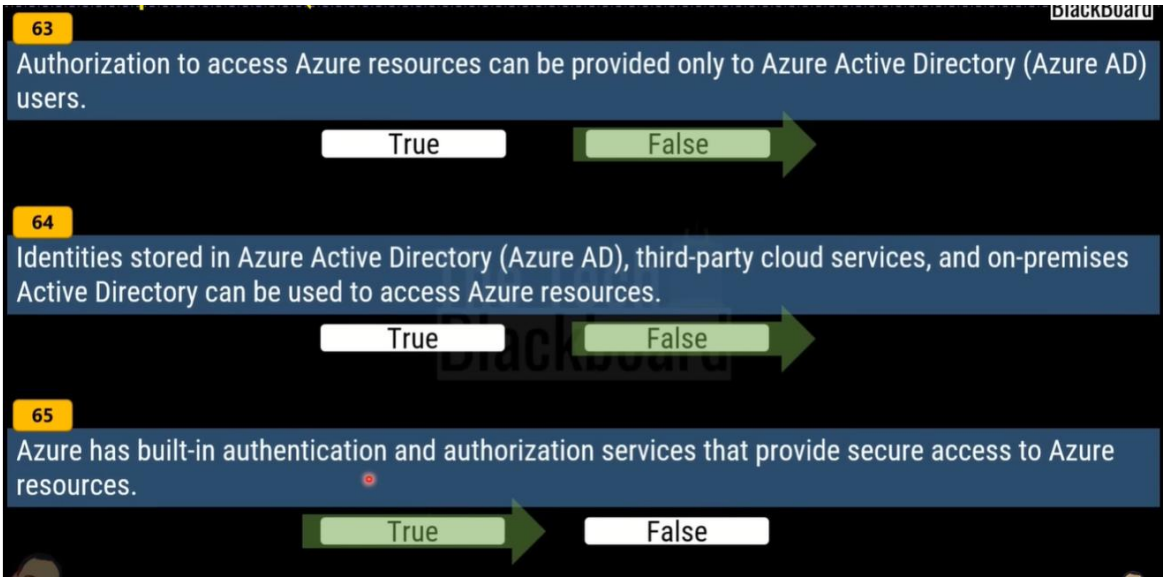
✓ Azure Service Health:
- Azure Service Health consists of three components: Azure Status, Azure Service Heath and Azure Resource Health.
- Azure service health provides a personalized view of the health of the Azure services and regions you're using.
- This is the best place to look for service impacting communications about outages, planned maintenance activities, and other health advisories because the authenticated Azure Service Health experience knows which services and resources you currently use.

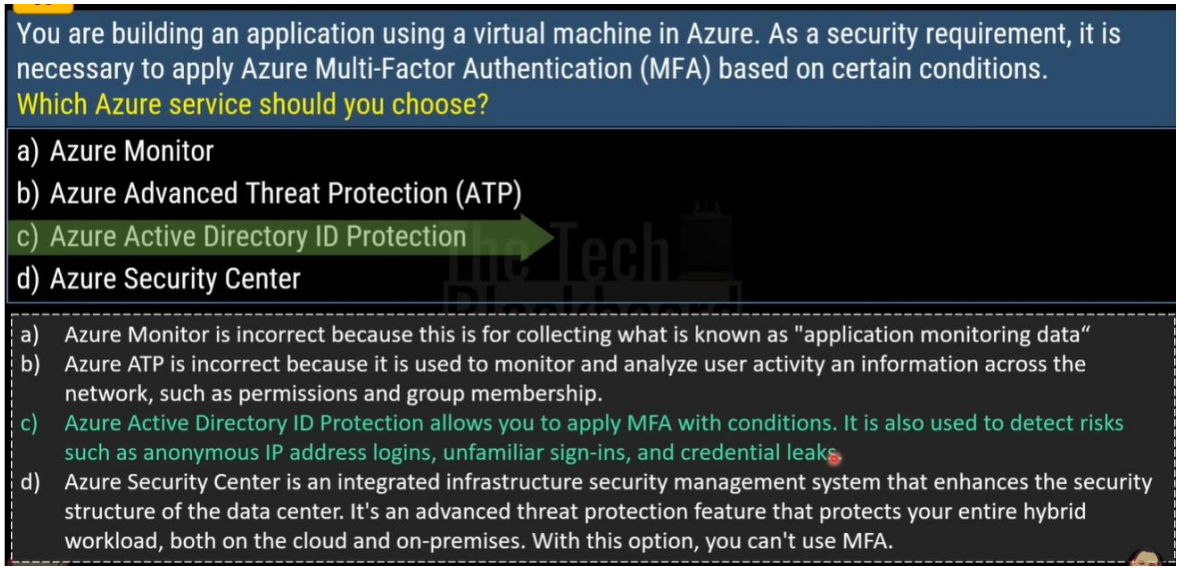
Statements	Yes	No
From Azure Service Health, an administrator can view the health of all the services in an Azure environment.	○	○
From Azure Service Health, an administrator can create a rule to be alerted if an Azure service fails.	○	○
From Azure Service Health, an administrator can prevent a service failure	○	○

3. Lift and Shift: IAAS

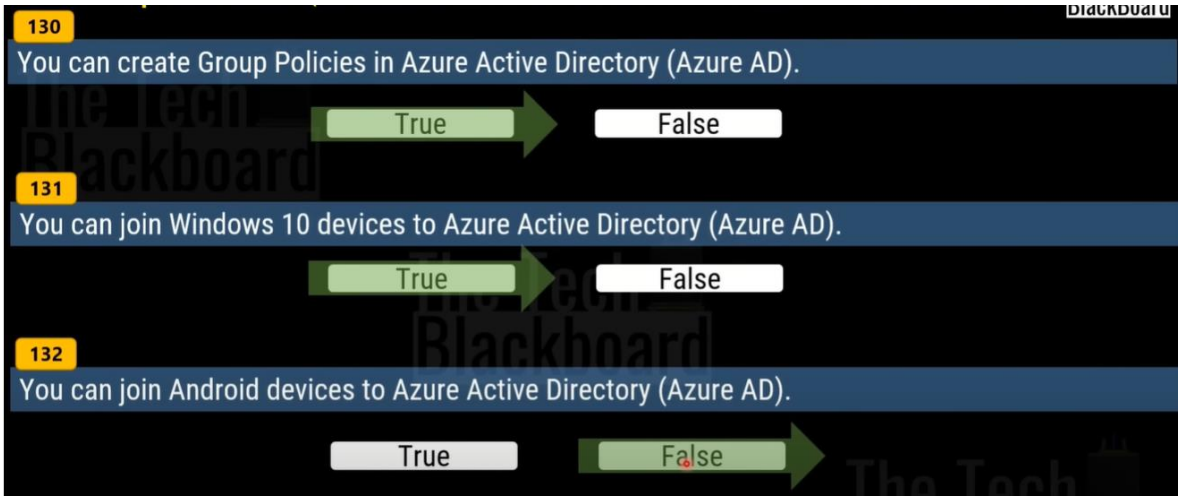
4. **Azure Active Directory (Azure AD) :**

- third-party cloud services and on-premises Active Directory can be used to access Azure resources. This is known as 'federation'.
- Azure Active Directory (Azure AD) is a centralized identity provider in the cloud. This is the primary built-in authentication and authorization service to provide secure access to Azure resources and Microsoft 365.
- Identities stored in an on-premises Active Directory can be sync to Azure Active Directory (Azure AD)
- User accounts in Azure Active Directory can be assigned multiple licenses for different Azure or Microsoft 365 services.
- Azure AD authenticates users and provides access tokens. An access token is a security token that is issued by an authorization server





- User accounts in Azure Active Directory can be assigned multiple licenses for different Azure or Microsoft 365 services



- Azure AD Identity Protection – To ensure that when Azure AD users connect to Azure AD from the internet by using an anonymous IP address, the users are prompted automatically to change their password

5. **Resource Lock:**
   - **CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.
   - **ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the **Reader** role.

Statements	Yes	No
An Azure resource can have multiple Delete locks.	○	○
An Azure resource inherits locks from its resource group.	○	○
If an Azure resource has a Read-only lock, you can add a Delete lock to the resource.	○	○

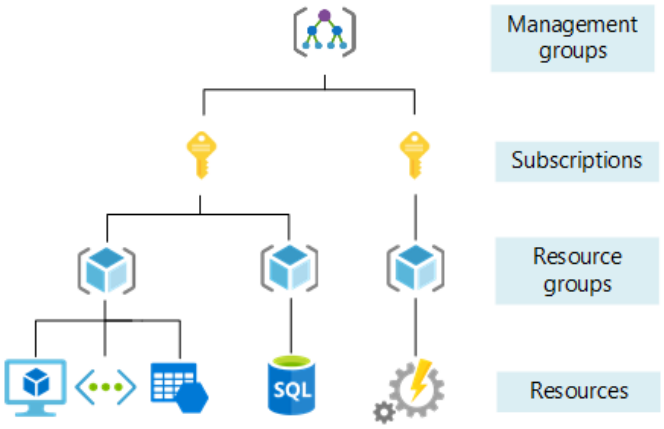
6. The Microsoft Privacy Statement explains what personal data Microsoft processes, how Microsoft processes the data, and the purpose of processing the data

7. Authentication is the process of verifying a user's credentials.

8. **Support plans:**
   - Premier, Professional Direct and standard Plans - Support Engineers via email or phone is available
   - The Premier support plan provides customer specific architectural support such as design reviews, performance tuning, configuration and implementation assistance delivered by Microsoft Azure technical specialists.

9. **Management levels and hierarchy**

   Azure provides four levels of management: management groups, subscriptions, resource groups, and resources. The following diagram shows the relationship between these levels.

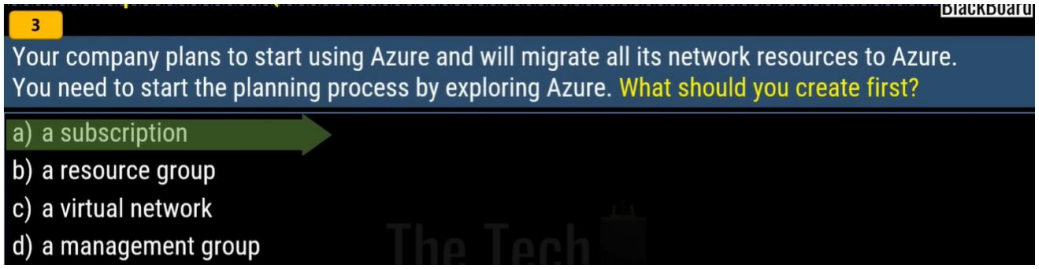


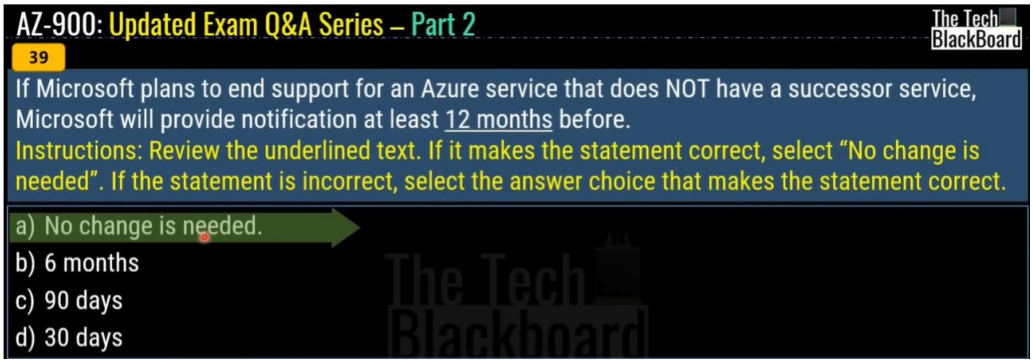
- **Management groups** help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions that are applied to the management group.
- **Subscriptions** logically associate user accounts with the resources that they create. Each subscription has limits or quotas on the amount of resources that it can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, and projects.
- **Resource groups** are logical containers where you can deploy and manage Azure resources like web apps, databases, and storage accounts.
- **Resources** are instances of services that you can create, such as virtual machines, storage, and SQL databases.

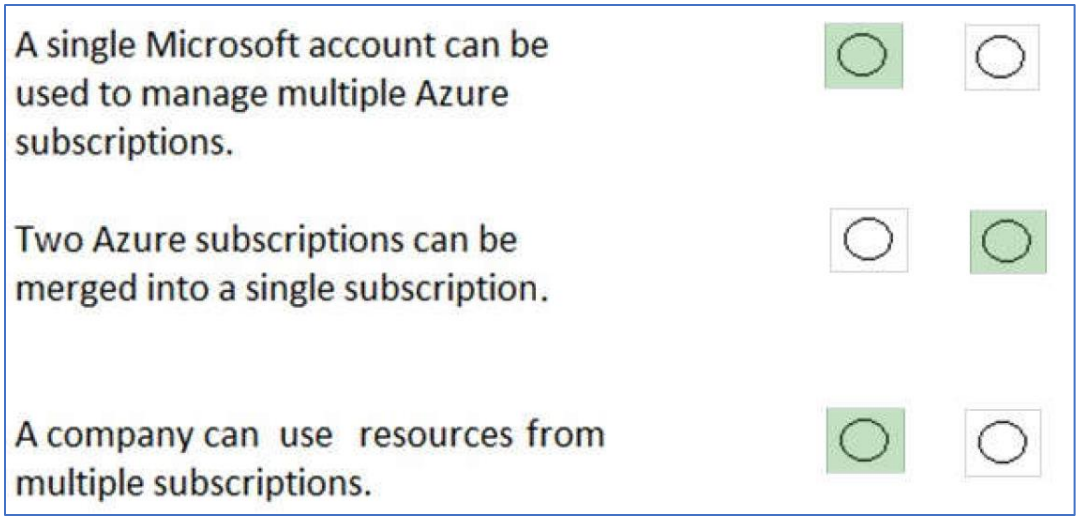
10. **PAAS:**
    - **SQL Server**
    - **Cosmos DB:**
        i. Can add data concurrently from multiple regions
        ii. Can store JSON documents

Practice Questions

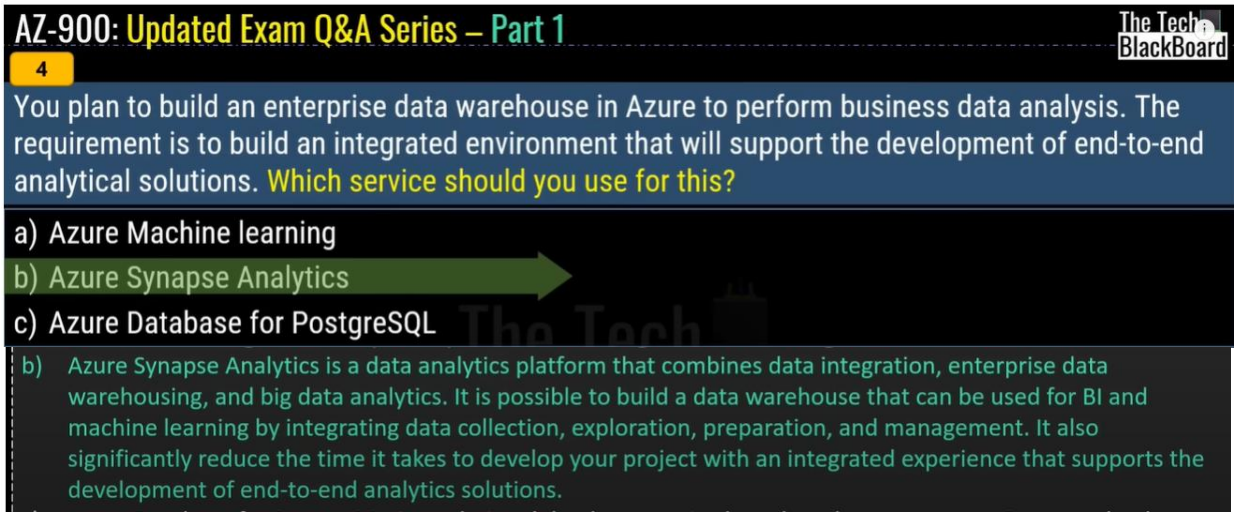
1. **Subscription**





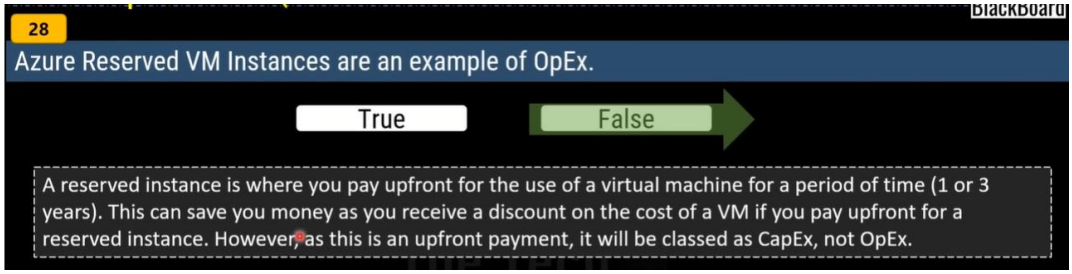


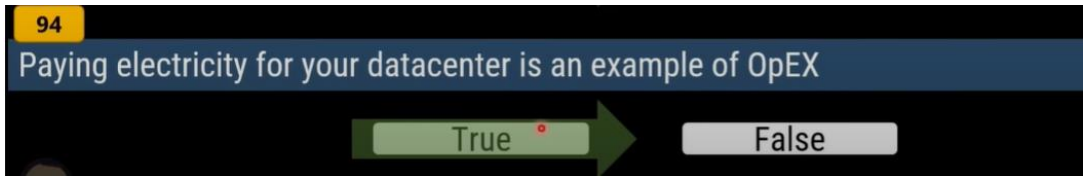
2. **Azure Synapse Analytics**



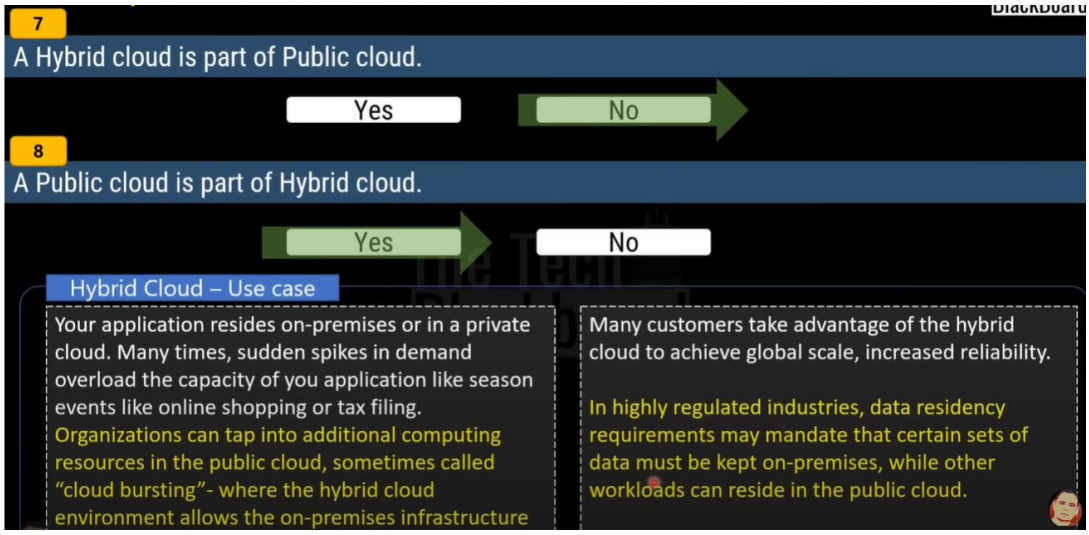
- Azure Synapse Analytics – Provides a cloud-based Enterprise Data Warehouse (EDW). Data analytics Platform

3. **OpEx and CapEx**

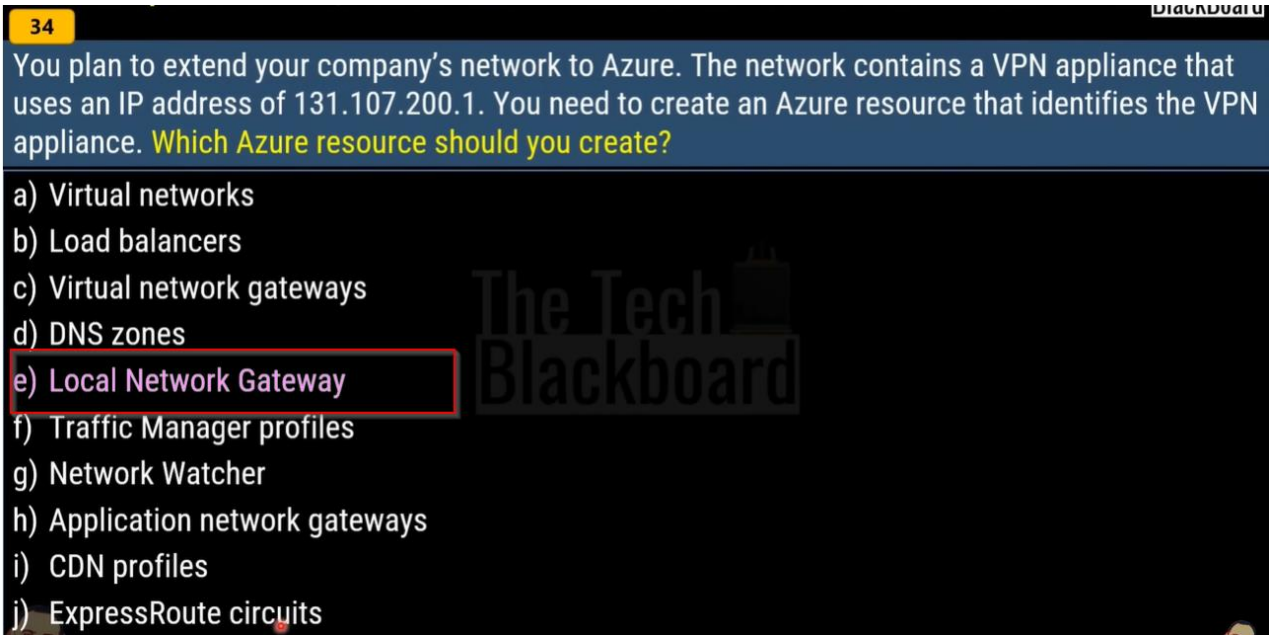


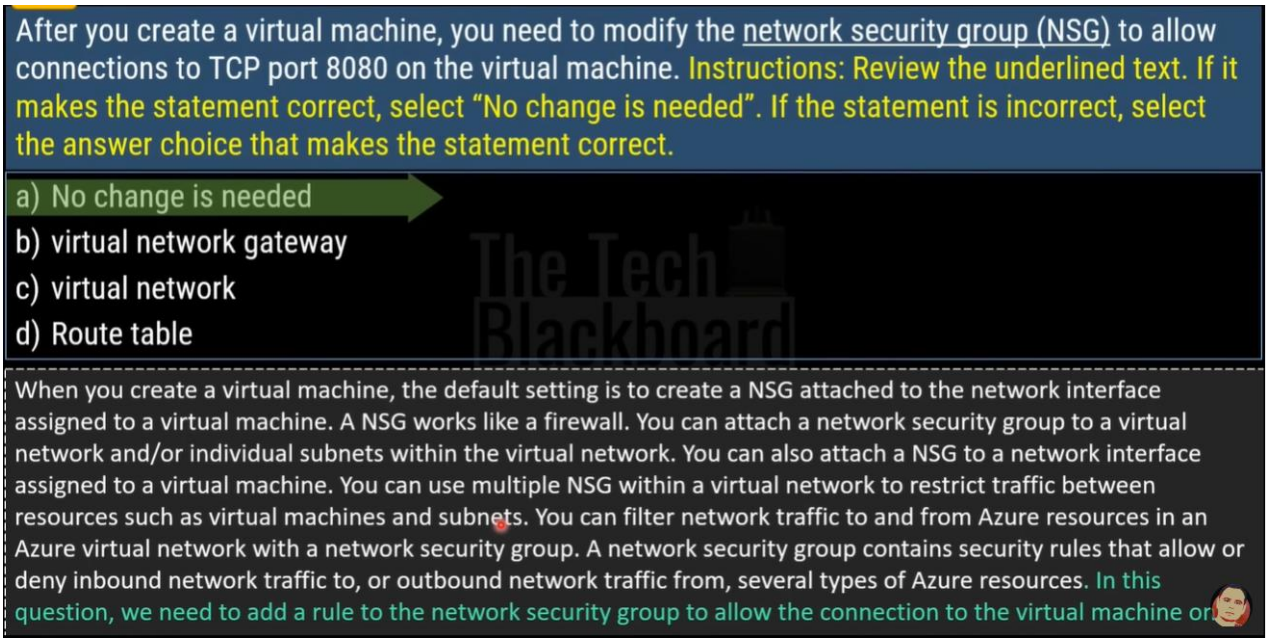


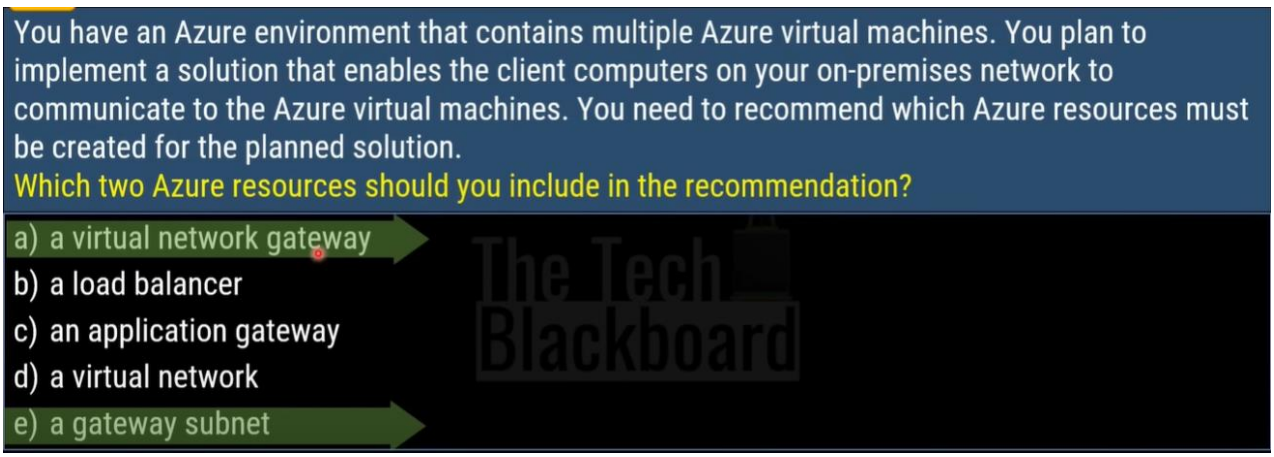
4. **Hybrid Cloud**



5. **Network**


34
You plan to extend your company's network to Azure. The network contains a VPN appliance that uses an IP address of 131.107.200.1. You need to create an Azure resource that identifies the VPN appliance. Which Azure resource should you create?
a) Virtual networks
b) Load balancers
c) Virtual network gateways
d) DNS zones
e) Local Network Gateway
f) Traffic Manager profiles
g) Network Watcher
h) Application network gateways
i) CDN profiles
j) ExpressRoute circuits


After you create a virtual machine, you need to modify the network security group (NSG) to allow connections to TCP port 8080 on the virtual machine. Instructions: Review the underlined text. If it makes the statement correct, select "No change is needed". If the statement is incorrect, select the answer choice that makes the statement correct.
a) No change is needed
b) virtual network gateway
c) virtual network
d) Route table
When you create a virtual machine, the default setting is to create a NSG attached to the network interface assigned to a virtual machine. A NSG works like a firewall. You can attach a network security group to a virtual network and/or individual subnets within the virtual network. You can also attach a NSG to a network interface assigned to a virtual machine. You can use multiple NSG within a virtual network to restrict traffic between resources such as virtual machines and subnets. You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. 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. In this question, we need to add a rule to the network security group to allow the connection to the virtual machine or


You have an Azure environment that contains multiple Azure virtual machines. You plan to implement a solution that enables the client computers on your on-premises network to communicate to the Azure virtual machines. You need to recommend which Azure resources must be created for the planned solution.
Which two Azure resources should you include in the recommendation?
a) a virtual network gateway
b) a load balancer
c) an application gateway
d) a virtual network
e) a gateway subnet

Use DDoS Protection service in combination with a web application firewall (WAF) for protection both at the ---------- (layer 3 and 4, offered by DDoS Protection Standard) and at the ---------- (layer 7, offered by a WAF).

a) Physical security
b) Identity and access
c) Perimeter
d) Network
e) Compute
f) Application
g) Data

By creating additional resource groups in an Azure subscription, additional costs are incurred.	○	○
By copying several gigabits of data to Azure from an on-premises network over a VPN, additional data transfer costs are incurred.	○	○
By copying several GB of data from Azure to an on-premises network over a VPN, additional data transfer costs are incurred.	○	○

6. **SLA:**

40

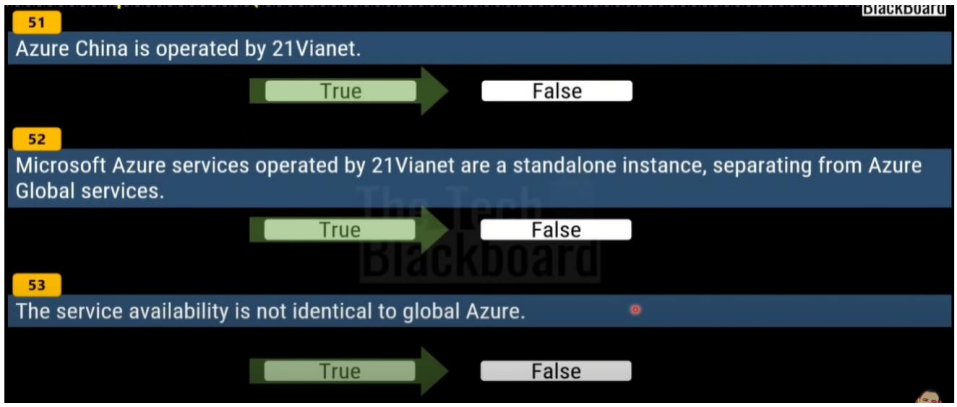
You have an application that is comprised of an Azure web app that has a Service Level Agreement (SLA) of 99.95 percent and an Azure SQL database that has an SLA of 99.99 percent. The composite SLA for the application is the product of both SLAs, which equals 99.94 percent.
Instructions: Review the underlined text. If it makes the statement correct, select "No change is needed". If the statement is incorrect, select the answer choice that makes the statement correct.

a) No change is needed.
b) the lowest SLA associated to the application, which is 99.95 percent
c) the highest SLA associated to the application, which is 99.99 percent
d) the difference between the two SLAs, which is 0.05 percent

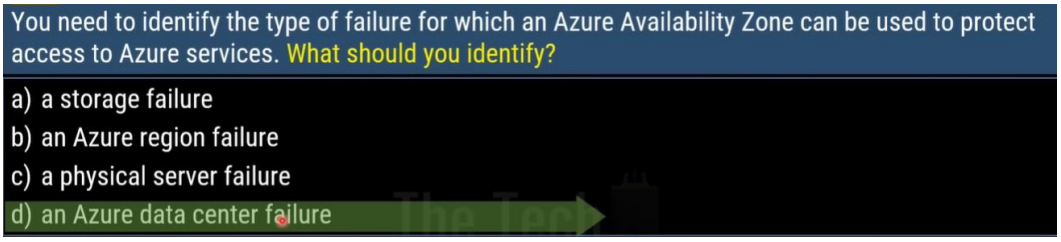
99.95% × 99.99% = 99.94%

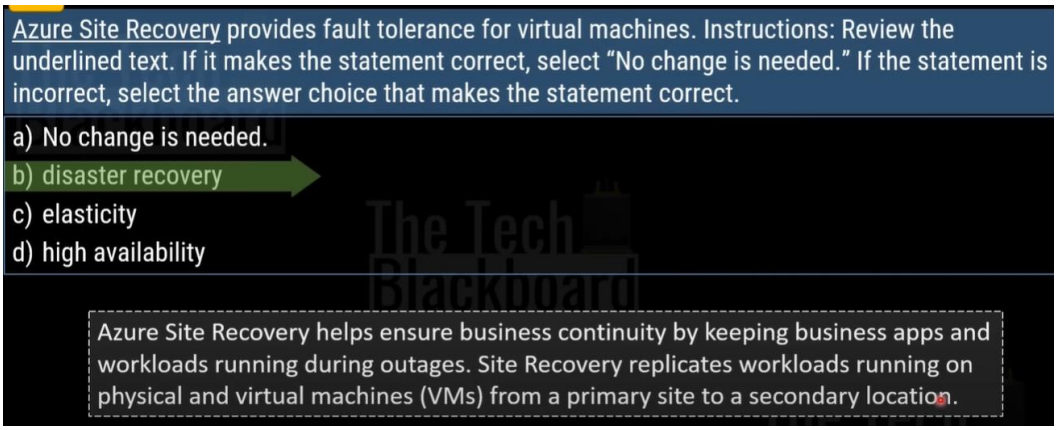
Statements	Yes	No
A Standard support plan is included in an Azure free account.	○	○
A Premier support plan can only be purchased by companies that have an Enterprise Agreement (EA).	○	○
Support from MSDN forums is only provided to companies that have a pay-as-you-go subscription.	○	○

7. **Availability:**



- Azure Germany can be used by legal residents of Germany only – any user or enterprise that requires its data to reside in Germany
- Azure Government is for USA
- Which two types of customer are eligible to use Azure Government to Develop a cloud solution?
  Ans: US Government entity and US government contractor





Statements	Yes	No
North America is represented by a single Azure region.	○	○
Every Azure region has multiple datacenters.	○	○
Data transfers between Azure services located in different Azure regions are always free.	○	○

An Availability Zone in Azure has physically separate locations [across two continents.]
Instructions: Review the underlined text. If it makes the statement correct, select "No change is needed." If the statement is incorrect, select the answer choice that makes the statement correct.

a) No change is needed.
b) within a single Azure region
c) within multiple Azure regions
d) within a single Azure datacenter

Availability Zones is a high-availability offering that protects your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region.

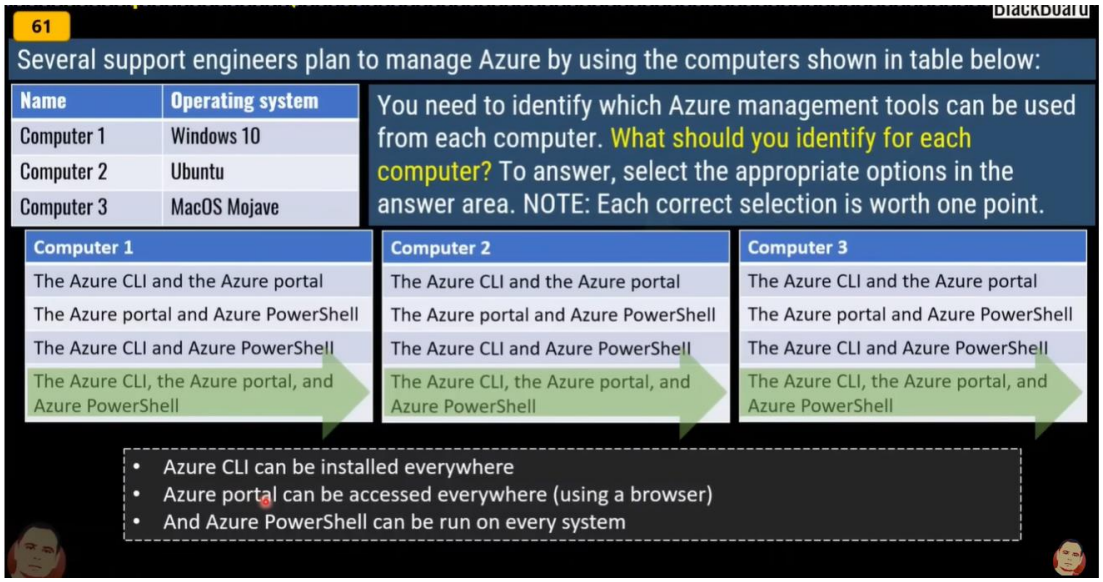
8. **Azure Advisor:**

57
Azure Advisor provides recommendations on how to improve the security of an Azure Active Directory (Azure AD) environment.
True False

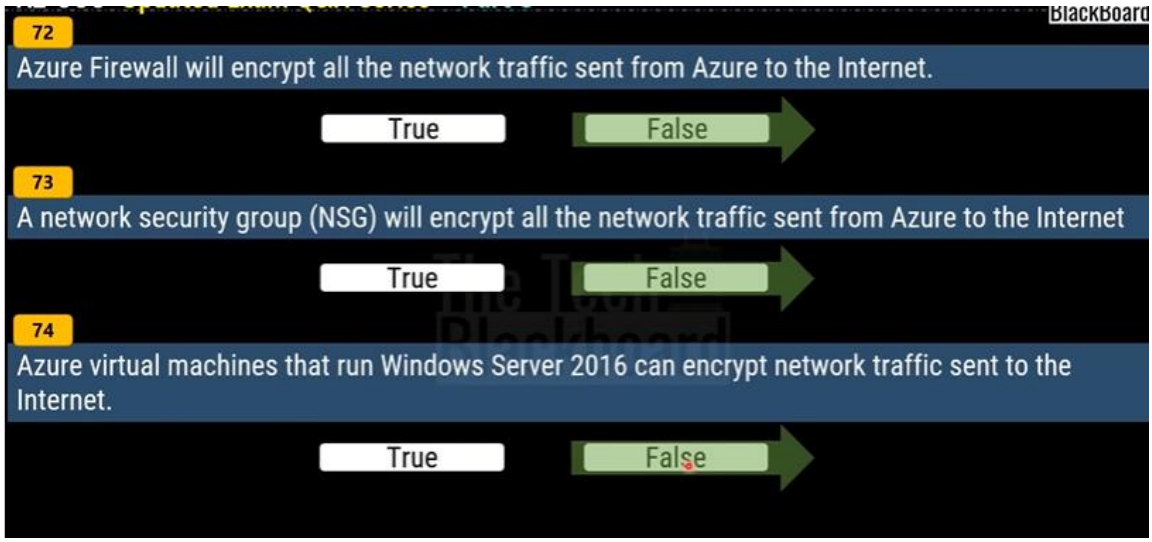
58
Azure Advisor provides recommendations on how to configure the network settings on Azure virtual machines.
True False

59
Azure Advisor provides recommendations on how to reduce the cost of running Azure virtual machines.
True False

9. Azure and Operating System:



10. Security (Azure Firewall, Network Security Group, DDoS)



Azure Firewall	Azure Network Security Groups
Azure Firewall is a **robust service** and a fully managed firewall.	Azure Network Security Group is a **basic firewall**.
It is loaded with tons of features to **ensure maximum protection** of your resources.	This solution is used to **filter traffic** at the network layer.
It can **analyze and filter** L3, L4 traffic, and L7 application traffic.	No such facility is available in Azure NSG.
Azure Firewall provides full support to application **FQDN tags**.	This feature is not available in Azure NSG.
It allows you to **mask the source and destination** network addresses	This feature is missing here.
It offers a **threat intelligence-based filtering** option.	This feature is missing in NSG.

78

You need to configure an Azure solution that meets the following requirements:

- Secures websites from attacks.
- Generates reports that contain details of attempted attacks.

What should you include in the solution?

a) Azure Firewall.
b) A network security group (NSG).
c) Azure Information Protection.
d) DDoS protection.

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns facing customers that are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

NSG can be applied to what level?

a) Subscription level
b) Subnet level
c) Management group level
d) Virtual Machine / NIC Level

NSG is mainly used for filtering traffic in and out of the Virtual Network (VNET) in Azure.

NSG can be applied at two levels : -

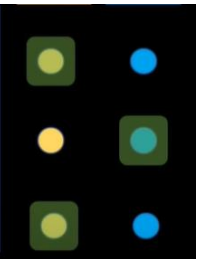
a) **Subnet**: If you implement NSG at the subnet level all VMs in that subnet will be applied with the rules imposed in NSG.
b) **VM / NIC**: If you apply at VM/NIC level , the rule will be implemented only for that VM.

NIC – Network Interface Card

a) You can associate a network security group (NSG) to a virtual network subnet.

b) You can associate a network security group (NSG) to a virtual network.

c) You can associate a network security group (NSG) to a network interface.



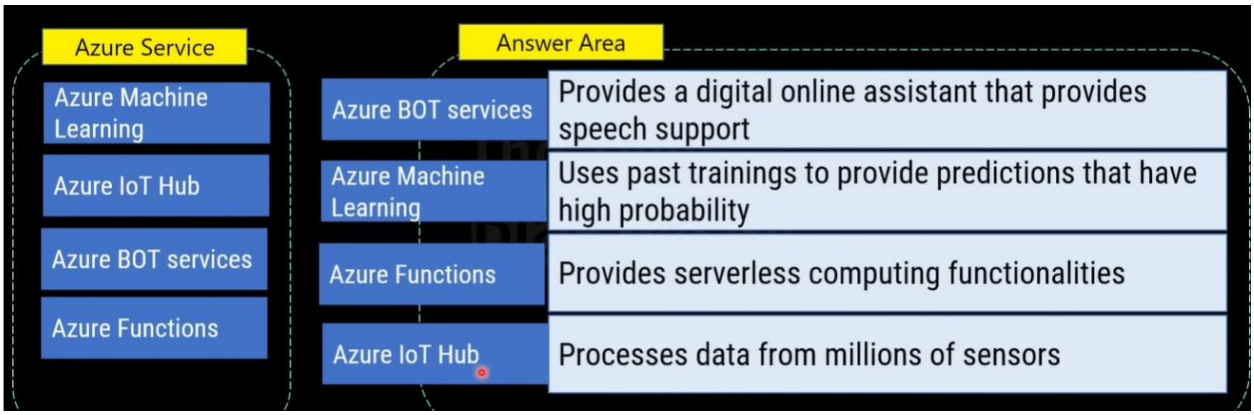
You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine

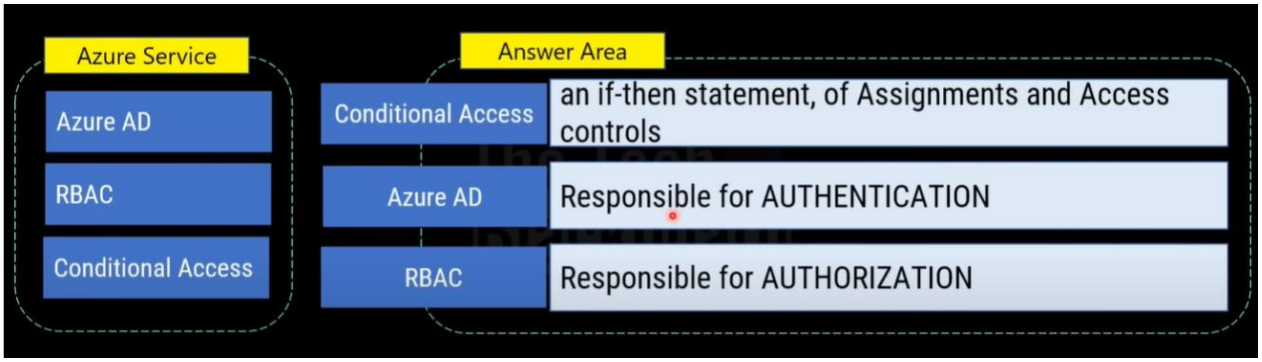
133

Which resources can be used as a source for a Network security group inbound security rule?

a) Application security groups only
b) IP Address only
c) Service Tags only
d) IP Addresses, Service tags and Application security groups

11. Match the following:





****Azure role-based access control (**Azure RBAC**) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Correct Answer:

Answer Options	Answer Area	
Azure Advisor	Azure DevOps	An integrated solution for the deployment of code
Azure Cognitive Services	Azure Advisor	A tool that provides guidance and recommendations to improve an Azure environment
Azure Application Insights	Azure Cognitive Services	A simplified tool to build intelligent Artificial Intelligence (AI) applications
Azure DevOps	Azure Application Insights	Monitors web applications

Correct Answer:

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

Services	Answer Area	
	Azure virtual machines	Provide operating system virtualization
	Azure Container Instances	Provide portable environment for virtualized applications
	Azure App Service	Used to build, deploy, and scale web apps
	Azure Functions	Provide a platform for serverless code

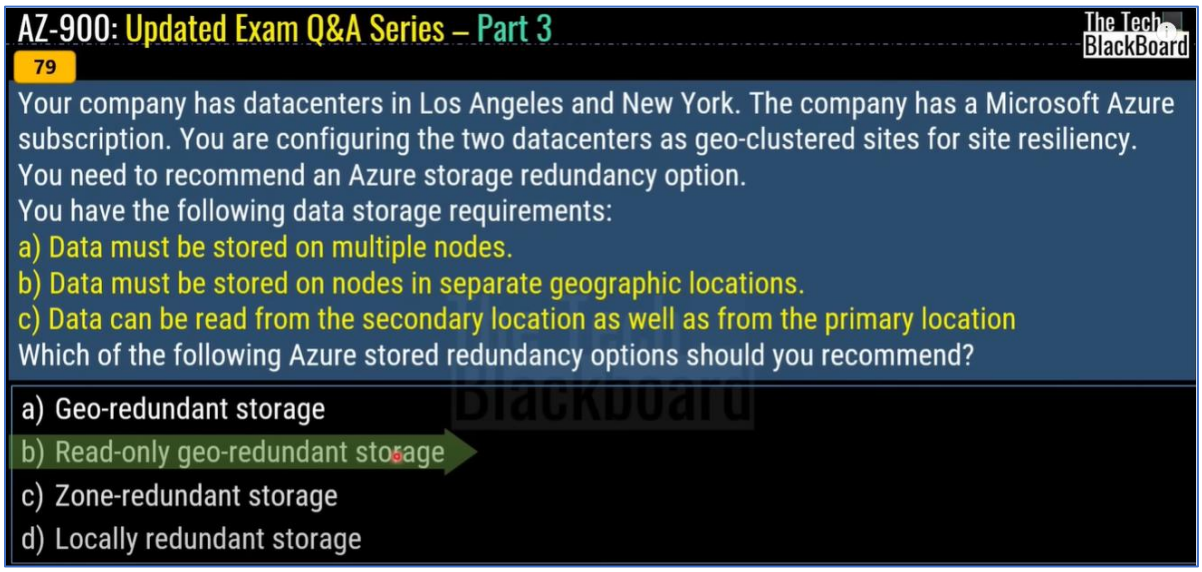
Azure Databricks	Azure Functions	Provides the platform for serverless code
Azure Functions	Azure Databricks	A big data analysis service for machine learning
Azure App Service	Azure Application Insights	Detects and diagnoses anomalies in web apps
Azure Application Insights	Azure App Service	Hosts web apps

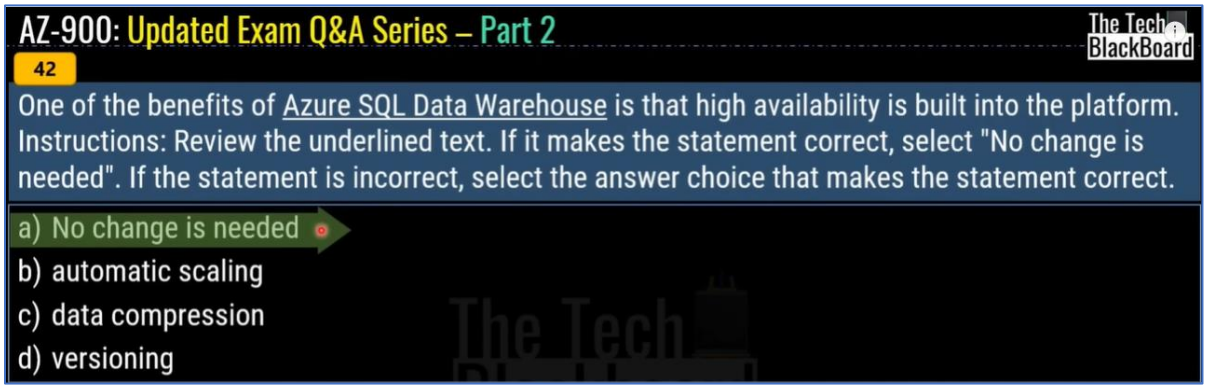
Statements	Yes	No
Azure Security Center can monitor Azure resources and on-premises resources.	○	○
All Azure Security Center features are free.	○	○
From Azure Security Center, you can download a Regulatory Compliance report.	○	○

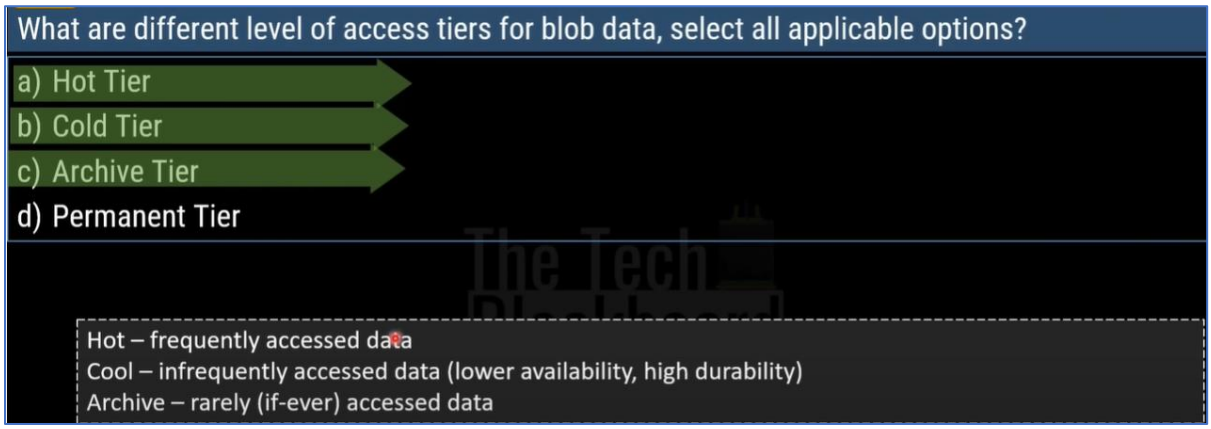
Statements	Yes	No
In Azure Active Directory Premium P2, at least 99.9 percent availability is guaranteed.	○	○
The Service Level Agreement (SLA) for Azure Active Directory Premium P2 is the same as the SLA for Azure Active Directory Free.	○	○
All paying Azure customers receive a credit if their monthly uptime percentage is below the guaranteed amount in the Service Level Agreement (SLA).	○	○

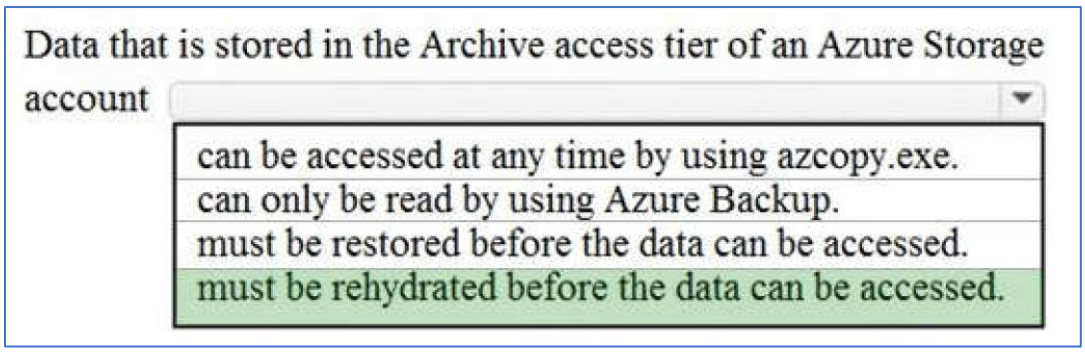
Azure Government	ISO	An organization that defines international standards across all industries.
GDPR	NIST	An organization that defines standards used by the United States government.
ISO	GDPR	A European policy that regulates data privacy and data protection.
NIST	Azure Government	A dedicated public cloud for federal and state agencies in the United States.

12. Storage


AZ-900: Updated Exam Q&A Series – Part 3
The Tech BlackBoard
79
Your company has datacenters in Los Angeles and New York. The company has a Microsoft Azure subscription. You are configuring the two datacenters as geo-clustered sites for site resiliency.
You need to recommend an Azure storage redundancy option.
You have the following data storage requirements:
a) Data must be stored on multiple nodes.
b) Data must be stored on nodes in separate geographic locations.
c) Data can be read from the secondary location as well as from the primary location
Which of the following Azure stored redundancy options should you recommend?
a) Geo-redundant storage
b) Read-only geo-redundant storage
c) Zone-redundant storage
d) Locally redundant storage

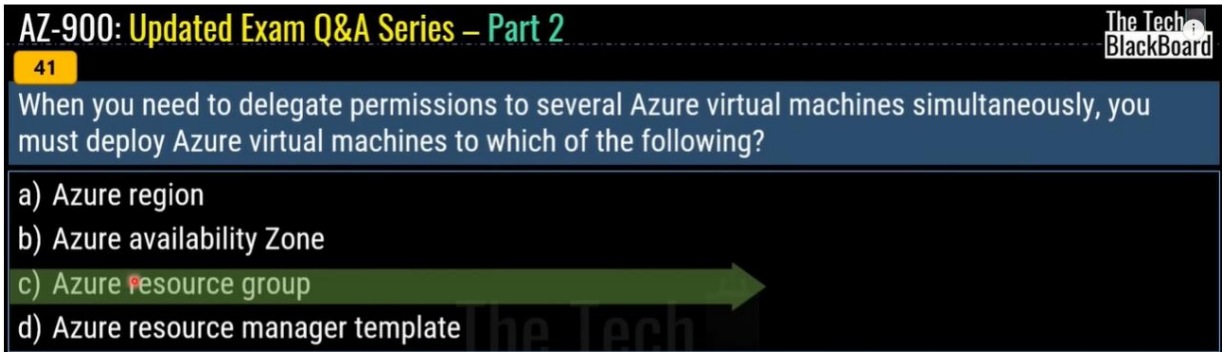

AZ-900: Updated Exam Q&A Series – Part 2
The Tech BlackBoard
42
One of the benefits of Azure SQL Data Warehouse is that high availability is built into the platform.
Instructions: Review the underlined text. If it makes the statement correct, select "No change is needed". If the statement is incorrect, select the answer choice that makes the statement correct.
a) No change is needed
b) automatic scaling
c) data compression
d) versioning

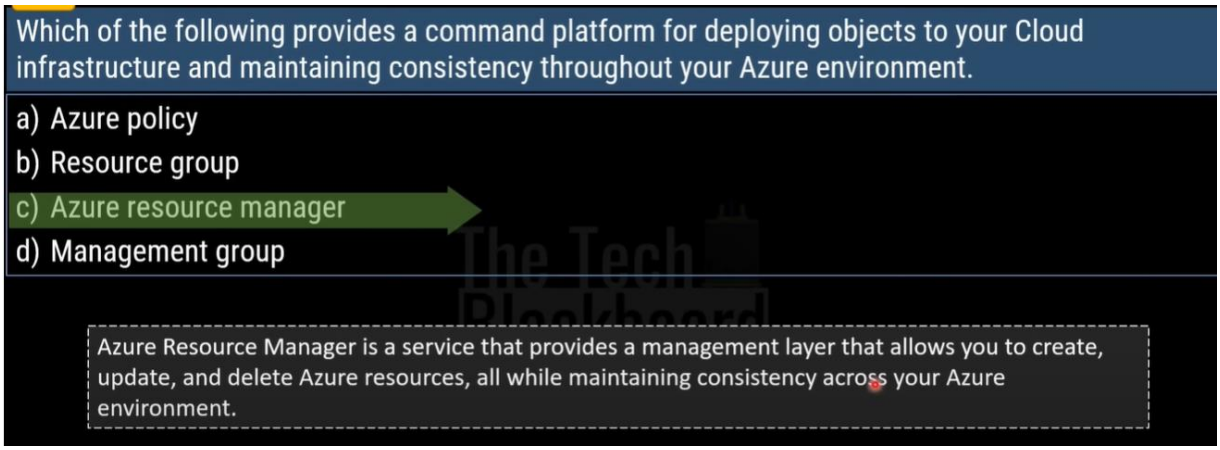

What are different level of access tiers for blob data, select all applicable options?
a) Hot Tier
b) Cold Tier
c) Archive Tier
d) Permanent Tier
Hot – frequently accessed data
Cool – infrequently accessed data (lower availability, high durability)
Archive – rarely (if-ever) accessed data


Data that is stored in the Archive access tier of an Azure Storage account
can be accessed at any time by using azcopy.exe.
can only be read by using Azure Backup.
must be restored before the data can be accessed.
must be rehydrated before the data can be accessed.

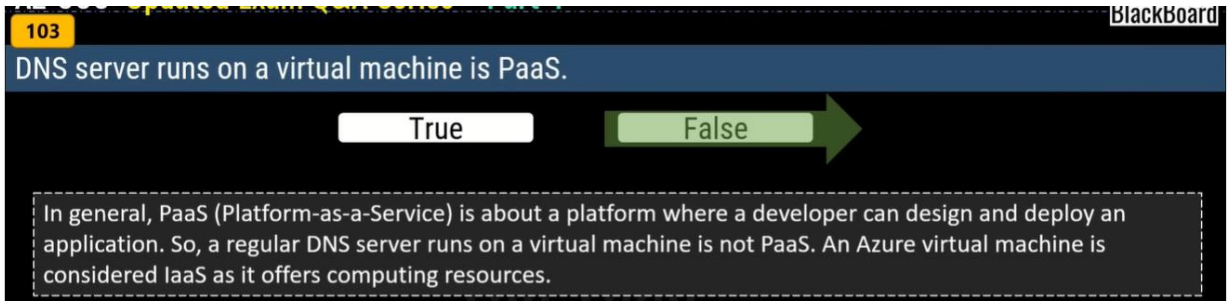
Statements	Yes	No
Data that is stored in an Azure Storage account automatically has at least three copies.	○	○
All data that is copied to an Azure Storage account is backed up automatically to another Azure data center.	○	○
An Azure Storage account can contain up to 2 TB of data and up to one million files.	○	○

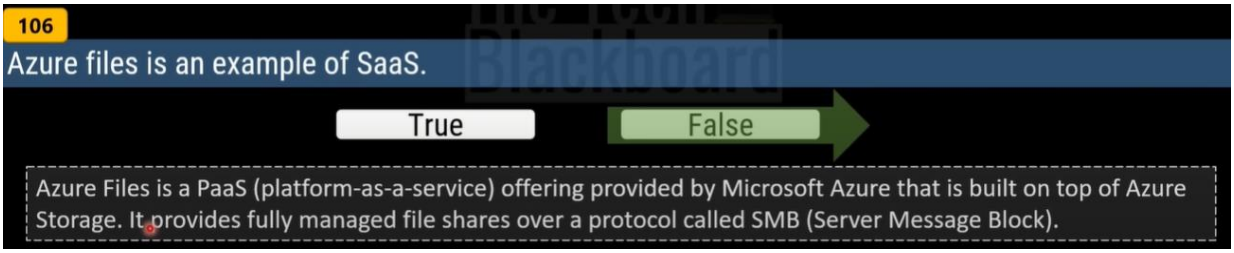
13. ARM (Azure Resource Manager)



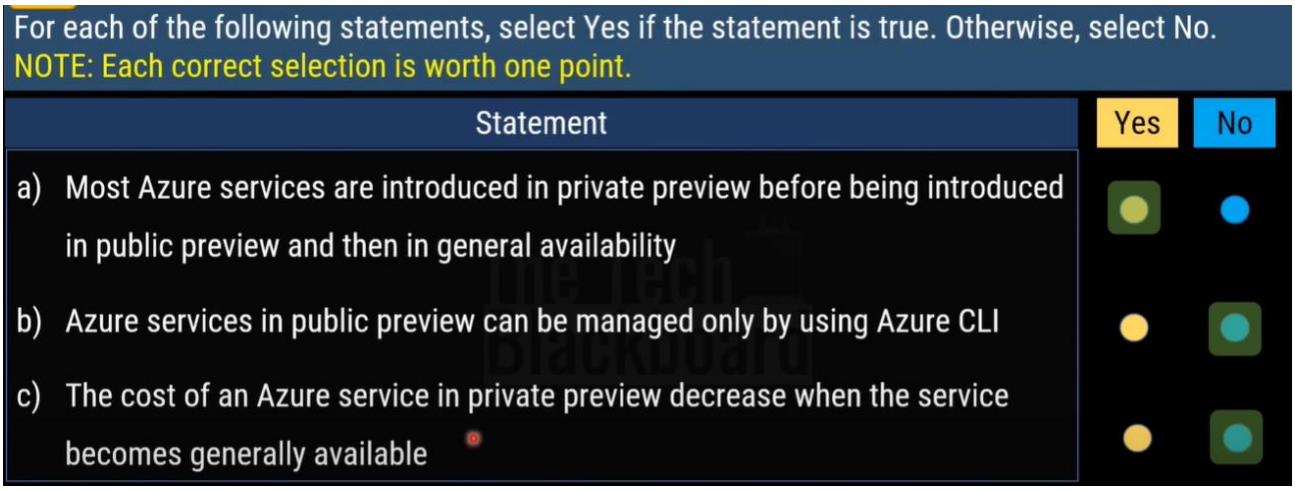


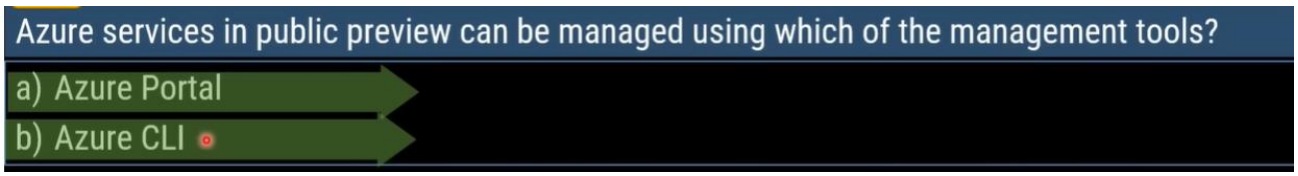
14. IAAS vs PAAS vs SAAS





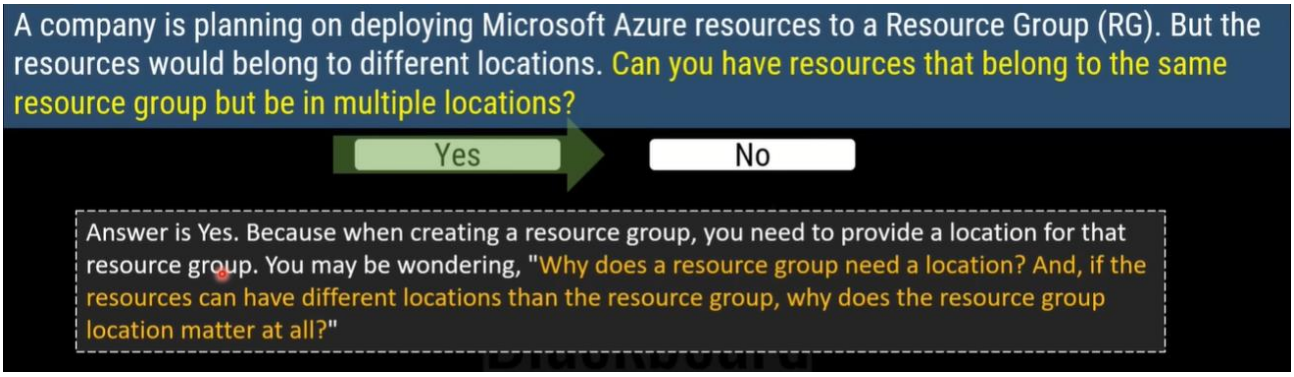
15. Public vs Private Preview:





Azure services in public preview can be managed using the regular management tools: Azure Portal, Azure CLI and Azure PowerShell.

16. Other:



You can enable just in time (JIT) VM access by using:

a) Azure Bastion
b) Azure Firewall
c) Azure Front Door
d) Azure Security Center

The just-in-time (JIT) virtual machine (VM) access feature in Azure Security Center allows you to lock down inbound traffic to your Azure Virtual Machines. This reduces exposure to attacks while providing easy access when you need to connect to a VM.

A company is using containers for deploying all of its web applications. During a security audit, you notice that Microsoft Defender for Cloud is not being used properly to provide misconfigurations related to containers. For which resource can you NOT use Microsoft Defender for Cloud to secure the containers?

a) Azure Kubernetes Service (AKS)
b) Container hosts (VMs running Docker)
c) Azure Container Registry (ACR)
d) Azure Container Instance (ACI)

Special Topics:

1. **Cloud Computing, High Availability, Scalability, Elasticity, Agility, Fault Tolerance, and Disaster Recovery**

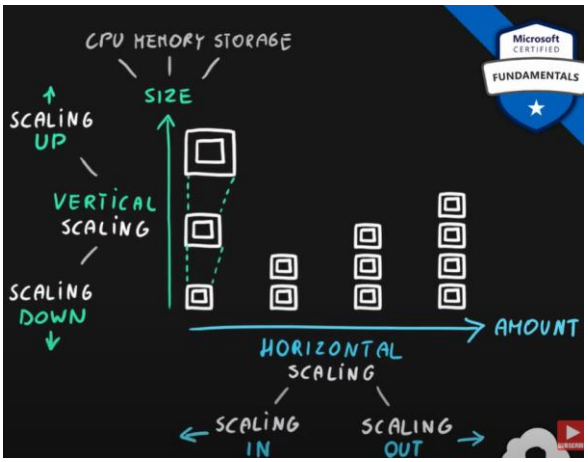
Cloud Computing

Service delivery model over the internet (cloud). This includes but is not limited to

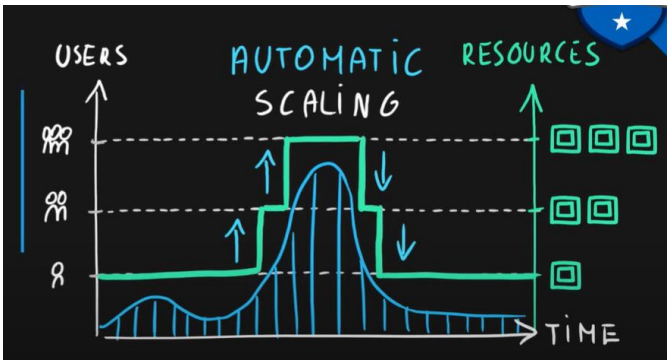
1. **compute power** meaning servers such as windows, linux, hosting environments, etc.
2. **storage** like files and/or databases
3. **networking** in azure but also outside when connecting to your company network
4. **analytics** services for visualization and telemetry data

Key concepts

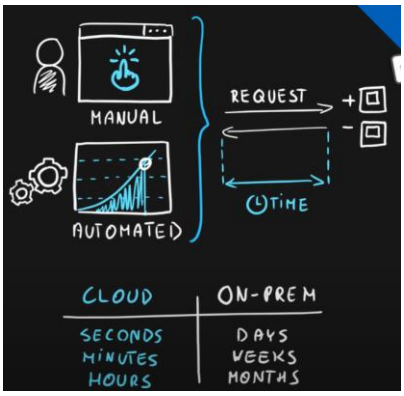
- **scalability** is the ability to scale, so allocate and deallocate resources at any time



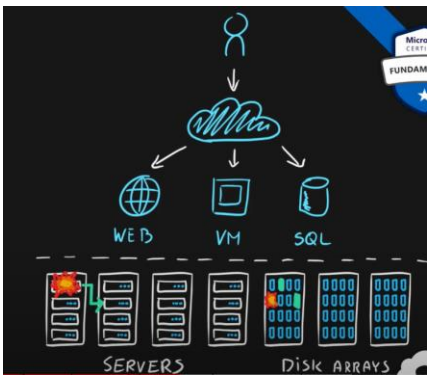
- **elasticity** is the ability to scale dynamically



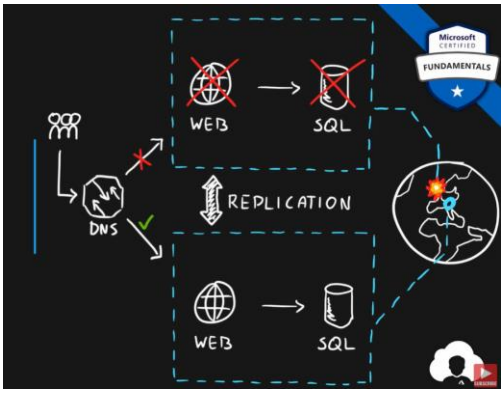
- **agility** is the ability to react fast (scale quickly)



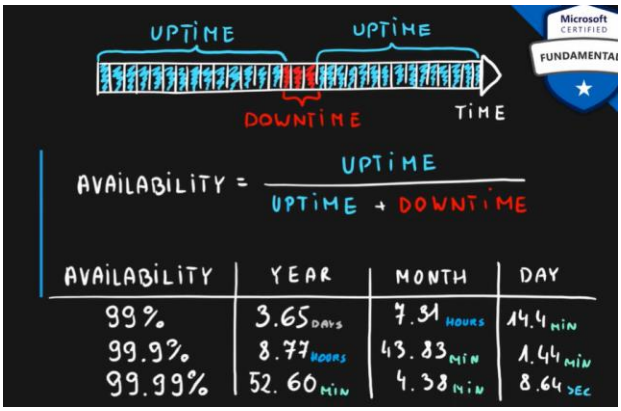
- **fault tolerance** is the ability to maintain system uptime while physical and service component failures happen



- **disaster recovery** is the process and design principle which allows a system to recovers from natural or human induced disasters



- **high availability** is the agreed level of operational uptime for the system. It is a simple calculation of system uptime versus whole lifetime of the system.
    - availability = uptime/(uptime + downtime)



Episode 2: Principles of economies of scale

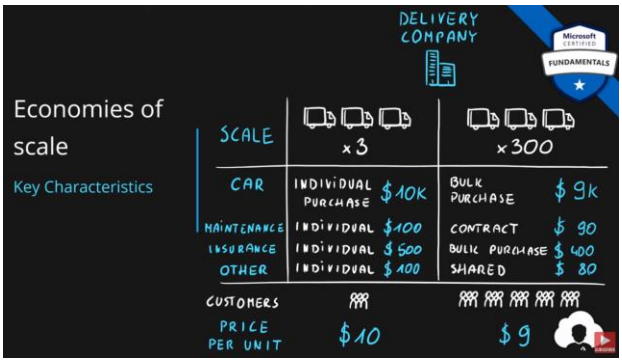
Economies of Scale

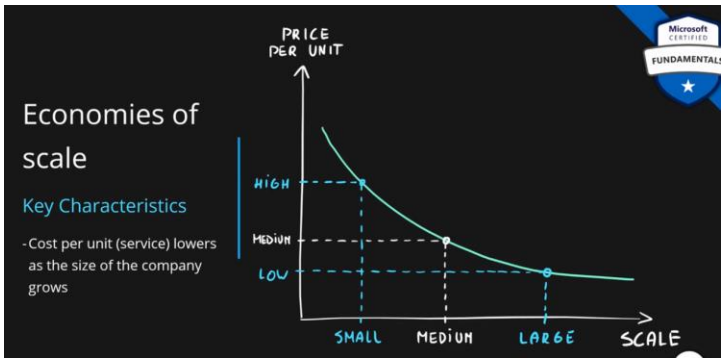
The principle of economies of scale states that as the companies grow they become more effective at managing shared operations. Be that HR and hiring, taxes, accounting, internal operations, marketing, big purchases via contracts meaning better discounts, etc. etc.

Because of those, companies can save/earn more which in return allows for reduction in cost of their services to their customers. This is so called 'price per unit'.

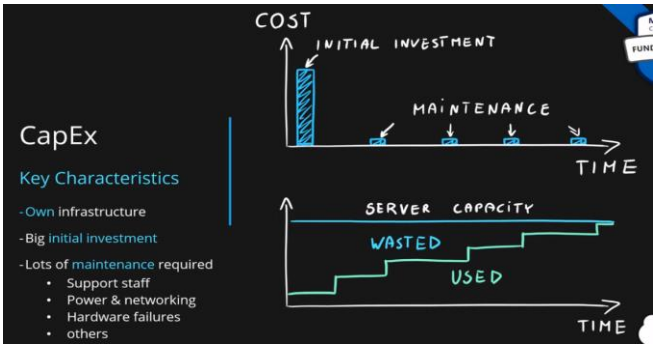
It's not possible to go to 0 because in the end some underlying infrastructure needs to run to provide the services. But the larger the scale the more benefits can be passed to customers.

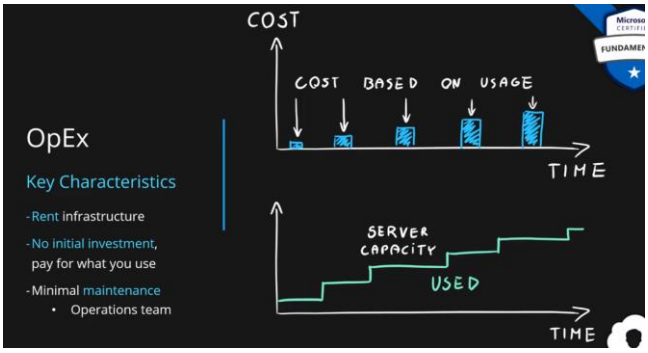
In fact, in the current scale, Microsoft can already offer multiple services for free due to how small a fraction of the cost it is for them.

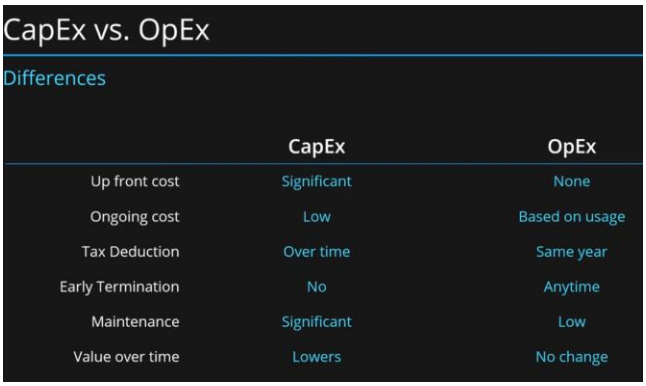




3. CapEx vs OpEx and their differences







4. <u>Consumption-based Model</u>

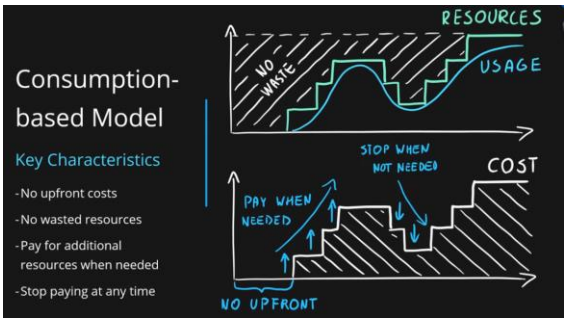
What is a consumption-based model?

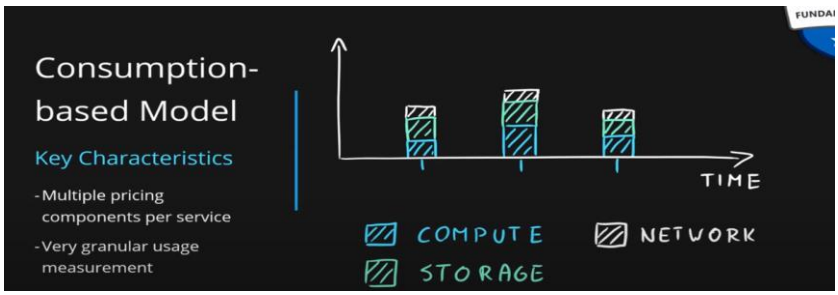
The consumption-based model is a **pricing model** used in the cloud so that customers are only charged **based on their resource usage**.

This model is characterized by

- **No associated upfront cost**
- **No wasted resources** as such *no charges are incurred for unused resources**. Unused in this case is different per service. For instance, blob storage that stores any data is considered to be used, as it consumes the storage space. Virtual Machines that are running consume CPU, memory and other resources even if there isn't any traffic. Hence they are considered to be used and will incur charges.
- **Pay for what you need**
- **Stop paying when you don't**

Consumption is the virtual metric used to calculate how much each resource (service) in Azure was used. Each service has many smaller metrics that track its consumption to offer best possible pricing model. Those metrics are tracked on very granular level.





<u>5 : IaaS vs PaaS vs SaaS cloud service models</u>

Service Models responsibilities

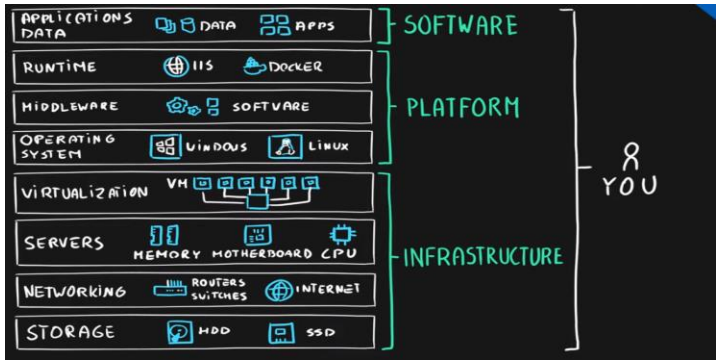
As a service means which party will manage the particular layer and all the layers below.

- **Software** layer consists the application (application code and set) & the application data
- **Platform** layer means all the supporting software and the operating system required to host the application

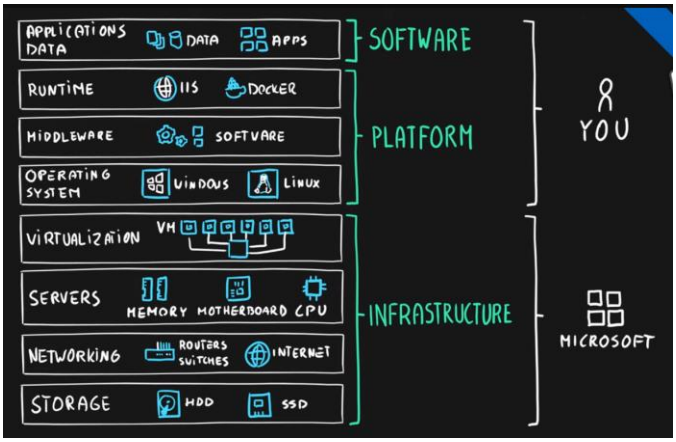
- **Infrastructure** layer consists hardware the infrastructure and virtualization required to host the platform

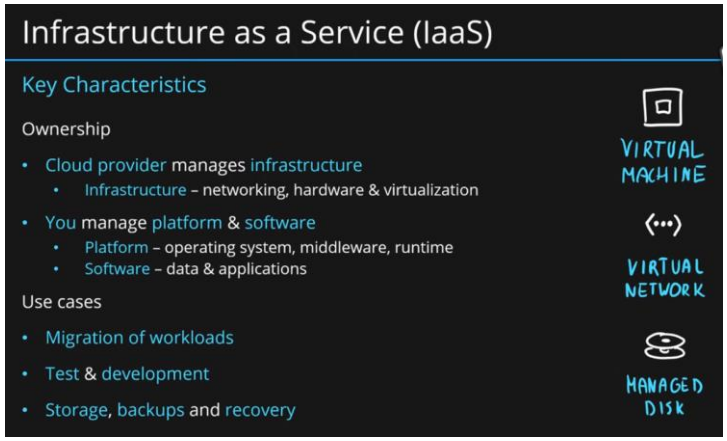
Layer	Layer
Application	Software
Data	Software
Runtime	Platform
Middleware	Platform
Operating System	Platform
Virtualization	Infrastructure
Servers	Infrastructure
Networking	Infrastructure
Storage	Infrastructure

A.. Private Cloud

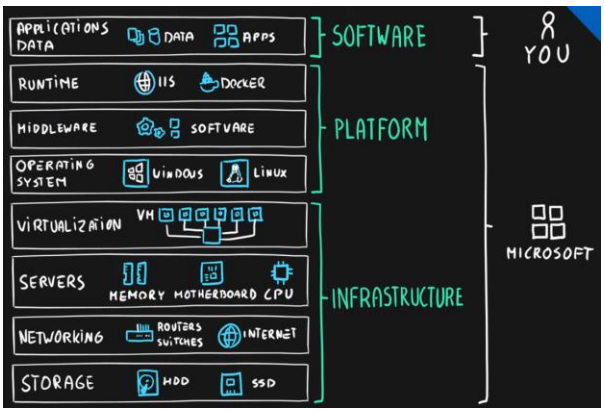


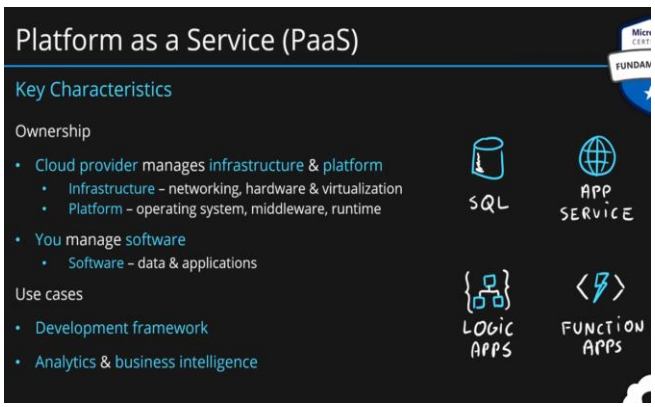
B. IAAS: (Infrastructure As A Service)



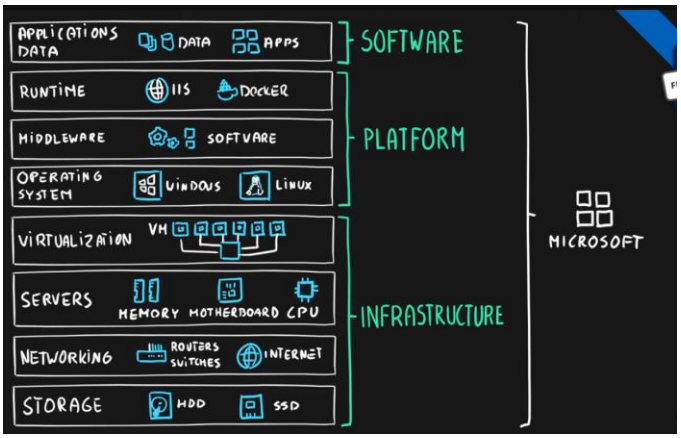


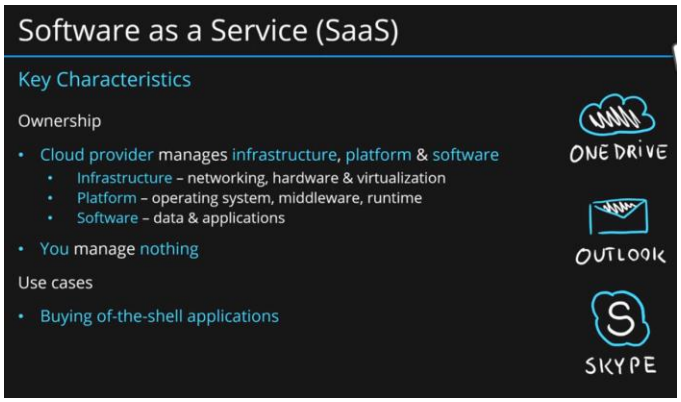
2. PAAS: (Platform As A Service)

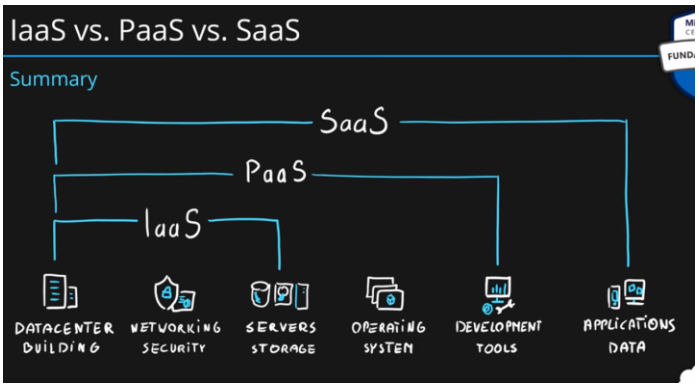




3. SAAS: (Software As A Service)







Responsibility Matrix

Layer	On-Premises	IaaS	PaaS	SaaS
Application	You	You	You	Cloud provider
Data	You	You	You	Cloud provider
Runtime	You	You	Cloud provider	Cloud provider
Middleware	You	You	Cloud provider	Cloud provider
Operating System	You	You	Cloud provider	Cloud provider
Virtualization	You	Cloud provider	Cloud provider	Cloud provider
Servers	You	Cloud provider	Cloud provider	Cloud provider
Networking	You	Cloud provider	Cloud provider	Cloud provider
Storage	You	Cloud provider	Cloud provider	Cloud provider

6 . **Public, Private & Hybrid cloud deployment models**

Cloud Deployment Model is simple a separation which describes where are the company resources deployed. Whenever this is in public cloud provider environment or private datacenter.

Below table presents high level deployment model separation

Layer	Cloud Provider	Own Datacenter
Public	✓	✗
Hybrid	✓	✓
Private	✗	✓

A. Public Cloud

Cloud Provider	Own Datacenter
✓	✗

Key Characteristics

- Everything runs on cloud provider hardware
- No local hardware
- Some services share hardware with other customers

Advantages

- No CapEx (No initial investment)
- High Availability
- Agility
- Pay as you Go (PAYG) pricing
- No hardware maintenance
- No deep technical skills required

Disadvantages

- Not all security and compliance policies can be met
- No ownership over the physical infrastructure
- Rare specific scenarios can't be done

B. Private Cloud

Cloud Provider	Own Datacenter
✗	✓

Key Characteristics

- Everything runs on your own datacenter
- Self-service should be provided
- You maintain the hardware

Advantages

- Can support any scenario
- Total control over security and infrastructure
- Can meet any security and compliance policy

Disadvantages

- Initial investment is required (CapEx)
- Limited agility constrained by server capacity and team skills
- Very dependent on IT skills & expertise

Hybrid Cloud

Cloud Provider	Own Datacenter
✓	✓

Key Characteristics

- Combines both Public & Private cloud

Advantages

- Great flexibility
- You can run any legacy apps in private cloud
- Can utilize existing infrastructure
- Meet any security& compliance requirements
- Can take advantage of all public cloud benefits

Disadvantages

1. Can be more expensive
2. Complicated to manage due to larger landscape
3. Most dependent on IT skills & expertise from all three models

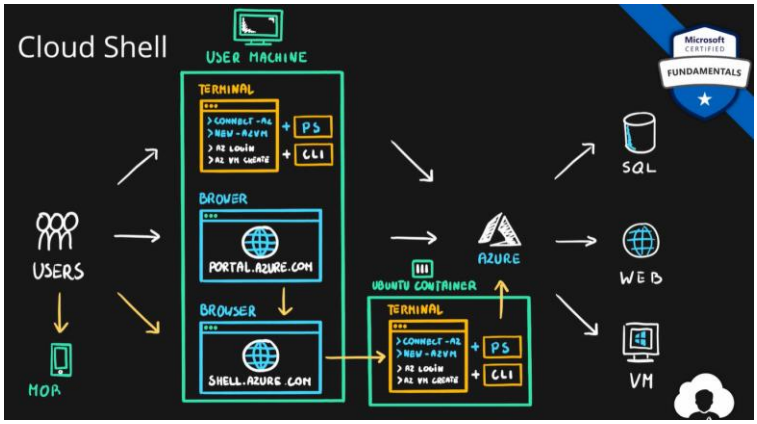
Hybrid Cloud

Advantages and Disadvantages

Advantages	Disadvantages
Great flexibility	Can be more expensive
Run legacy apps in private cloud	Complicated to manage
Utilize existing infrastructure	IT skills & expertise are mandatory
Meet any security requirements	

PART - II

1. Azure Portal, CLI, PowerShell & Cloud Shell



A. Azure Portal

- Public web-based interface for management of Azure platform
- Designed for self-service
- Customizable
- Simple tasks

B. **Azure PowerShell**

- PowerShell and module
- Designed for automation
- Multi-platform with PowerShell Core
- Simple to use
    - Connect-AzAccount – log into Azure
    - Get-AzResourceGroup – list resource groups
    - New-AzResourceGroup – create new resource group
    - New-AzVm – create virtual machine

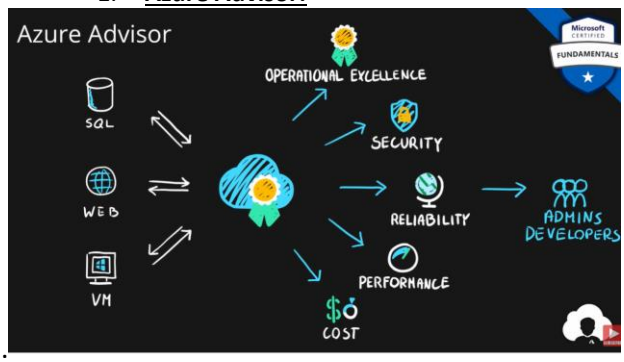
C. Azure CLI

- Command Line Interface for Azure
- Designed for automation
- Multi-platform (Python)
- Simple to use
    - az login – log into Azure
    - az group list – list resource groups
    - az group create – create new resource group
    - az vm create – create virtual machine
- Native OS terminal scripting

D. Azure Cloud Shell

- Cloud-based scripting environment
- Completely free
- Supports both Azure PowerShell and Azure CLI
- Dozen of additional tools
- Multiple client interfaces
    - Azure Portal integration (portal.azure.com)
    - Shell Portal (shell.azure.com)
    - Visual Studio Code Extension
    - Windows Terminal
    - Azure Mobile App
    - Microsoft Docs integration

1. **Azure Advisor:**

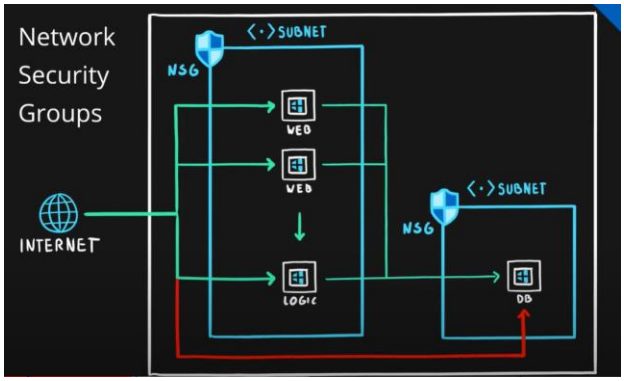


- Personalized consultant service
- Designed to provide **recommendations** and **best practices** for
    - Cost (SKU sizes, idle services, reserved instances, etc.)
    - Security (MFA settings, vulnerability settings, agent installations, etc.)
    - Reliability (redundancy settings, soft delete on blobs, etc.)
    - Performance (SKU sizes, SDK versions, IO throttling, etc.)
    - Operational Excellence (service health, subscription limits, etc.)
- Actionable recommendations. Its Free!

2. Azure security Group:

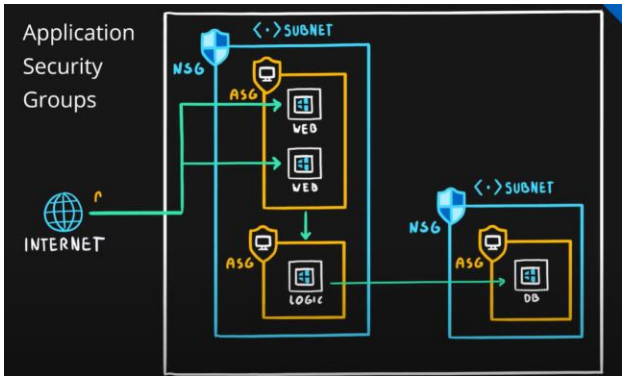
- Designed to filter traffic to (inbound) and from (outbound) Azure resources located in - Azure Virtual Network
- Filtering controlled by rules
- Ability to have multiple inbound and outbound **rules**
- Rules are created by specifying
    - **Source/Destination** (IP addresses, service tags, application security groups)
    - **Protocol** (TCP, UDP, any)

- **Port** (or Port Ranges, ex. 3389 – RDP, 22 – SSH, 80 HTTP, 443 HTTPS)
- **Direction** (inbound or outbound)
- **Priority** (order of evaluation)



Application Security Group:

- Feature that allows grouping of virtual machines located in Azure virtual network
- Designed to reduce the maintenance effort (assign ASG instead of the explicit IP address)



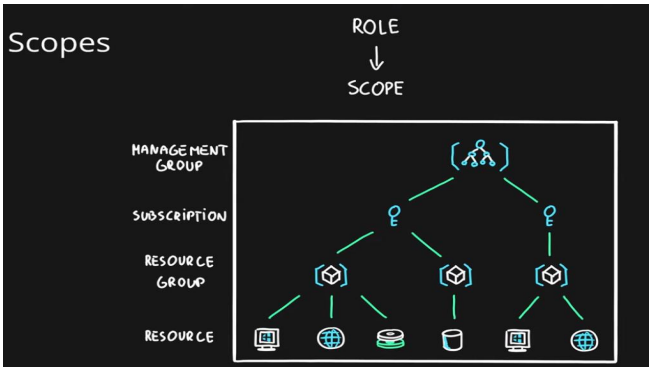
3. Azure Key Vault

- Managed service for securing sensitive information (application/platform) (**PaaS**)
- Secure storage service for Keys, Secrets and Certificates. All information stored in the Key Vault is encrypted. ***
- Highly integrated with other Azure services (VMs, Logic Apps, Data Factory, Web Apps, etc.)
- Centralization, Access monitoring and logging
- Azure Key Vault is used to store secrets for server application ***

4. RBAC (Role Base Access Control)

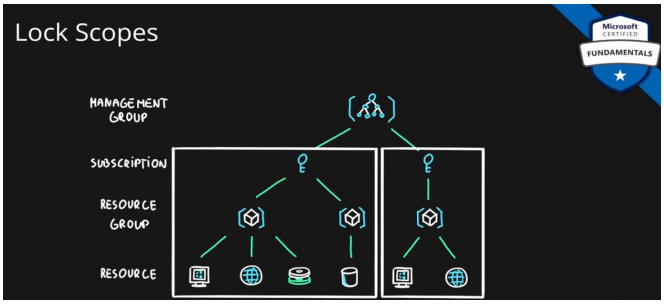
- Authorization system built on Azure Resource Manager (ARM)
- Designed for fine-grained access management of Azure Resources
- Role assignment is combination of
  - **Role definition** – list of permissions like create VM, delete SQL, assign permissions, etc.
  - **Security Principal** – user, group, service principal and managed identity

- **Scope** – resource, resource groups, subscription, management group
- Hierarchical
  - Management Groups > Subscriptions > Resource Groups > Resources
- Built-in and Custom roles are supported



5. Resource Lock:

- Designed to prevent accidental deletion and/or modification
- Used in conjunction with RBAC
- Two types of locks
  - **Read-only** (**ReadOnly**) – only read actions are allowed
  - **Delete** (**CanNotDelete**) – all actions except delete are allowed
- Scopes are **hierarchical** (**inherited**)
  - Subscriptions > Resource Groups > Resources
- **Management Groups** can't be locked
- Only **Owner** and **User Access Administrator** roles can manage locks (**built-in** roles)

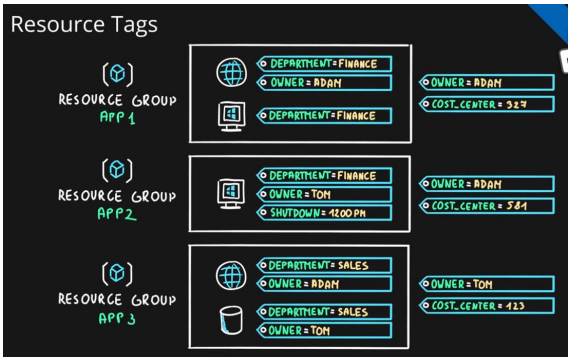


6. Azure TAGS:

- Tags are simple **Name** (key) - **Value pairs**
- Designed to help with **organization of Azure resources**
- Used for resource **governance**, **security**, **operations management**, **cost management**, **automation**, etc.
- Typical **tagging strategies**
  - **Functional** – mark by **function** (ex: environment = production)
  - **Classification** – mark by **policies used** (ex: classification = restricted)
  - **Finance/Accounting** – mark for **billing purposes** (ex: department = finance)

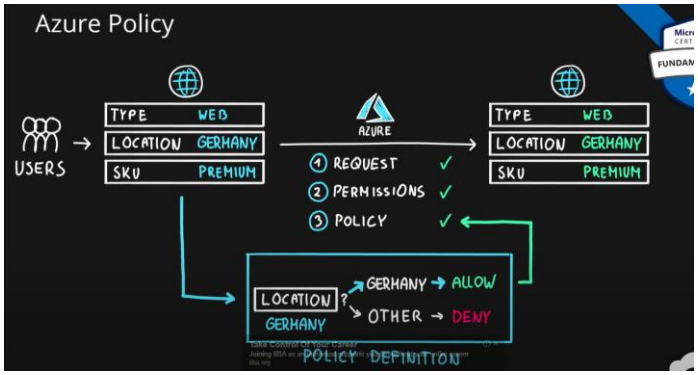
- **Partnership** – mark by **association of users/groups** (ex: owner = adam)

- Applicable for resources, resource groups and subscriptions
- NOT inherited by default



7. Azure Policy:

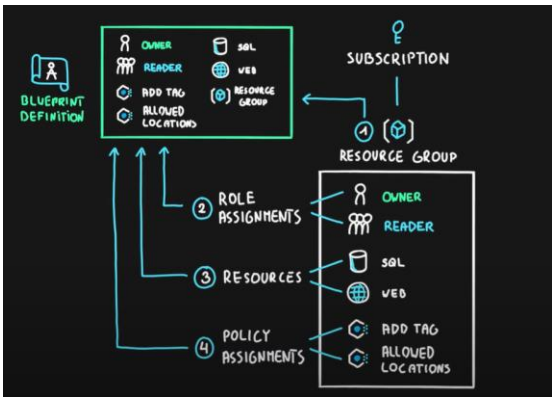
- Designed to help with resource **governance**, **security**, **compliance**, **cost management**, etc.
- **Policies** focus on resource properties (**RBAC** focused on **user actions**)
- Policy **definition** – Defines what should happen
    - Define the **condition** (if/else) and the **effect** (deny, audit, append, modify, etc.)
    - Examples include allowed *resource types*, *allowed locations*, *allowed SKUs*, *inherit resource tags*
- **Built-in** and **custom** policies are supported
- Policy **initiative** – a group of policy definitions
- Policy **assignment** – assignment of a policy definition/initiative to a scope
    - Scopes can be assigned to: Management Groups > Subscriptions > Resource Groups > Resources
- Policies allow for **exclusions of scopes**
- Checked during **resource creation** or **updates** and **existing ones with remediation tasks**

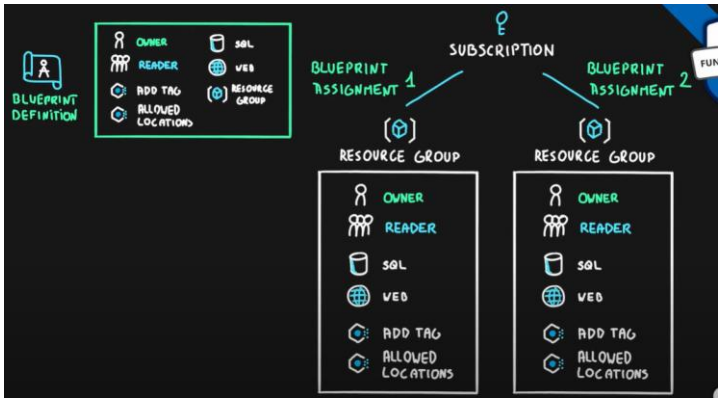


8. Azure BluePrint:

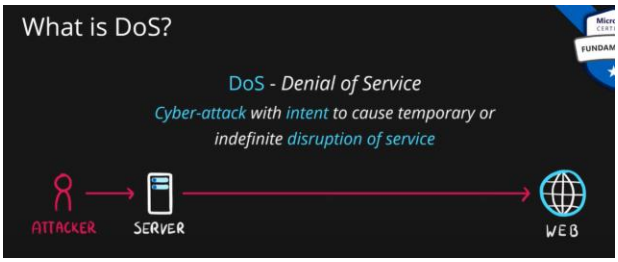
- Package of various Azure components (artifacts)
    - Resource Groups, ARM Templates, Policy Assignments, Role Assignments
- Centralized storage for organizationally approved design patterns
- **Blueprint definition** – describing what should happen (reusable package)

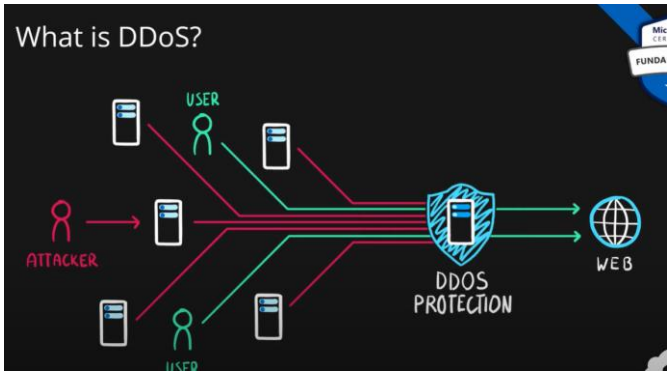
- **Blueprint assignment** – describing where it should happen (package deployment)





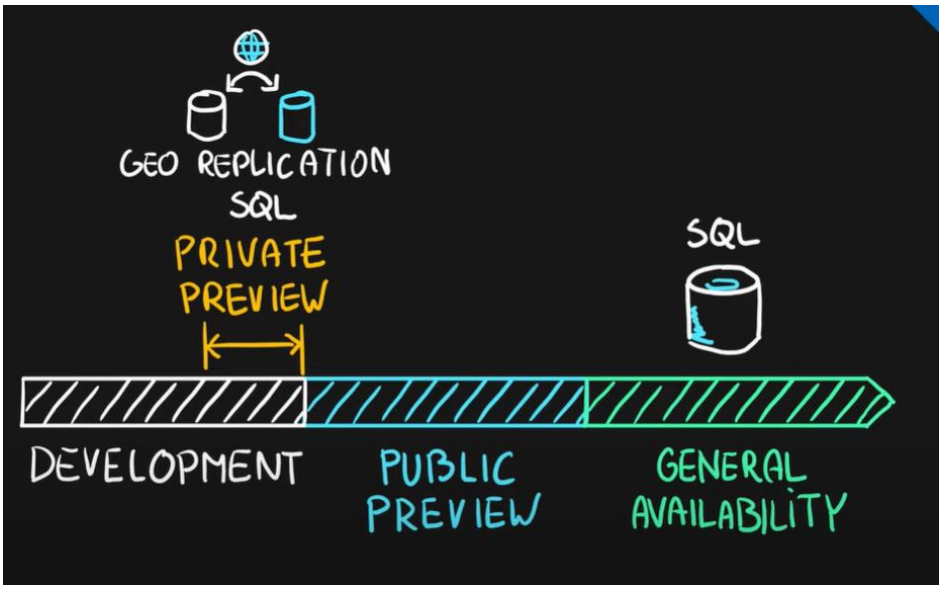
9. Azure DDoS Protection:





- DDoS protection service in Azure
- Designed to
  - Detect malicious traffic and block it while allowing legitimate users to connect
  - Prevent additional costs for auto-scaling environments
- Two tiers
  - **Basic** – automatically enabled for Azure platform
  - **Standard** – additional mitigation & monitoring capabilities for Azure Virtual Network resources
- Standard tier uses machine learning to analyze traffic patterns for better accuracy

10. Service Lifecycle in Azure | Public Preview and General Availability



Service Lifecycle

- Every service in Azure follows its own service lifecycle
- **Public preview** is a **‘beta’** stage of the service available to general public use
- **Features** can also be in **preview** stages
- Designed for **testing**, **not production** solutions
- **General availability** is a **‘production’** release of the service

Public Preview Key Info

- No SLA
- Some services have no support coverage
- Limited region availability
- Limited functionality
- Pricing changes
- Direction changes
- Azure Portal Previews (https://preview.portal.azure.com)

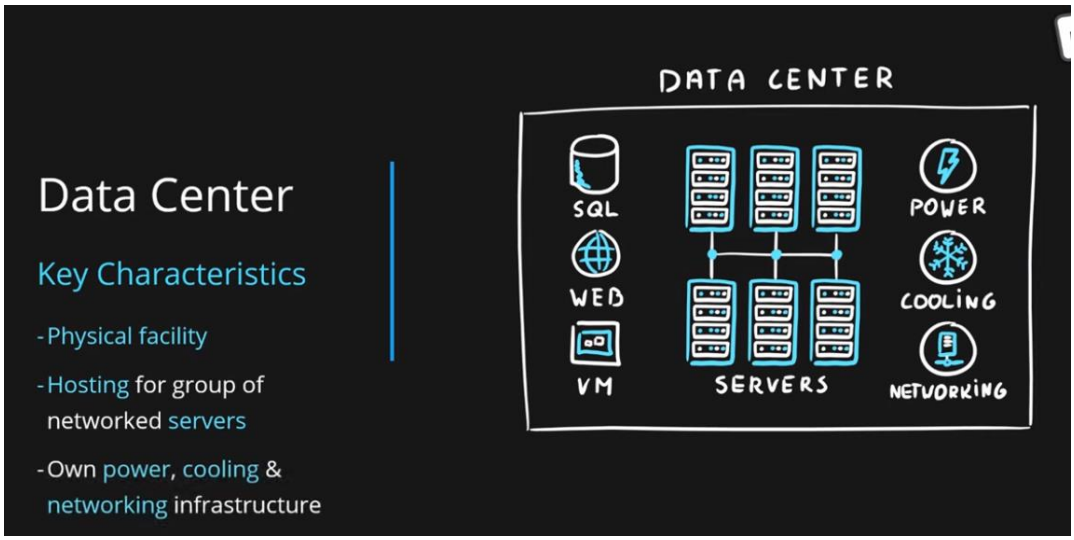
PART-III

(Describe Azure architecture and services)

Episode 7 : Geographies, Regions & Availability Zones

Data Center

- **Physical facility**
- **Hosting for** group of networked **servers**
- Own **power**, **cooling** & **networking** infrastructure

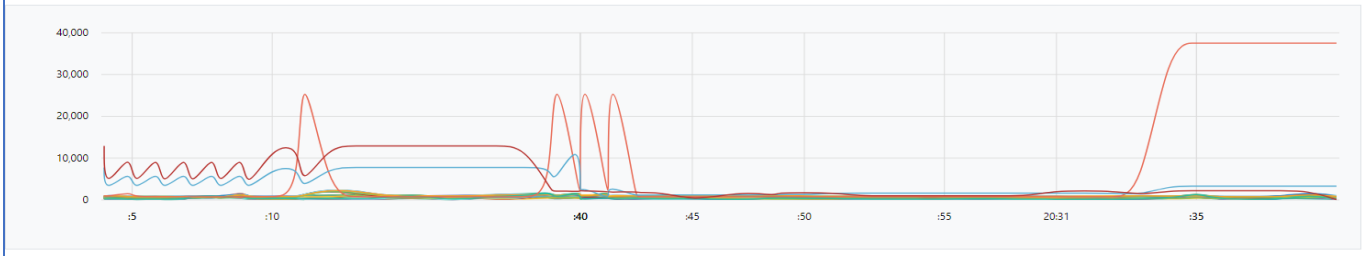


Region

- **Geographical area** on the planet
- **One but usually more datacenters** connected with **low-latency network** (<2 milliseconds)
- **Location** for your services (check where the resources can be deploy)
- Some services are **available only in certain regions**
- Some services are **global services**, as such are not assigned/deployed in specific region
- Globally available with **50+ regions**
- Special **government regions** (US DoD Central, US Gov Virginia, etc.)
- Special **partnered regions** (China East, China North)

Azure Speed Test: https://www.azurespeed.com/Azure/Latency

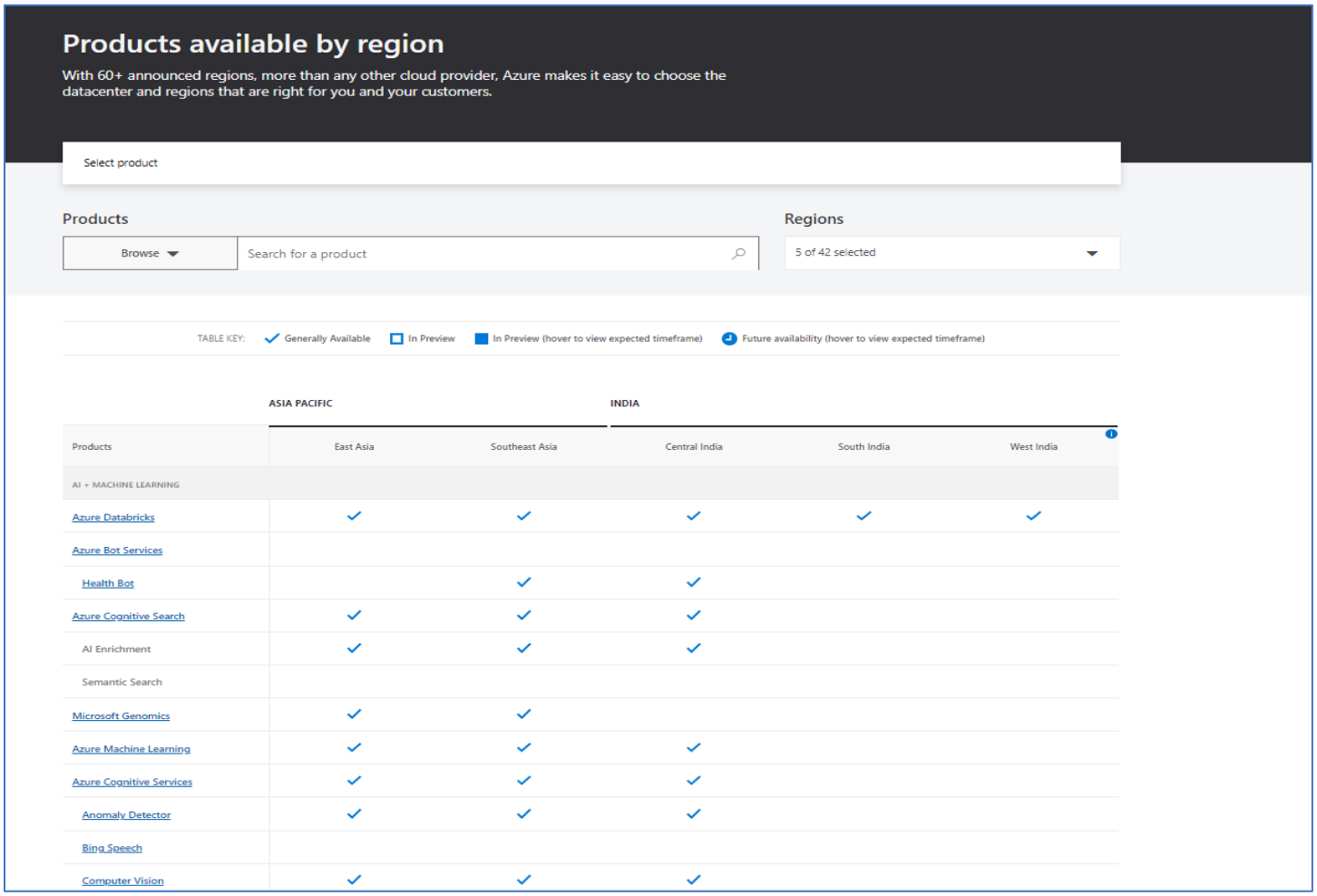
East Asia (Hong Kong)	155 ms
Central India (Pune)	181 ms



Latency Test

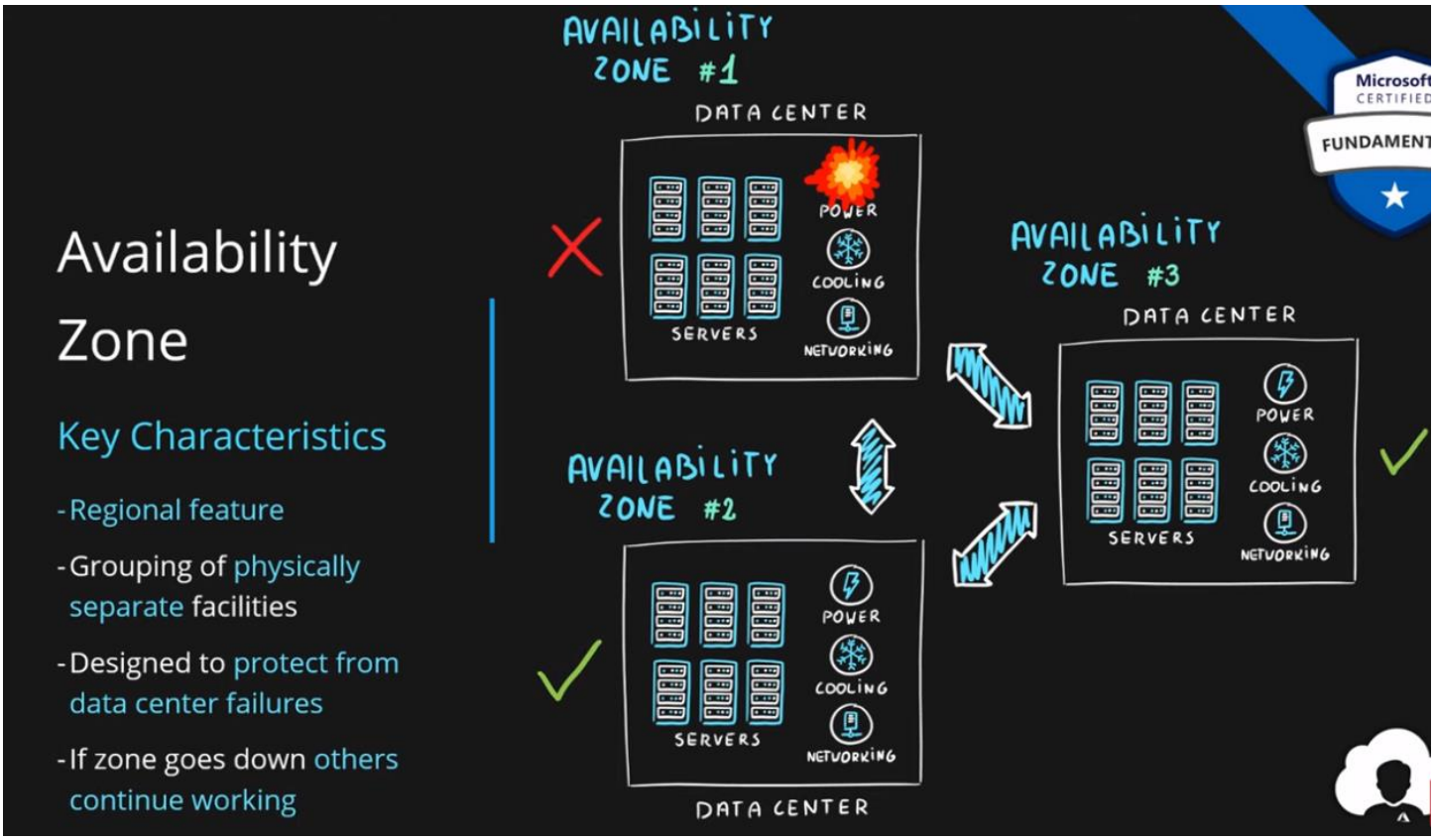
Geography	Region	Physical Location	Average Latency (ms)
Asia Pacific	Australia Central	Canberra	385 ms
Asia Pacific	Australia East	New South Wales	550 ms
Asia Pacific	Australia Southeast	Victoria	337 ms
Asia Pacific	Central India	Pune	181 ms
Asia Pacific	East Asia	Hong Kong	155 ms
Asia Pacific	Japan East	Tokyo, Saitama	316 ms
Asia Pacific	Japan West	Osaka	277 ms
Asia Pacific	Korea Central	Seoul	298 ms
Asia Pacific	Korea South	Busan	257 ms
Asia Pacific	Southeast Asia	Singapore	132 ms
Asia Pacific	South India	Chennai	197 ms
Asia Pacific	West India	Mumbai	218 ms
US	Central US	Iowa	904 ms

Product Available by Region: https://azure.microsoft.com/en-us/explore/global-infrastructure/products-by-region/



Availability Zone

- **Regional feature**
- Grouping of **physically separate** facilities
- Designed to **protect from data center failures**
- If zone goes down **others continue working**
- Two service **categories**
    - **Zonal** services (Virtual Machines, Disks, etc.)
    - **Zone-redundant** services (SQL, Storage, etc.)
- **Not all** regions are **supported**
- **Supported** region has **three or more zones**
- A **zone** is **one or more data centers**

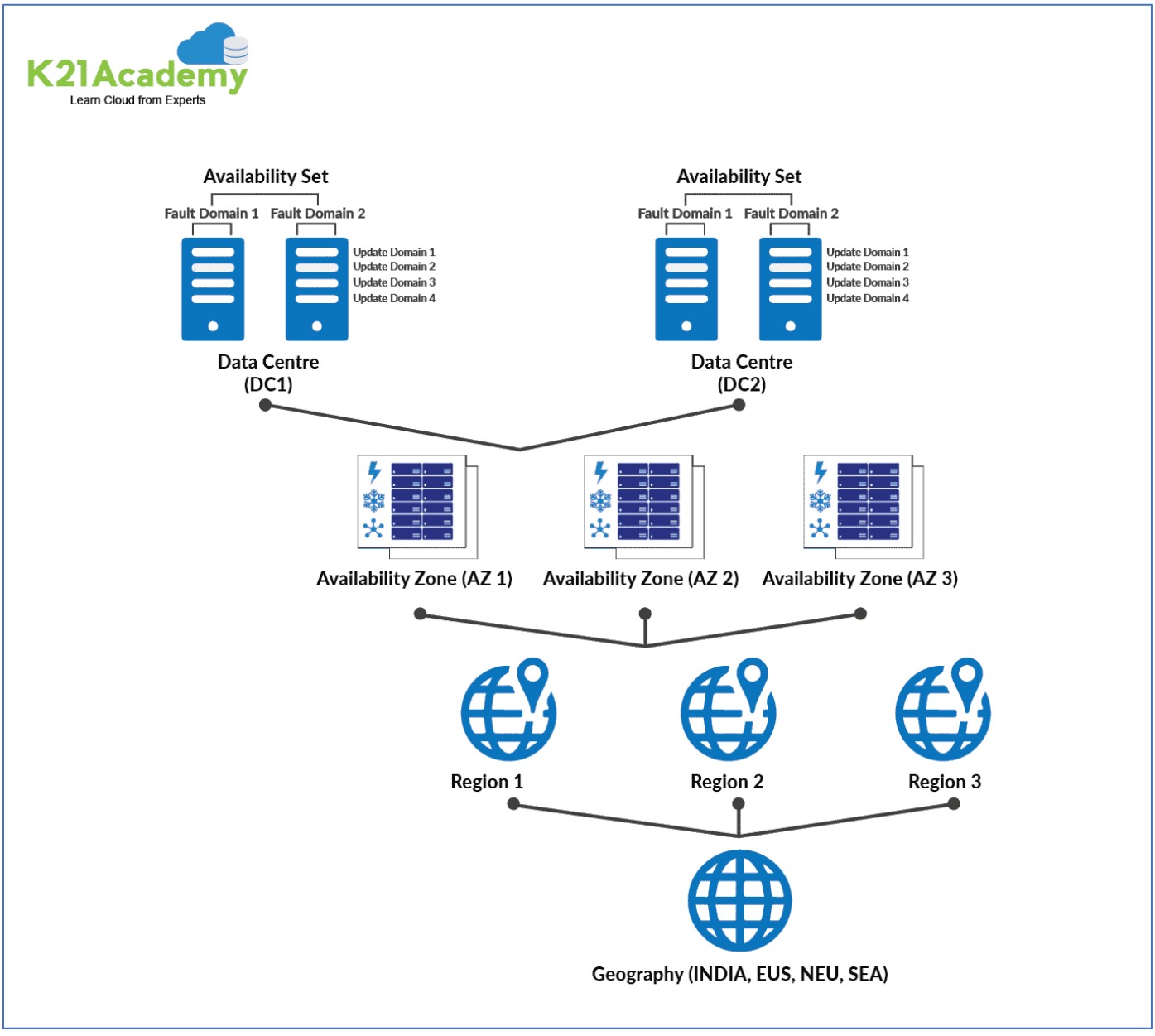


Region Pair

- **Each region** is **paired** with another region making it a region pair
- Region **pairs are static** and cannot be chosen
- Each pair resides within the **same geography***
    - Exception is Brazil South

- **Physical isolation** with at least 300 miles distance (when possible)
- Some services have **platform-provided replication**
- **Planned updates** across the pairs
- **Data residency** maintained for disaster recovery

Region Pair A	Region Pair B
East US	West US
UK West	UK South
North Europe (Ireland)	West Europe (Netherlands)
East Asia (Hong Kong)	Southeast Asia (Singapore)

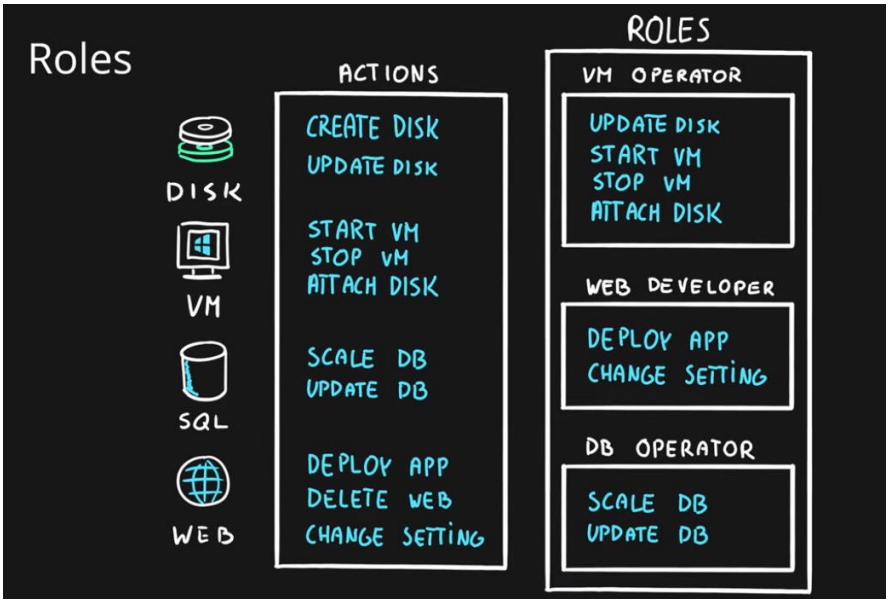


Episode 28:

What is a Role?

Role (role definition) is a **collection of actions** that **the assigned identity** will be able to perform.

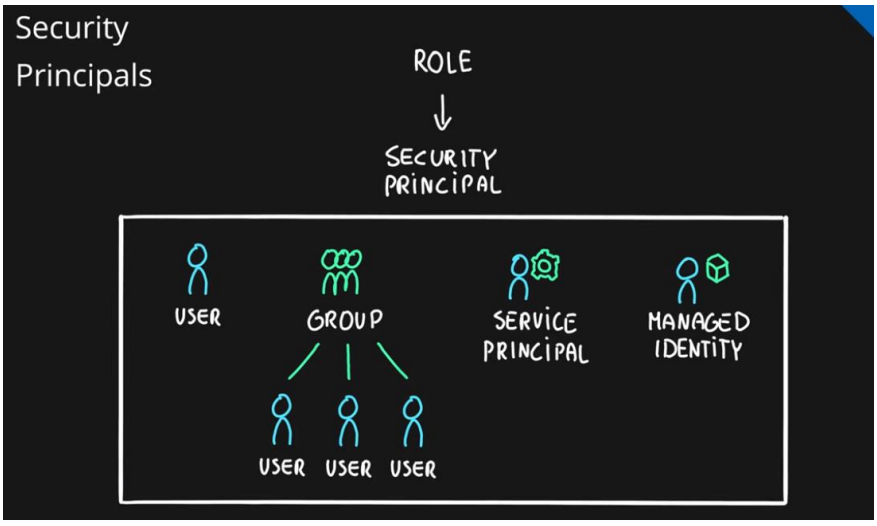
Role definition is an answer to a question "**What** can be done?"

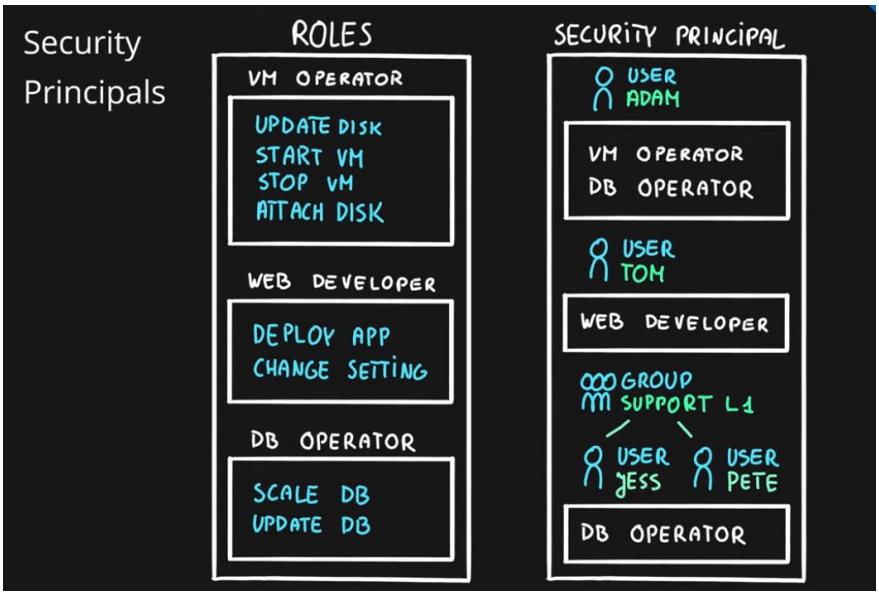


What is a Security Principal?

Security Principal is an Azure object (identity) that can be assigned to a role (ex. users, groups or applications).

Security Principal assignment is an answer to a question "**Who** can do it?"

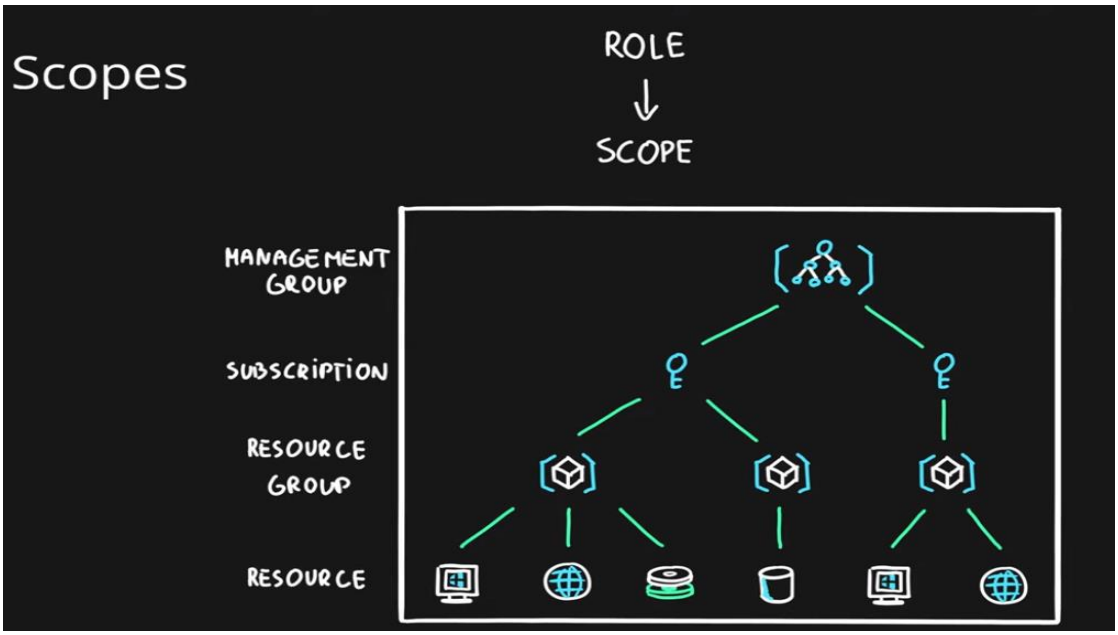




What is a Scope?

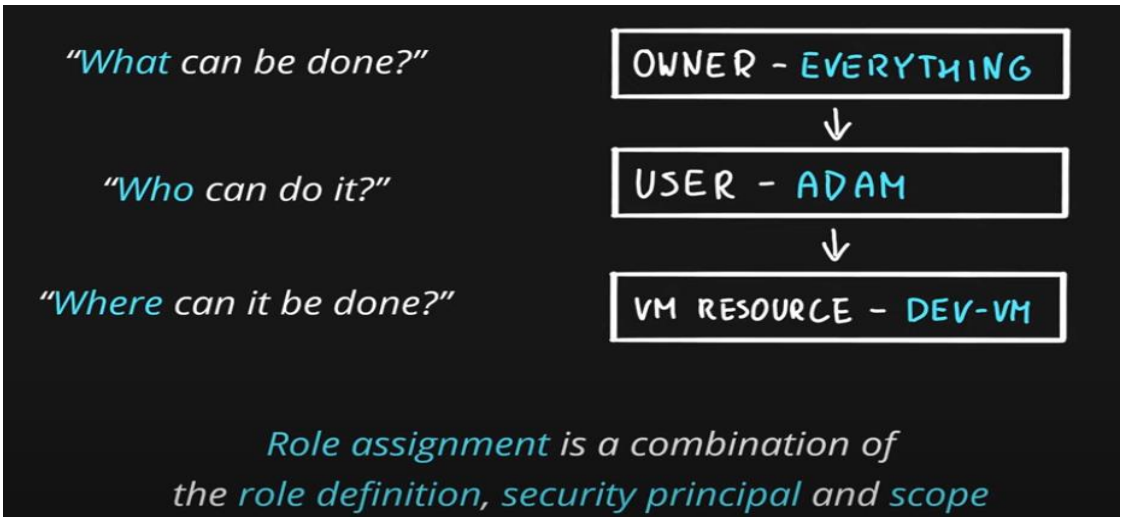
Scope is one or more Azure resources that the access applies to.

Scope assignment is an answer to a question "**Where** can it be done?"



What is a Role Assignment?

Role assignment is a combination of the **role definition**, **security principal** and **scope**.



Azure Role-based Access Control (RBAC)

- Authorization system built on Azure Resource Manager (ARM)
- Designed for fine-grained access management of Azure Resources
- Role assignment is combination of
    - **Role definition** – list of permissions like create VM, delete SQL, assign permissions, etc.
    - **Security Principal** – user, group, service principal and managed identity and
    - **Scope** – resource, resource groups, subscription, management group
- Hierarchical
    - Management Groups > Subscriptions > Resource Groups > Resources
- Built-in and Custom roles are supported

Question 10

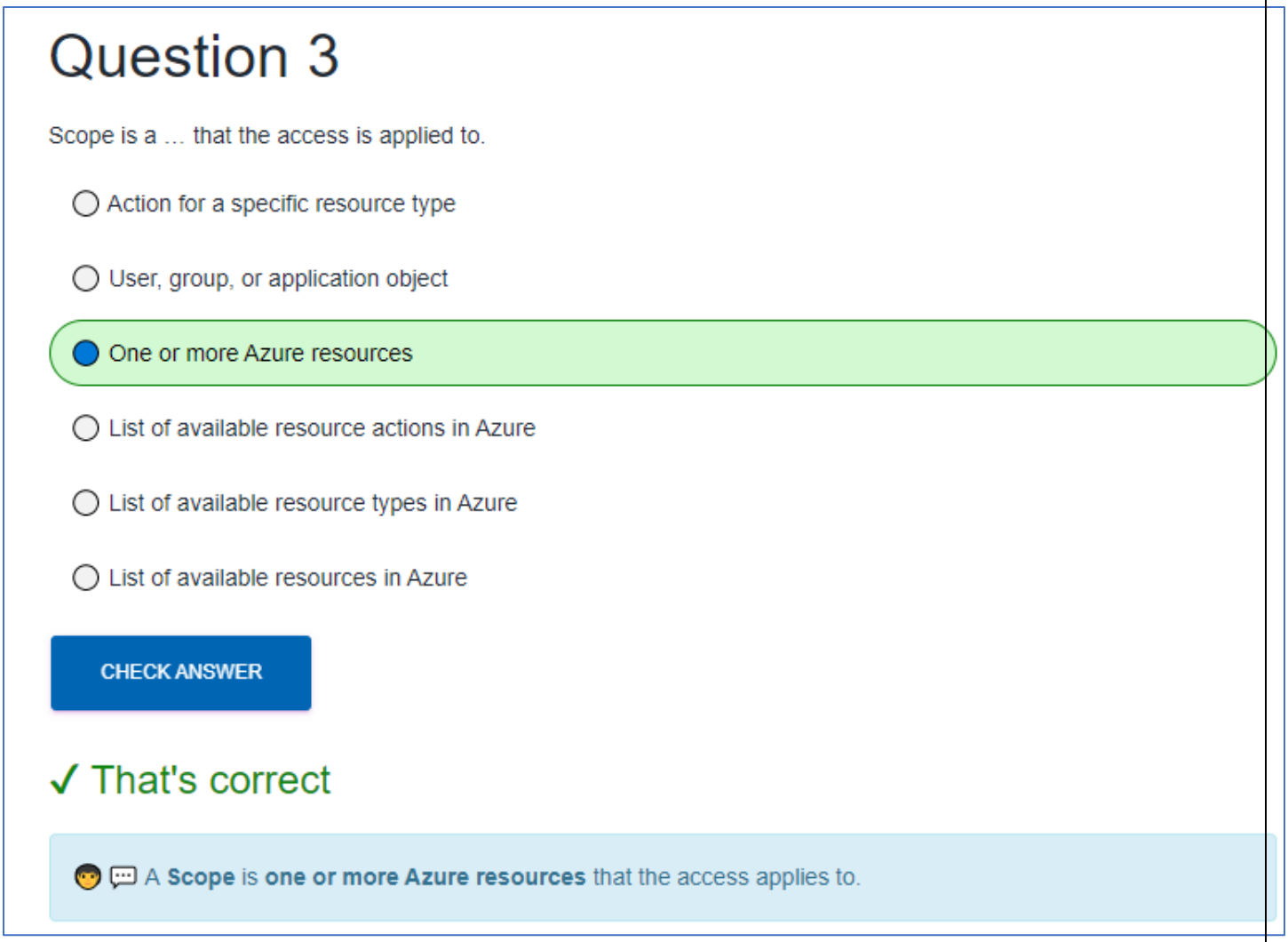
What is the proper order of actions that must be taken to grant a role in Azure Portal
A. Click Add Role Assignment button
B. Open Access Management (IAM) blade
C. Navigate to Azure resource, resource group, subscription, or management group
D. Click Save button
E. Select Role and Sercurity Principal

- ○ A > B > D > C > E
- ○ E > D > C > B > A
- ○ A > B > C > E > D
- ● C > B > A > E > D

Question 12

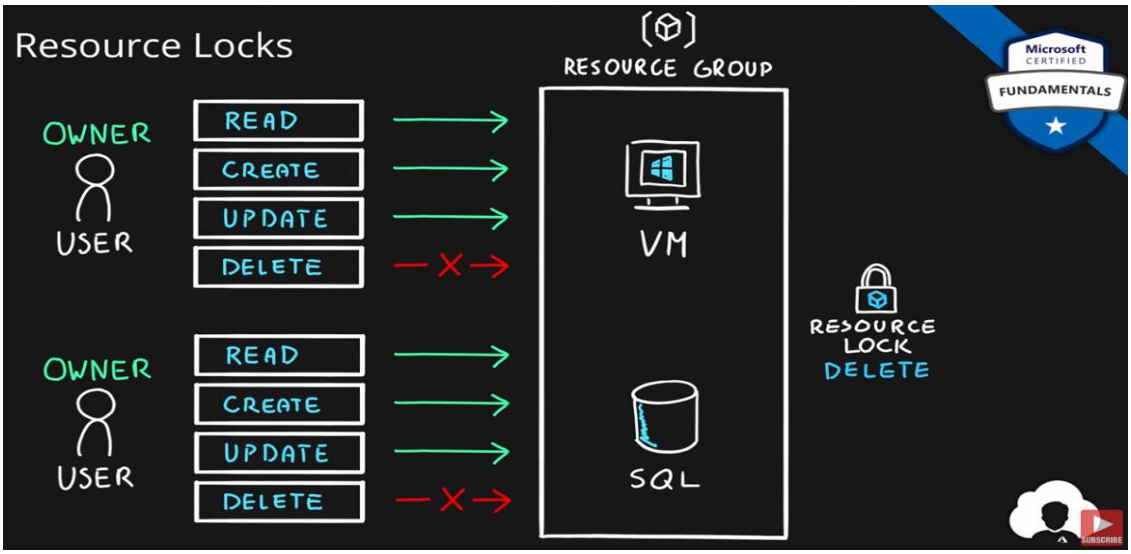
Contoso company wants to allow their development team to deploy web application to Azure App Service. What is the best strategy to do this following least-privilege required principle and that requires the least amount of effort?
Hint: All specified roles allow for web app deployments.

- 1.Assign an Owner role to all individual members of the development team on the resource group where Azure App Service is located
- 1.Assign a Owner role to all individual members of the development team on the Azure App Service resource
- 1.Create Azure AD group for the development team
  2.Assign a Website Contributor role to that group to the resource group where Azure App Service is located
- **1.Create Azure AD group for the development team**
  2.Assign a Website Contributor role to the Azure App Service resource
- 1.Create Azure AD group for the development team
  2.Assign an Owner role to that group to the resource group where Azure App Service is located
- 1.Create Azure AD group for the development team
  2.Assign an Owner role to that group to the resource group where Azure App Service is located

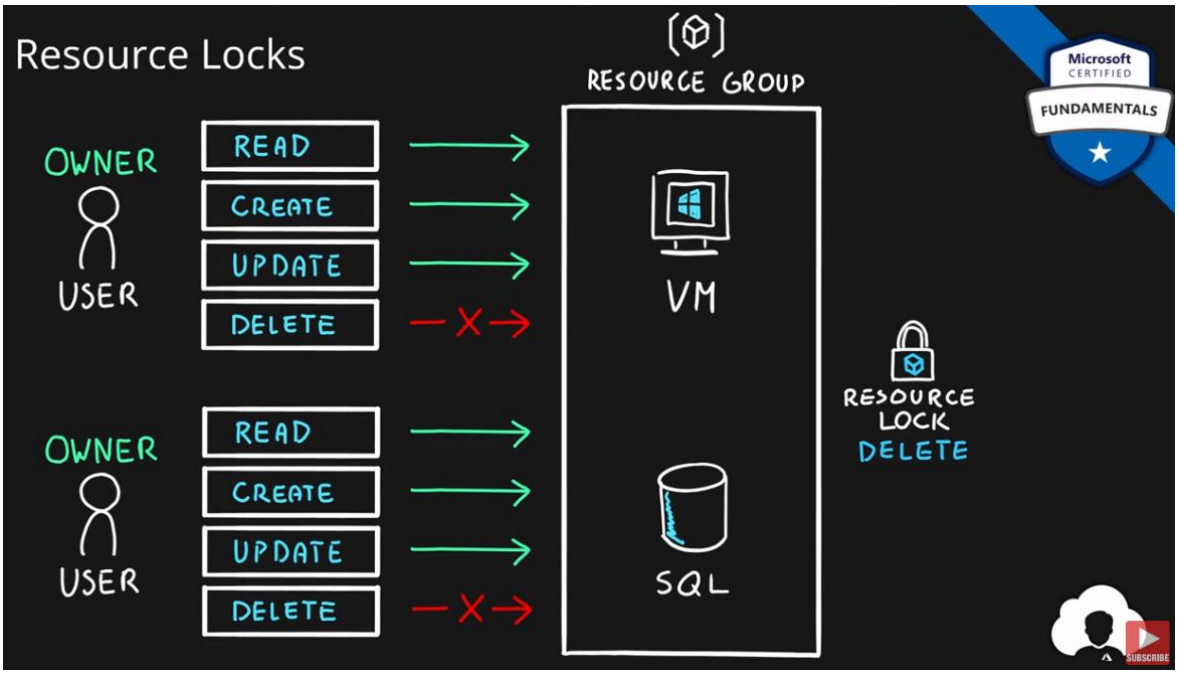


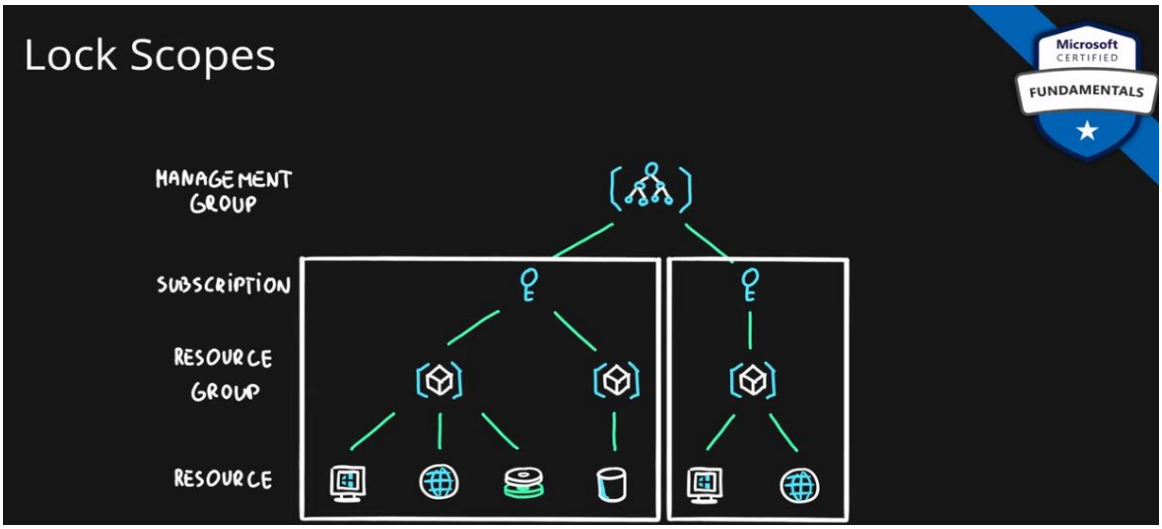
Episode 29: Resource Locks

What is an Azure Resource Lock?



- Designed to **prevent accidental deletion** and/or **modification**
- Used in conjunction with RBAC
- Two types of locks
    - **Read-only** (**ReadOnly**) – only read actions are allowed
    - **Delete** (**CanNotDelete**) – all actions except delete are allowed
- Scopes are **hierarchical** (**inherited**)
    - Subscriptions > Resource Groups > Resources



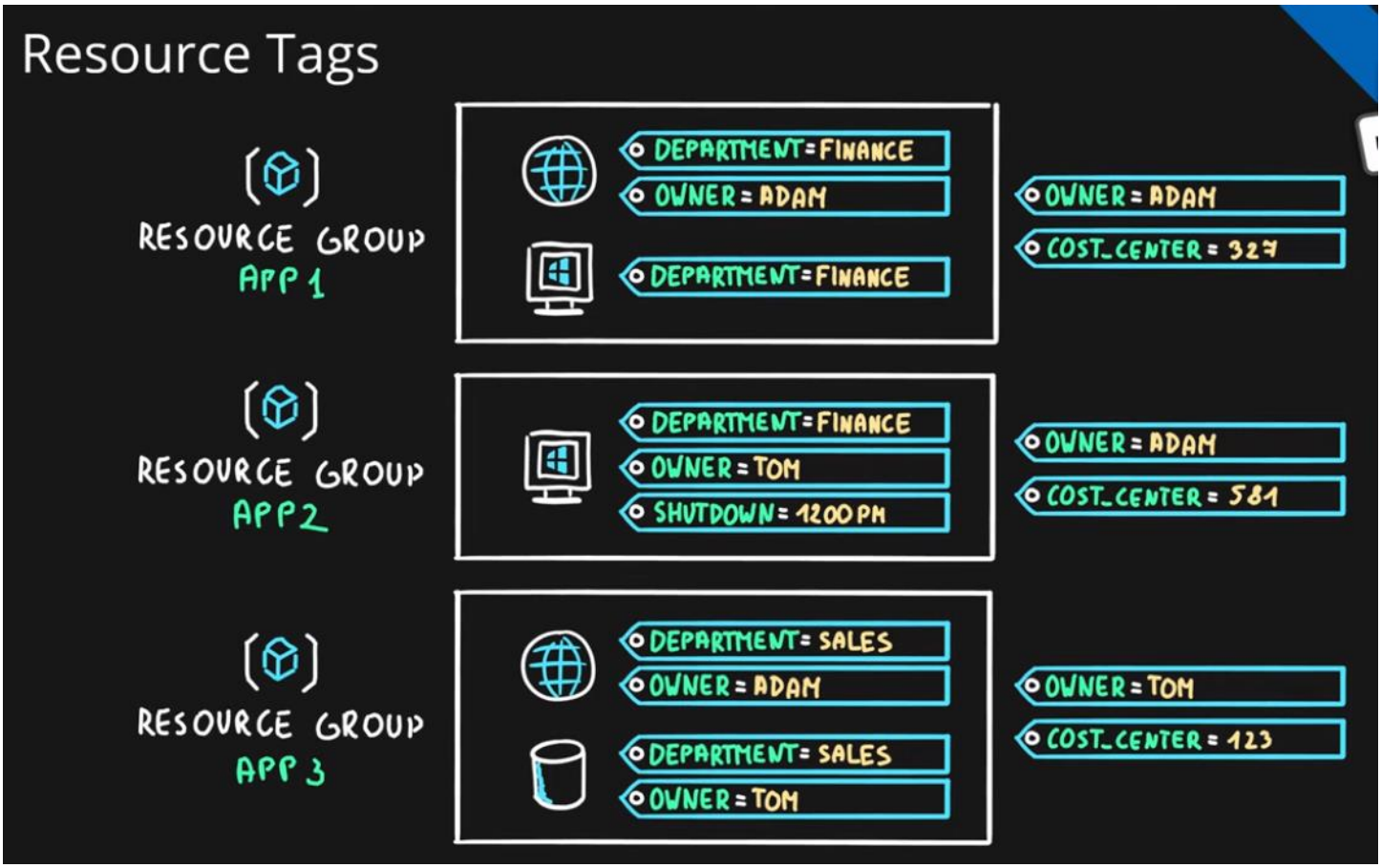


- **Management Groups** can't be locked
- Only **Owner** and **User Access Administrator** roles can manage locks (**built-in** roles)

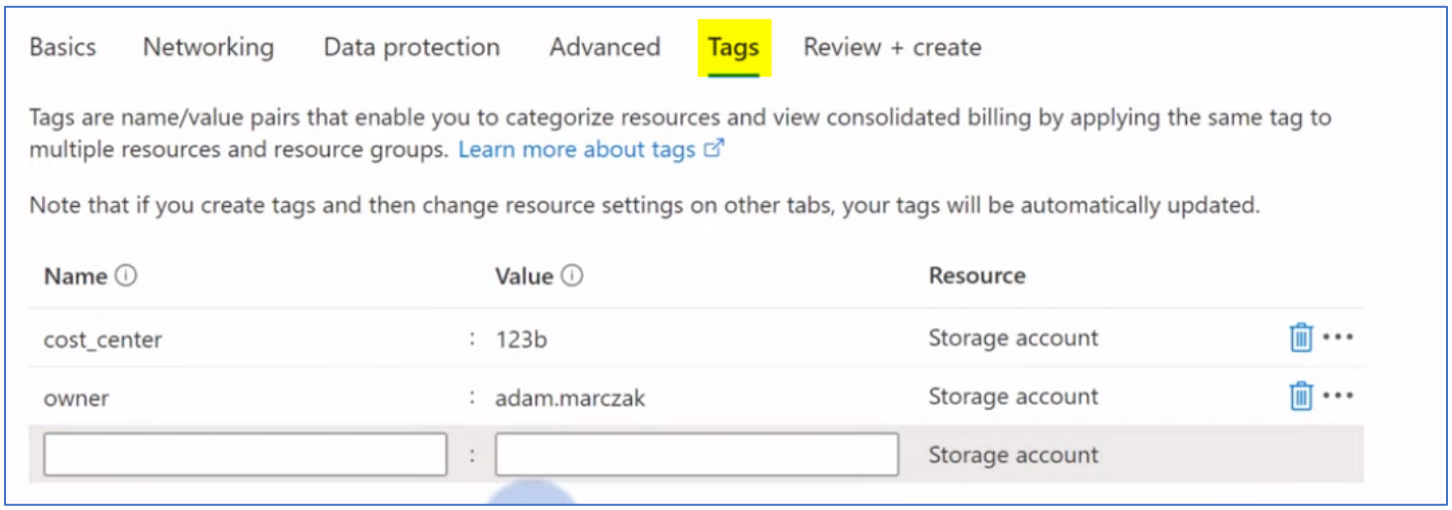
Episode 30 | Azure Resource Tags

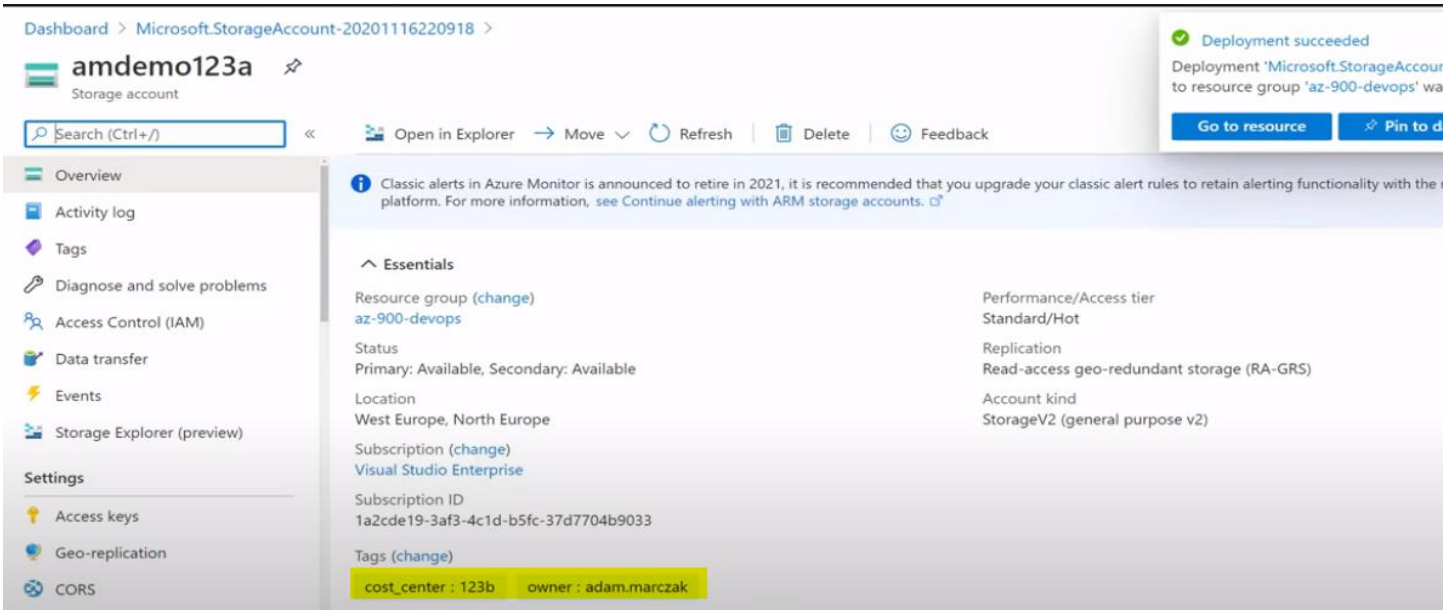
Azure Resource Tags

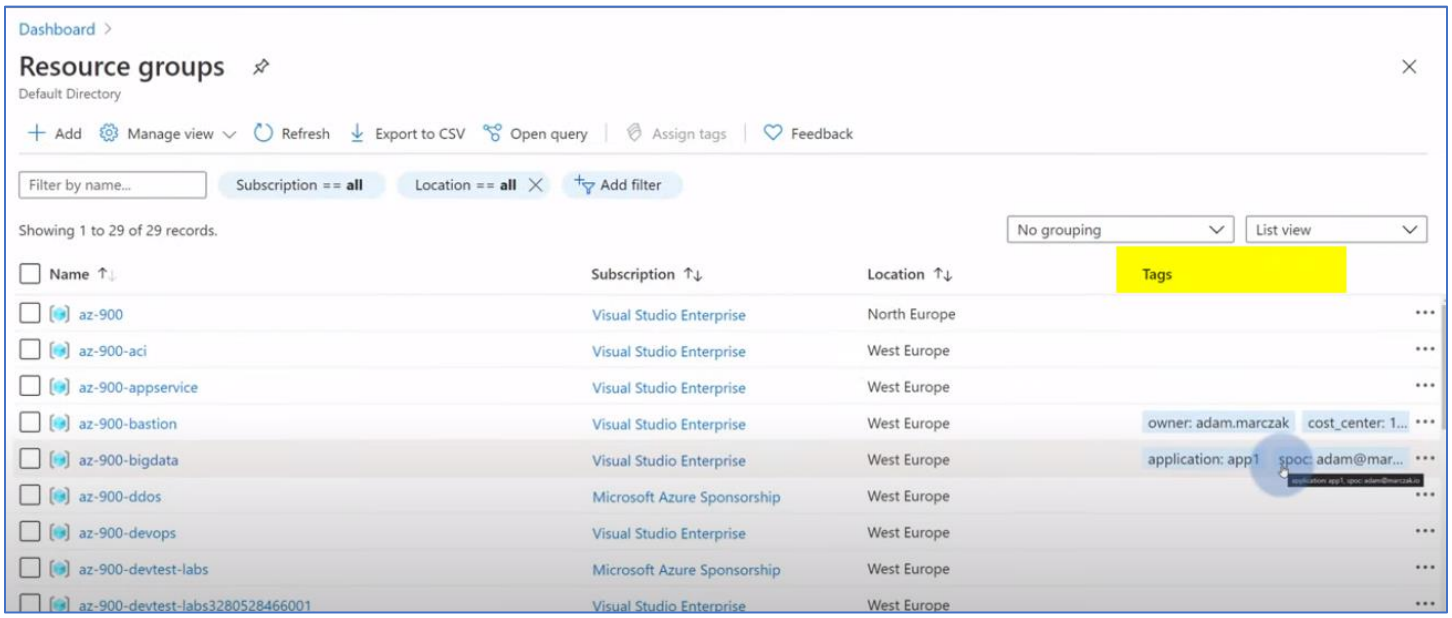
- Tags are simple **Name** (key) - **Value pairs**
- Designed to help with **organization of Azure resources**
- Used for resource **governance**, **security**, **operations management**, **cost management**, **automation**, etc.
- Typical **tagging strategies**
    - **Functional** – mark by **function** (ex: environment = production)
    - **Classification** – mark by **policies used** (ex: classification = restricted)
    - **Finance/Accounting** – mark for **billing purposes** (ex: department = finance)
    - **Partnership** – mark by **association of users/groups** (ex: owner = adam)
- Applicable for **resources**, **resource groups** and **subscriptions**
- **NOT inherited** by default



Resource Tages:







Azure Shell Query to review all tags: