**Azure Policy** is a service in Azure that you use to create, assign, and manage policies.

A **management group**  you can organize subscriptions into containers called "management groups" and apply your governance conditions/policies to the management groups.

A **read-only lock** is used to ensure that authorized users can read a resource, but they cannot delete or update the resource.

A **reservation** you can save money, resource costs up to 72% on pay-as-you-go prices.

Azure **Security Center** is an advanced, unified infrastructure security management that provides features such as security health monitoring for both cloud and on-premises workloads.

**Network security group (NSG)** is rules to allow all inbound connection from Port 80/8080 to reach VM

**Azure virtual network gateway** it is the VPN device in your Azure virtual network used to set up a site-to-site VPN connection between an Azure virtual network and your local network, or a VNet-to-VNet VPN connection between two Azure virtual networks. It can also be used to connect a virtual network to an ExpressRoute circuit.

**Azure Route table** is INCORRECT because A route table contains a set of rules (routes) that specifies how packets should be routed in a virtual network. **an Azure virtual machine** is CORRECT here because Azure VM is based on the Infrastructure as a Service through which the users can obtain more control over the environment to customize the hosting or development environment.

**an Azure web app** it's a Platform as a service used to build applications in azure platform without having to deploy, configure and maintain your own Azure VM's.

**Azure logic app** it's a Platform as a 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 SQL** database is INCORRECT here since it’s a platform as a service SQL serves as a relational database platform that is present in the cloud where users can host the data without having to worry about any infrastructure.

**Software as a Service (SaaS)** a “custom app” in first-line tells that it can’t be SaaS.

**Platform as a Service (PaaS)** don’t need to install any prerequisite application.

**Azure Functions** is a serverless compute service/platform that lets you run event-triggered code without having to explicitly provision or manage infrastructure.

**Azure Virtual Machines** is Infrastructure as a Service through which the users can obtain more control over the environment to customize the hosting or development servers.

**Azure storage account** is not a compute resource. It's a durable store in the cloud that allows developers to store tables, blobs, and message queues without worrying about the underlying storage server and hardware.

**Azure Container Instances** is a service that enables a developer to deploy containers on the Microsoft Azure public cloud without having to provision or manage any underlying infrastructure.

**Azure IoT Hub** is connected to millions of IoT devices. IoT hub can scale to millions of simultaneously connected devices and millions of events per second. This cannot provide serverless computing functionalities.

**Azure Machine Learning** is used to build Machine Learning Models based on past data and is used to prepare forecasts, trends, outcomes, and future behaviors.

**The Azure Portal and the Azure Cloud Shell** these are the two Azure Management tools that can be used from an iPhone and both these tools support the iOS – the operating system of an iPhone.

**Windows PowerShell** supports only the Windows operating system.

**Azure Storage Explorer** a standalone app that makes it easy to work with Azure Storage data on Windows, macOS, and Linux. It does not support iOS.

**Azure AD Identity Protection** (pre-requisite is that MFA has already been configured) any user who signs from the internet using an anonymous IP address would be prompted for password change.

**Azure AD Connect Health** is used for monitoring of identity governance or identity infrastructure of the on-premises resources or servers. We can Use the Azure AD Connect Health portal to view alerts, performance monitoring, usage analytics, and other information.

**Azure AD Privileged Identity Management** provides just-in-time access, prevent malicious activities, fully integrated reviews of the “privileged roles” in real time. This also helps to manage privileged admin roles across Azure resources and Azure AD.

**Azure Advanced Threat Protection (ATP)** is used to detect threat from on-premises resource, suspicious user activities (within the company itself) protect user identities etc.

**Azure Multi-factor authentication (MFA)** is only an authentication service when a user logs in via an Azure portal or he connects to any of the azure resources in Azure Public cloud. Using this the user accounts from on-premises cannot be moved to Azure

**The Azure Security Center** helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources.

**The Knowledge Center** gives most of your answers related to Azure Services

The **Advisor blade from Azure Portal** is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyses your resource configuration and usage telemetry and then recommends solutions.

No such thing as the **Security Trust Portal in Azure.**

**Azure Activity Log** you can drill down which user had turned off a specific VM. Logs are available for two weeks and therefore we can track back which user had turned off the virtual machine in the last 14 days. Azure Activity logs gives subscription-level events that have occurred in Azure. This can be got from the “Monitor” section of the Azure portal. Azure Activity log can also be used to look for the activity of a Azure resource.

**Azure Monitor** is used to Detect and diagnose issues across applications. This is also used for collecting and analyzing data from Azure public cloud and also from the “on-premises” environment.

**Azure Event Hubs** is an ingestion service. Ingestion mean to input something. Here it means to input events. Event Hubs are also used as streaming platforms. Data collected by Azure Event Hubs are used for real time analytics like live telemetry.

**Azure Service Health** gives the health view of the various Azure services and resources in the Azure Subscription. It also gives the status of the service outages in Azure.

**DDoS protection** is combined with application design best practices, provide defence against DDoS attacks. This means that this would protect websites from various malicious attacks and it has the capability to generate detailed report on the various attacks.

**Azure Firewall** is a managed, cloud-based network security service that protects your Azure Virtual Network resources. Filters network traffic.

**A Network Security Group** is used to filter network traffic to and from Azure resources in an Azure [virtual network](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview) with a network security group.

**Azure Information Protection** protects documents and emails by applying labels.

**Azure Advanced Threat Protection (ATP)** has built-in sensors through which it can monitor the user activities across the Azure network. It is also used to detect suspicious user activities, malicious attacks within an organization itself. It is also used to protect user identities in Azure Active Directory (AD).

**Azure Monitor** collects monitoring data on application, guest operating system, Azure resources, and Azure subscriptions and also about the Azure tenant. The data collected can be of two types: Logs and Metrics. “Log Analytics”

**Azure Active Directory (Azure AD) Identity Protection** this is used for risk analysis.

The **multi-factor authentication** MFA only allows you to set trusted locations, not define locations from which one must login from.

**Azure Bastion** Bastion host is nothing but a jump host that enables a user to get Secured Shell(SSH) and Remote Desktop Protocol access (RDP) to a virtual machine(VM) through the Azure Portal.

**Azure Front Door** you can configure your routing for web applications for high availability and very high performance.

**Azure App Service** is used to build, deploy and scale the user’s web applications.

**PowerApps** is a data platform that provides a rapid application development environment to build custom apps for your business needs.

**Microsoft Azure Machine Learning Studio** (classic) is a collaborative, drag-and-drop tool you can use to build, test, and deploy predictive analytics solutions on your data

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

**Budget alerts** are used to notify you when spending based on usage or cost reaches or exceeds the amount defined in the alert condition of the budget.

**An Azure AD** role is nothing but a collection of permissions

You can move an app to another **App Service plan**, as long as the source plan and the target plan are in the same resource group and geographical region.

The region in which your app runs is the region of the App Service plan it's in. However, you cannot change an App Service plan's region.

**Route-based VPN devices** use any-to-any (wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface).

**Policy-based VPN devices** use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.

**Inbound NAT rule** to port forward traffic from a specific port of a specific frontend IP address to a specific port of a specific backend instance inside the virtual network.

**Dedicated hardware** is not available in a **Public** cloud.

**Azure Import/Export service** – DataSet.csv and DriveSet.csv

The data in an **Azure storage account** is automatically replicated **thrice**

**Azure storage account** is automatically replicated (consider it as a “copy” or as a “backup”) within the data center only and NOT to another Azure data center

**Azure Storage Account**- No size limit

**“General Purpose V2”** is used as “Storage Account Type” as shown below, in addition to storage costs you are also CHARGED for the read and write operations.

**“Outbound”** data transfer is CHARGED between two “different” regions.

**Azure Data Lake** is CORRECT here because it is used for storing different kinds of data such as structured, semi-structured, or unstructured data which is generated from a variety of applications including social networks, IoT hubs and sensors, relational data, videos, web apps, mobile or desktop devices

One **Azure subscription** might be linked with multiple Azure Active Directory tenants.

**The Azure AD tenant** does NOT get deleted automatically if an Azure subscription expires

**NSGs** can be attached to the subnets and allow preventing unwanted traffic to pass through the servers at the backend

**NSGs** cannot be attached directly to the scope of Virtual Networks

**NSGs** have the capability to implement traffic security rules on the NIC (Network Interface Cards) level

**Each Azure subscription** is associated with a single AD tenant and NOT with multiple AD tenants and therefore the answer is NO here

**Local Network gateways**is **CORRECT** as it is used to represent the on-premises VPN device while creating a connection between your on-premises network to Azure VNet. We assign this gateway the IP of the VPN appliance being used in on-premises networks.

**NAT Gateways is INCORRECT** as NAT gateway resources are part of Virtual Network NAT and provide outbound Internet connectivity for one or more subnets of a virtual network. It cannot be used to identify the on-premises VPN device, instead, it enables the outbound connectivity for Azure resources only.

**Virtual Network Gateways**is **INCORRECT** as VNet gateways are used to represent the Azure side of the VPN device while creating the connection between the on-premises network and the Azure virtual network. Hence it cannot be used.

**Application Gateways**is **INCORRECT** as Application gateways are used to route web traffic to your applications both on HTTP and HTTPS.

**Azure Stack edge/ Data box gateway**is **INCORRECT** as it is an AI-enabled edge computing device with network data transfer capabilities.

**An Azure VM is a resource** that CANNOT be deployed across multiple Resource Groups in an Azure subscription

**Azure Sentinel** uses Azure Log Analytics Workspace to store the logs and events

If you **assign permissions** for a user to manage a resource group, the user can manage all the Azure resources in that resource group

**Azure Virtual Machines** provides VIRTUALIZATION.

**Azure Active Directory Premium P2** guarantees at least 99.9 percent availability

**Azure PowerShell** modules can be installed on macOS

It is not a pre-requisite to implement the security recommendations provided by Azure Advisor within a period of 30 days to maintain **Microsoft support.**

**Azure Firewall** does not have “encryption” as one of it’s feature and therefore it will NOT encrypt all the network traffic sent from Azure to internet

**NSG** is used only to filter network traffic to and from Azure and the internet and it will **NOT** encrypt the network traffic

**Azure VMs** that run on Windows Server 2016 does NOT encrypt the network traffic sent

Only one **Azure Free Account** can be created using the same Microsoft account

**Azure subscription** can have only one account administrator

**Azure subscriptions** can be maintained by various companies using their own accounts with an open authentication server eg: Okta Oauth2.0

**Azure services in public preview** “can” be used in production environments

**Azure services in public preview** are not covered under any Service Level Agreement (SLA)

**Azure Free Account** has a spending limit of $200 for the first 30 days

**Inbound data transfer** (into Azure) is ALWAYS FREE irrespective of the account in Azure

**Azure Free Account** can have only 10 web apps as shown below

When **Azure Trial Account** expires you cannot start a new Virtual Machine

**Azure Services** which you deploy are billed against the **subscription** you have

When an organization hosts its infrastructure in the **public cloud**, it no longer requires a data center

There are 13 different type of **metrics** in **Application Gateway** that a user can use for **troubleshooting** the **performance** issue

A user needs to create a TXT record type so that so that the custom domain can be joined to **Azure Active Directory**

**Azure DevOps** **cannot** be used to build and host web apps

**Azure Databricks** is an Apache Spark-based analytics service?